

# Protecting the Public Core of the Internet Perspectives from the Netherlands and Republic of Korea

Edited by Dennis Broeders, Byoung Won Min,  
Arun Sukumar and In Tae Yoo



THE HAGUE  
PROGRAM  
on International  
Cyber Security



DANKOOK UNIVERSITY



이화정치연구소  
EWhA INSTITUTE OF POLITICS



Universiteit  
Leiden

## Acknowledgements

This publication is the result of a bilateral Cyber Dialogue on the Public Core of the Internet held in Seoul on Friday 12 April 2024. The dialogue brought South Korean and Dutch scholars together to discuss domestic and diplomatic approaches to safeguarding the technical and logical infrastructure of the global internet. The dialogue was organised by Dankook University, the Ewha Womans University on the Korean side and Leiden University's The Hague Program on International Cyber Security on the Dutch side. The organisers wish to thank the Dutch Ministry of Foreign Affairs and the Korean Internet Security Agency (KISA) for their support of this academic dialogue. We also wish to thank Dutch ambassador Peter van der Vliet and his team for the support and hospitality offered in Seoul. The responsibility for the content of the contributions lies with the authors.

### Suggested citation:

Dennis Broeders, Byoung Won Min, Arun Sukumar and In Tae Yoo (eds.) (2024) *Protecting the Public Core of the Internet: Perspectives from the Netherlands and Republic of Korea*. The Hague: The Hague Program on International Cyber Security. November 2024.

## Table of contents

### Introduction

1. Korean and Dutch approaches to safeguarding the technical and logical infrastructure of the global internet: convergences and divergences 2  
Dennis Broeders, Byoung Won Min, Arun M. Sukumar and In Tae Yoo

### The concept of the public core

2. Technical precision and diplomatic ambiguity 9  
Olaf Kolkman
3. EU policy and the public core of the Internet: an ever more strategic relationship 20  
Paul Timmers
4. Why multistakeholderism? Ruling the Internet without multilateralism 30  
Byoung Won Min

### Protecting global critical Internet infrastructure: relationship between the public core and internet governance

5. Governing the public core of the Internet: a snapshot of the Netherlands' practices 40  
Jan Aart Scholte & Bibi van den Berg
6. The public core from the perspective of Internet governance 48  
Jungsup Park

### Protecting global critical Internet infrastructure: relationship between the public core and (inter)national security

7. Protecting the public core of the Internet: the Netherlands' security perspective 62  
Paul Ducheine and Peter Pijpers
8. Evolving South Korea's cybersecurity strategy and implications for global critical Internet infrastructure 70  
In Tae Yoo

- Authors 78

# 1. Korean and Dutch approaches to safeguarding the technical and logical infrastructure of the global internet: convergences and divergences

Dennis Broeders, Byoung Won Min, Arun Sukumar and In Tae Yoo

## Introduction

In April 2024, a group of Dutch and South Korean Internet scholars convened for a day long discussion in Seoul on the international protection of core logical and physical infrastructure of the global internet – sometimes discussed as the protection of the “public core of the internet”. This discussion was set up against the background of increasing diplomatic engagement between the Republic of Korea and the Kingdom of the Netherlands, including on the terrain of cyber security. A recent example of cooperation in the field of security, technology and governance are the ReAIM (Responsible Use of AI In the Military Domain) conferences, which were held in The Hague in February 2023 and in Seoul in September 2024. Our academic exchange in Seoul was meant to present and discuss ideas, policies, politics and practices in both countries related to core internet infrastructure and to uncover convergences and divergences. Given the global nature of the internet and, more importantly, the inherently transnational character of its core logical and physical architecture, the internet is an infrastructure that is internationally governed – in addition to the need for sound national policies and maintenance.

The Netherlands and South Korea are both highly digitized capitalist democracies whose economies, societies and governments are intertwined with the internet. Both countries need the internet to be functional, available and free from issues of integrity. Both countries are – to different degrees – aligned with the United States and/or the ‘western likeminded block’ in internet governance, but are also navigating their own course when it comes to the increasingly dominant Sino-American geopolitical and geoeconomic tensions. There are also significant differences between the two countries, that play out in their views on internet governance and international cyber security. Despite the de-territorial nature of the internet, the Republic of Korea is a neighbour of the People’s Republic of China. Proximity is still an important factor in international politics and that also goes for the Republic of Korea’s northern neighbour. The omnipresent threat of the Democratic People’s Republic of Korea – also in cyberspace – is a constant factor in Korean politics. On the Dutch side, the context of the European Union is a constant factor in the development of economic and increasingly security related policy making. Diplomacy and policy making related to – the global – internet is a shared responsibility between member states like the Netherlands and the EU.

Despite these differences both countries can be seen as middle-sized, globally oriented and active agents in the international diplomatic field and within their respective regions, that may benefit by identifying points of convergence and divergence. This project, organised by the University of Leiden, EWha Womans University of Seoul and Dankook University, therefore sought to understand how the two countries think about the concept of the public core of the Internet, how they might differ, and whether there are areas of common ground. To that end, academics and practitioners from both countries prepared short discussion papers that were at the basis of our discussion at the conference. The revised versions of those papers are included in this edited volume.

## *The public core of the internet: concept, norm and short history<sup>1</sup>*

The need to protect the public core of the Internet was highlighted in the recent reports of two intergovernmental groups – the 2019-2021 UN Group of Governmental Experts (GGE) and the 2019-2021 UN Open-Ended Working Group (OEWG) on cyber security – both of which were adopted by consensus.<sup>2</sup> Between 2018 and 2021, there were two parallel UN processes that deliberated rules and norms of responsible state behaviour in cyberspace. While the UN GGE comprised 25 states, the OEWG was open to all UN member states. Notably, the consensus reports of both groups linked the protection of the public core to existing norms on the protection of critical infrastructure. 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).<sup>3</sup> The UN GGE report underlined that such infrastructure is transnational, and goes beyond the protection of national critical infrastructure to include such infrastructure that “provides services across several States such as the technical infrastructure essential to the general availability or integrity of the Internet”.<sup>4</sup>

With the adoption of these reports, the issue of protecting the public core has been placed within the ambit of the UN First Committee on Disarmament and International Security, and states will need to elaborate the precise scope and application of such protections. The concept of the public core has gained acceptance since 2015, and some of its history may speak to interpretations of its content and to growing state and non-state support.

The call to protect the public core of the Internet was originally formulated by the Netherlands Scientific Council for Government Policy in 2015 as a 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.<sup>5</sup> Both states and non-state actors have subsequently deliberated the concept at length, specifically

- 1 This section is adapted from Dennis Broeders and Arun Sukumar (2024) ‘Core concerns: The need for a governance framework to protect global Internet infrastructure’, *Policy & Internet*, Vol. 16(2): 411-427
- 2 United Nations General Assembly, *Open-ended working group on developments in the field of information and telecommunications in the context of international security (“OEWG Report”)*, Final Substantive Report, UN Doc A/AC.290/2021/CRP.2.; United Nations General Assembly. *Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (“UN GGE Report”)*, UN Doc A/ 76/135.
- 3 *OEWG Report*, B.26; For an in-depth analysis of the OEWG and GGE processes and the public core, see Author (2021)
- 4 *UN GGE Report*, III.46.
- 5 Broeders, D. (2015). *The public core of the internet: An international agenda for internet governance*. Amsterdam University Press.

developing proposals for state behaviour on the protection of the public core. The Netherlands addressed the protection of the public core of the Internet in its 2017 *International Cyber Strategy*<sup>6</sup> and in the same year, the multi-stakeholder Global Commission on the Stability of Cyberspace (GCSC) published a norm on the issue.<sup>7</sup> The commission 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”.<sup>8</sup> Since 2017, this norm has found wide support from states. In 2018, it was absorbed into the *Paris Call for Trust and Security in Cyberspace*, a multi-stakeholder initiative championed by the French government.<sup>9</sup> While non-binding in character, the Paris Call has, at the time of writing, been endorsed by 81 states, with the United States joining in November 2021. The ‘public core’ concept has become part of the *EU Cyber Security Act*, which gives ENISA – 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”.<sup>10</sup> In 2022, the European Union updated the Network and Information Systems Directive (NIS2), reiterating its support for the protection of the public core. The directive underlines the cross-border nature of both critical infrastructure and cyber-attacks and urges member states to adopt policies that sustain “the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables”.<sup>11</sup> In April 2022, the US-sponsored *Declaration for the Future of the Internet*<sup>12</sup> called on states to “refrain from undermining technical infrastructure essential to the general availability and integrity of the Internet”. The Declaration has been signed by over 65 states, including the Netherlands and the Republic of Korea, indicating that state support for protecting the public core continues to grow.

However, the norm on the protection of the public core of the internet has also become part of the tug of war in the UN first committee debates about cyber security between the ‘likeminded’ states – a loose coalition of states led by the United States – and states like Russia and China that are arguing for an internet made up of ‘cyber-sovereign states’. For example, Russia circulated a proposal in the ITU in 2021 using the language of the public core of the internet to argue in favour of an international cyber treaty – a long standing wish of the Russian Federation – that would transfer the administration of critical internet resources from the current multistakeholder model to an intergovernmental model. In other words, despite the spread of the norm, a common

6 Government of the Netherlands. “Building Digital Bridges: International Cyber Strategy: Towards an Integrated International Cyber Policy”, 2017: 5. <https://www.government.nl/documents/parliamentary-documents/2017/02/12/international-cyber-strategy>; the new 2023 International Cyber Strategy reiterates the importance of the Protection of the public core of the internet, see: Government of the Netherlands (2023) International Cyber Strategy 2023–2028. *Decisive Diplomacy in the Digital Domain, International Cyber Strategy 2023-2028* | Publication | Government.nl.

7 GCSC, “Call to Protect the Public Core of the Internet” (2017), <https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-Internet.pdf>.

8 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>.

9 Ministère de l’Europe et des Affaires étrangères, *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*, France Diplomacy - Ministry for Europe and Foreign Affairs, <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> (last visited Jun 21, 2021).

10 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

11 Directive (EU) 2022/2555 of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the Union, 14th December 2022, (NIS 2 Directive)

12 *Declaration for the Future of the Internet*, at <https://www.state.gov/declaration-for-the-future-of-the-Internet>.

understanding of it – and the protection that this would support - is not a done deal. Emphasizing the need to protect the public core was an important first step, but equally important is addressing the extent to which states can and cannot assert their jurisdictional claims to such infrastructure.

### *Dutch and Korean perspectives on public core protection*

Even though the concept of the public core is coming up on ten years of history, the respective engagements with the concept differs substantially between the two countries. While the concept originated in the Netherlands and the Dutch government is a staunch norm entrepreneur in favour of the adoption of this norm, the Republic of Korea has not actively engaged with the concept itself - as opposed to (transnational) critical internet infrastructure which is firmly on the national radar - at the policy level. In the papers for this project and in the discussions in Seoul these differences are reflected. However, they also highlighted that the underlying aim of the concept – to safeguard the functionality, availability and integrity of core internet logical and technical infrastructure and the international governance challenges that come with that goal - were a shared concern. There are good reasons why the protection of the public core is of interest to both the Republic of Korea and the Netherlands.

From a Dutch perspective, there are three reasons. In the first place, the Netherlands has a considerable material interest in the protection of the public core of the internet. It is a highly digitised society and economy with an outspoken ambition to be the digital gateway to Europe. Moreover, in terms of core internet infrastructure and organisations the country houses a number of prime assets as it hosts many landing stations for internet sea cables, one of the largest internet exchanges in the world (AMS-IX) and is home of RIPE-NCC, one of the five Regional Internet Registries (RIRs), an organisation that manages the allocation and registration of Internet number resources within a region of the world. Secondly, the Netherlands has an interest in being an international norm entrepreneur in cyberspace. The Netherlands is traditionally a very active member of the international multilateral system and – as an early adopter of the internet – a long time supporter of the multistakeholder model that underpins internet governance. Since organising the 2015 Global Conference on Cyberspace (as part of the so-called London process) the Dutch have invested considerably in their diplomatic efforts in cyberspace. They founded and funded the Global Commission on the Stability of Cyberspace and were a member of the 2017 and the 2021 UN GGEs. Thirdly, these efforts are meant to contribute to a more predictable and stable cyberspace, which is in the interest of a small, heavily digitised, middle power like the Netherlands. As geopolitical tensions are rising and a growing number of countries have designated cyberspace as the ‘fifth domain of warfare’ – including the Netherlands and South Korea itself – and intelligence driven cyber operations are on the rise, the need for ‘rules of the road’ for states in cyberspace is perceived to be vital.

From the perspective of the Republic of Korea many of these themes and ambitions are shared – albeit formulated in different language. Like the Netherlands, South Korea is a major digital hub in the region and home to many cable landing stations. As a peninsular state with a hostile neighbour to the North it has significant interests in protecting subsea cables and satellite connectivity in particular. Moreover, as an internet powerhouse, South Korea has benefited greatly from connectivity and access to the internet for economic development and innovation. In recent years, the development of key emerging technologies, including semiconductors, and the upgrading of defence capabilities that rely on the development of such technologies have

become critical, all of which requires seamless, secure and fast internet connectivity. In this context, supply chain security and data security have become increasingly important. In addition, the need for cybersecurity-related human resources is also very high, and the national efforts are accelerating the development of related industries and human resources. Like the Netherlands, South Korea has a vested interest in ensuring that geopolitical tensions between US and China do not compromise digital accessibility and connectivity. So far the notion of the public core of the internet is not explicitly used in that context, but the fact that South Korea is a signatory to the *2022 Declaration for the Future of the Internet*, that includes the public core norm, suggests that internet connectivity is increasingly regarded to be a transnational diplomatic point of concern, in addition to a domestic policy interest. Moreover, in September 2024, a group of influential states that included the US, EU, the Netherlands and the Republic of Korea endorsed a joint statement calling for the “Security and Resilience of Undersea Cables in a Globally Digitalized World”<sup>13</sup>, underlining a joint commitment to protect the international cable system, a vital element of the public core of the internet. Given the fact that the Republic of Korea is a major power in East Asia that has ambitions to play a larger diplomatic role in the region and at the global stage, the public core might be a concept that fits with its interests in safeguarding stability in cyberspace at both the technical and the political level. In fact, the Republic of Korea was an early player in the cyber field as it hosted the *2013 Global Conference on Cyberspace* in Seoul, drawing in approximately 1,600 attendees with greater representation from countries in the global south. The principle outcome of the third GCCS was the Seoul Framework for and Commitment to Open and Secure Cyberspace, which highlights the importance of universal Internet access. Domestically, there have been concerted calls for the Republic of Korea to develop and a more assertive global agenda in order to fulfil its role as a responsible international actor.

### *Potential convergences and divergences in the approach of both countries*

Despite shared interests and concerns there are also points of divergence, differences in approach, and other concerns that may constrain cooperation and even hinder global dialogue on the issue of the protection of the public core of the internet.

As noted in the report of the Netherlands’ Scientific Council on Government Policy the issue of the protection of the public core of the internet is affected by a growing tension between internet security – the security of the internet as a network of networks - and national security, highlighting state threats through the internet and the possibilities to conduct military and intelligence operations through the internet. That means that many states are grappling with the use of cyberspace as a tool of statecraft. While most states will value the stability of the internet as an infrastructure (with a functional public core) they will at the same time be reluctant to pass on the possibilities the internet offers for offensive and intelligence operations. That potentially provides states with a conundrum. For example, Dutch and Korean intelligence agencies, much like those of other states, would not want to limit their ability to surveil global networks and infrastructure. Question is to what extent this would limit cyber diplomacy towards public core protections? In the Netherlands it has not limited the diplomatic effort to advocate and spread the norm –

13 “Multilateral Meeting on Security and Resilience of Undersea Cables during UN General Assembly High Level Week.” September 25, 2024. *United States Department of State* (blog). Accessed October 14, 2024. <https://www.state.gov/multilateral-meeting-on-security-and-resilience-of-undersea-cables-during-un-general-assembly-high-level-week>.

not in the least because many later formulations create some space for intelligence activities<sup>14</sup> – but for some other countries the norm has seemed too constraining to support.

The multistakeholder model for the governance of the internet – both domestically and internationally – may be a point of Dutch-Korean divergence, although the differences may be less stark than they initially seem. Both the Netherlands and the Republic of Korea have some form of multistakeholder models of internet governance, but perceptions and the mechanisms of those models differ widely. The Netherlands is an open supporter of multistakeholder governance at both the domestic and the international level, whereas the Republic of Korea leans towards greater state involvement and control of domestic internet governance. In the Netherlands the private sector is more active in policy and standard setting while in South Korea the state plays a more coordinating and ‘first-among-equals’ role in the governance process. The central role of the Korea Internet and Security Agency (KISA) may be seen as a kind of compromise between government-led governance and the civil society led governance. Moreover, at the international level South Korea may have questions about the legitimacy of the – American dominated – governance of core critical internet resources. It is an open question to what extent these differences in governance model help or hinder cooperation on public core protections.

While the Republic of Korea and the Netherlands are both concerned about rising geopolitical tensions, especially between the United States and China, the nature of those concerns are different, as is their joint ability to tackle them. Both countries are arguably closer to the US than they are to China, but as a neighbour of China, South Korea has to manage this sensitive diplomatic and strategic relationship more closely. Moreover, the security arrangement between South Korea and the United States is unique in its level of intensity and overall integration as evidenced by the ROK-US Combined Forces Command. This arrangement cannot be compared to the Dutch military connection to the US through NATO, especially not in the post-cold war period. This means that the Republic of Korea has had to figure out its regional and global roles, considering the demands of the United States for a long time and has restricted room to manoeuvre diplomatically oftentimes. In addition to the structural challenges of the US-China strategic competition, South Korea also faces the threat of North Korea. The level of threat is perceived differently by different governments, but globally, North Korea is recognised as a cyber problem state. South Korea is the country that has taken this issue to heart the most. The level of threat posed by North Korea will affect the intensity of South Korea’s response and its overall national security strategy, which influence its approach to the public core of the Internet.

### *Overview of the Track 2 dialogue*

The NL-RoK Track 2 discussions on core internet infrastructure and cyber diplomacy were held on April 12, 2024 in Seoul. The discussions were organized around four distinct topics. The meeting kicked off with a session on the concept of the public core, exploring areas of convergence, differences, and further deliberation between both sides. Here, participants exchanged at length Dutch and Korean perspectives on what they considered part of the public core. The second

14 For example the Global Commission on the Stability of Cyberspace (2017) 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’. This formulation of the norm highlights ‘intentional and substantial damage’ to the public core, acknowledging that many states will allow military and intelligence operations that (mis)use public core protocols and infrastructure, while disallowing substantial damage with intended or unintended transnational effects.

session explored the relationship between the public core of the internet, as well as protections offered under multistakeholder models of internet governance. The idea behind this session was to explore how current protections serve the public core and what could be done by both sides to help enhance those protections through existing internet governance models. The post-lunch session covered increasing threats to the public core – as such threats have grown in severity, it is important to understand the geopolitical motivations of major players towards such threats as well as protections against them. The concluding session wrapped up the daylong dialogue, inviting participants to offer their reflections and also think about how to further revise their papers that had been food-for-thought for the dialogue.

### Papers in this publication

The dialogue produced seven papers that correspond to many of the thematic sessions organized on the day. Jan Aarte Scholte and Bibi van den Berg outline the Dutch approach to governing the public core and its protection, describing it as “polycentric”, i.e., spread across multiple sites. Cutting across a governance landscape filled with actors from various sectors, the governance of core infrastructure in the Netherlands is also “transscalar”, they point out, arguing that these actors have varying global, domestic and local remits. Jungsup Park offers an overview of the landscape of internet governance in Korea, drawing attention in particular to the technical bodies and standards agencies responsible for the protection of core infrastructure. Highlighting the complex architecture of institutions involved in cybersecurity of core infrastructure, including at the Korean Internet Security Agency (KISA), Park notes that the Korean regulatory landscape is comparatively dense. Although there are numerous policies and legislation for the management of major Internet infrastructure (physical and virtual), the governance systems in place reduce scope for government interference or manipulation by major industry players, he notes. Byoung Won Min addresses this tension as well, and in his paper points out that KISA is a semi-governmental agency, while Korea champions multistakeholder governance abroad. His paper takes stock of multistakeholderism in internet governance at the global level, and address how it can be made more participatory, accountable and effective, especially in the protection of core infrastructure.

Olaf Kolkman offers a briefing paper that explores the technical contours of the public core, but also reviews progress made by multistakeholder bodies such as the Global Commission on the Stability of Cyberspace in articulating and implementing norms for its protection. The geopolitical and diplomatic aspects of public core protections are significant. Paul Ducheine and Peter Pijpers review the Dutch position on the protection of the core, and outlines the effectiveness of existing international law in offering adequate protection from state-backed attacks on the core. Paul Timmers examines the role, historical concerns, and evolution of European Union policy towards protecting the public core of the Internet. Having adopted the public core formulation in its Cybersecurity Act, the EU is progressively taking steps to address the resilience of its core infrastructure like subsea cables, Timmers notes. In Tae Yoo points out that the Republic of Korea, while not having embraced the concept of the public core, has put in place regulations to protect critical information and communication infrastructure. It is important for Korea to acknowledge the importance of international cooperation and diplomatic initiatives on the public core, he notes, given the importance of transnational critical infrastructure to the country’s interests.

## 2. Technical Precision and Diplomatic Ambiguity

Olaf Kolkman<sup>1</sup>

### Introduction

In this paper I share a perspective on the public core and the understanding of its technical aspects. The perspective is one of an Internet architecture expert that entered the world of ‘cyber’ after engaging in Internet governance and developing and standardising Internet security solutions for the Internet naming system (domain name security extensions or DNSSEC).

Below we first describe the context in which the first discussions of the concept of the public core took place. We then look at how the definition of the technical terms evolved and finally provide a perspective on that evolution and the future of the term ‘public core’ and its definitions.

### The context

I first learned about the concept of the public core in April 2015 through a publication from the Scientific Council for Government Policy in the Netherlands (the WRR Report),<sup>2</sup> but it was only around the end of 2015 that I got involved in the discussions about defining a norm based on it. After an introduction through a mutual acquaintance, Dennis Broeders invited me to give a lecture on Internet governance *with a (strong) emphasis on how the technical side thereof is managed. In other words, not a story about WSIS and IGF, but much more a story about the IETF, W3C, and IAB. What are the stakes, how do people work, participation and membership, steering role, changing context etc.*<sup>3</sup> It must have been around that lecture that Dennis and I started discussing a norm based on the concept of the public core.

That conversation took place in a context.

<sup>1</sup> I’d like to acknowledge Pablo Hinojosa, Catherina Garcia and Dennis Broeders for their valuable thoughts during the development of this paper.

<sup>2</sup> Dennis Broeders, *The Public Core of the Internet: An International Agenda for Internet Governance* (Amsterdam: Amsterdam University Press, 2015).

<sup>3</sup> Dennis Broeders, private communication, 9 September 2015, quoted with permission.

The first half of the 2010s had seen a number of events that had rattled the Internet governance world. Below are a few examples that had made it onto the radar of members of the Internet technical community<sup>4</sup> such as myself.

- In 2012 the World Conference on International Communications (WCIT) took place. The conference was strongly divided on whether the Internet should be seen as traditional telecommunications infrastructure and therefore subject to the regulatory regime imposed by the treaty instead of the light-handed multistakeholder approach of Internet governance. Eventually 55 International Telecommunication Union (ITU) member states did not sign the final acts. In her review of the conference, which describes among other things the opposing views on Internet governance, settlement regimes and cybersecurity, Deborah Housen-Couriel called this ‘the Dubai clash’.<sup>5</sup>
- In 2013 Edward Snowden revealed thousands of classified documents from the US National Security Agency, suggesting Internet-scale surveillance.<sup>6</sup> As a result, technical specialists in the Internet Engineering Task Force reassessed the threat models and decided that pervasive surveillance is *an attack on privacy of Internet users and organisations*.<sup>7</sup>
- In March 2014 the US government announced the conditions under which it was willing to transition key domain name functions, namely its responsibilities in maintaining the ‘root’ of the DNS.<sup>8</sup> Historically there had been a lot of tension around the direct (contractual) involvement of the United States in one of the few centralised functions needed for Internet operations: the DNS root zone.
- In April 2015 the Global Conference on CyberSpace was held in The Hague, the fourth edition of the London Process.<sup>9</sup> The Netherlands had chosen to bring various communities together, and while civil society and the private sector had been engaged in the London process, it was the first time that members of the Internet technical community were present. An explanation is that Internet governance issues are mostly dealt with by the Ministry of Economic Affairs, and by involving it in the organisation, together with the Ministries of Security and Justice and Foreign Affairs, its network was drawn into the conference as well. The result was that a number of panels had members of the technical community who brought a unique perspective – namely a deep understanding of a globally interoperable open technical infrastructure –

4 The term ‘technical community’ is a term of art in this context: in Internet governance the concept of the technical community – a community of practitioners with a clear understanding of the technology – as a stakeholder in governance was recognised in the Tunis Agenda. See <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>.

5 Deborah Housen-Couriel, ‘The “Dubai Clash” at WCIT-12: Freedom of Information, Access Rights, and Cyber Security’, in *Law and National Security: Selected Issues*, ed. Pnina Sharvit Baruch and Anat Kurz (Tel Aviv: Institute for National Security Studies, 2014), pp. 85–102.

6 E.g. Ewen Macaskill and Gabriel Dance, ‘NSA Files: Decoded’, *The Guardian*, 1 November 2013. <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>.

7 Internet Engineering Task Force memo, ‘Pervasive Monitoring Is an Attack’, May 2014. <https://datatracker.ietf.org/doc/html/rfc7258>. As an aside, it should be noted that ‘attack’ should be interpreted in the context of information security and not in the context of cyber diplomacy. The request for comments is very precise in defining the word ‘attack’ for its own purpose: ‘The term “attack” is used here in a technical sense that differs somewhat from common English usage. In common English usage, an attack is an aggressive action perpetrated by an opponent, intended to enforce the opponent’s will on the attacked party. The term is used here to refer to behavior that subverts the intent of communicating parties without the agreement of those parties.’ We mention this because it is not uncommon for stakeholders with different backgrounds to attach slightly different meanings to the same word.

8 National Telecommunications and Information Administration, ‘NTIA Announces Intent to Transition Key Internet Domain Name Functions’, 14 March 2014. <https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>.

9 <https://web.archive.org/web/20180421055009/http://gccs2015.com>.

and thereby enriched and broadened the discussion,<sup>10</sup> but also a panel was specifically focused on Internet governance institutions – a topic that was mostly foreign to the GCCS crowd.<sup>11</sup> The Internet Society introduced the concept of collaborative security<sup>12</sup> at the conference. Broeders’ WRR publication on the public core appeared around the same time.

Of course, cybersecurity incidents had been part of the daily routine of anybody connected to the Internet ever since the Morris worm, and in the cybersecurity world ‘advanced persistent threats’ (APTs) was already a commonly used term. But cybersecurity culture was mostly limited to protecting the assets of an organisation (or country). That security posture is about assessing the risks and analysing the threats to one’s own assets, not to the global system as a whole.

In the Internet technical community there had been work to mitigate security issues inherent to the global Internet, and on the naming and routing protocols fundamental to securing the global Internet. In particular, the protocol used for Internet naming had been developed. (Technically, the domain name system (DNS) was extended with the security feature called DNSSEC.<sup>13</sup>) In 2015 production-quality DNSSEC implementations had been developed and seen limited deployment.<sup>14</sup> For the numbering and routing infrastructure the first steps in attaining global security had been taken by the standardisation and deployment of the Routing PKI (RPKI), a cryptographic infrastructure needed to bind addressing resources to networks. At the same time technologies to secure the routing were being standardised.<sup>15</sup> Also, around that time, the first steps for establishing the Mutually Agreed Norms for Routing Security (MANRS), a community-based best-practices approach to routing security, had been taken.<sup>16</sup> Participants in the MANRS initiative, such as network providers and Internet exchange points, pledge to take certain actions that eventually will increase routing security and resilience.

In preparation of the 2015 GCCS we realised that those two security postures – focusing on one’s own assets vs protecting the global public commons – needed to be made explicit. With the Internet Society’s collaborative security approach<sup>17</sup> we tried to bridge these two worlds – corporate and Internet – and laid out five key elements for approaching cybersecurity in a global Internet-wide setting. The concept of the public core and the collaborative security approach shared the idea that for a secure cyberspace one has to take care not only of the individual pieces of Internet infrastructure but also of the system as a whole.

10 <http://web.archive.org/web/20160321213134/https://www.gccs2015.com/programme>. Notice the presence of Internet Society staff on multiple panels; however, others that often identify as being members of the technical community also gave input in various sessions.

11 See ‘Programme Global Conference on CyberSpace 16 and 17 April 2015’ <http://web.archive.org/web/20160321213134/https://www.gccs2015.com/programme?programme=2>. The parallel session on 17 April at 11:15 was on ‘Internet Governance – Global Cooperation for a Sustainable Future’.

12 Internet Society, ‘Collaborative Security: An Approach to Tackling Internet Security Issues’ <https://www.internetsociety.org/wp-content/uploads/2015/04/Collaborative-Security.pdf>.

13 <https://datatracker.ietf.org/doc/html/rfc4033>, <https://datatracker.ietf.org/doc/html/rfc4034>, <https://datatracker.ietf.org/doc/html/rfc4035> and others.

14 For instance, the first root signing ceremony had taken place on 16 June 2010 (see <https://www.iana.org/dnssec/ceremonies/1>).

15 RFC 8205 would appear in September 2017, but standardisation work had started in 2011. See <https://datatracker.ietf.org/doc/html/rfc8205>.

16 Andrei Robachevsky, ‘First Draft of Routing Resilience Manifesto Now Available for Comment’ <https://manrs.org/2014/07/first-draft-of-routing-resilience-manifesto-now-available-for-comment>.

17 Internet Society, ‘Collaborative Security’.

All this is to illustrate that the idea of forming a norm for the public core fell on fertile ground. It connected thoughts from the Internet community to a world different from the Internet technical community, and the more traditional cybersecurity community: the cyber-stability community.

### Development of the norm

The WRR report called for a norm but did not go into specific definitions: ‘In order to protect the Internet as a global public good there is a need to establish and disseminate an international standard stipulating that the Internet’s public core – its main protocols and infrastructure, which are a global public good – must be safeguarded against intervention by governments.’<sup>18</sup> The intent was to develop wording that could be used as input to the 2016–2017 Group of Governmental Experts (GGE) process, in which the Netherlands had a seat. Below we recall how the technical definition(s) evolved.

#### UNIDIR/CSIS

On 9 and 10 February 2016 the United Nations Institute for Disarmament Research (UNIDIR) and the Center for Strategic International Studies (CSIS) organised a workshop at the Palais des Nations in Geneva titled ‘International Security Cyber Issues Workshop Series:’<sup>19</sup> The Future of Norms to Preserve and Enhance International Cyber Stability’. Session 2, titled ‘Technologists’ Perspectives and Ideas for Future Norms’, brought the perspectives of some members of the Internet technical community. As such the panel brought several arguments as to why further development of a norm for the public call is relevant.<sup>20</sup> It also brought the realisation *that the tech community is speaking a completely different language to that of the policy community, and that further progress may require development of a ‘common dialect’ for technologists, diplomats, and researchers.*

To illustrate the language differences, just look at the word ‘norm’, as its use might lead to confusion. In the technical community it can be interpreted as a ‘normative specification’ imposing fairly strict rules to enable technical interoperability, while diplomats see it as voluntary behaviour of states. Communities also take a baseline level of knowledge for granted. For the cyber-stability community, ‘critical infrastructure’ has a legal context and critical infrastructure is identified by sovereigns; technologists have a different intuition with the word and see e.g. the routing system as a critical infrastructure. Moreover, for technologists it is often important to get to a mathematical, precise, unambiguous formulation of a specification, while for diplomats a certain amount of diplomatic ambiguity might be needed to get consensus during the negotiation of text and treaties.

<sup>18</sup> Broeders, *The Public Core of the Internet*, p. 95.

<sup>19</sup> UNIDIR and CSIS, *Report of the International Security Cyber Issues Workshop Series*. <https://unidir.org/files/publication/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf>.

<sup>20</sup> UNIDIR and CSIS, *Report of the International Security Cyber Issues Workshop Series*, p. 13.

### Clingendael

On Monday 11 July 2016, the Netherlands Institute of International Relations Clingendael and the Netherlands Ministry of Foreign Affairs organised an expert meeting in The Hague on international norm setting to protect the public core of the Internet. The aim of the brainstorm session was to draft a norm that could possibly be submitted to the 2016 report of the UN Group of Governmental Experts (UNGGE).

The outcome from the workshop was a non-paper on the norm of non-intervention in the public core of the global Internet. It contained the following rendition of the norm: *Without prejudice to its rights and obligations under international law, a State should not conduct or knowingly [support/condone/allow] [ICT] activity that intentionally damages the extraterritorial availability or integrity of the core forwarding and naming functions of the [Internet/global public network].*<sup>21</sup>

The report provided definitions for all terms in the norm. Looking at the more technical terms in the Clingendael non-paper, we see that *integrity* refers to the ability to cryptographically verify integrity but does not explicitly refer to the infrastructure and the protocols needed for that. The definitions of *forwarding* and *naming* refer to a number of elements that we will also see in the reports from the Global Commission on the Stability of Cyberspace, in the next section.

The non-paper also provided examples of what constitutes violation of the norm to help the reader interpret the technical meaning.

### The Global Commission on the Stability of Cyberspace

The Global Commission on the Stability of Cyberspace (GCSC) was established on 18 February 2017. Twenty-six commissioners with various backgrounds and experience (public sector, private sector, academia, civil society and technical community) proposed eight norms for consideration by the UNGGE and in other processes. During the Global Cyber Security Conference in New Delhi in November 2017 the commission issued ‘a call for the protection of the public core of the Internet’,<sup>22</sup> which reads:

#### Non-Interference with the public core

*Without prejudice to their rights and obligations, state and non-state actors should not conduct or 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.*

In a footnote it explains: ‘Elements of the public core include, inter alia, Internet routing, the domain name system, certificates and trust, and communications cables, which have been further defined in the Definition of the Public Core, to which the norm applies.’

<sup>21</sup> ‘Clingendael: Non-paper on the Norm of Non-Intervention in the Public Core of the Global Internet’, from the archive of the author.

<sup>22</sup> Global Commission on the Stability of Cyberspace, ‘Call to Protect the Public Core of the Internet’, November 2017. <https://cyberstability.org/assets/images/norms/call-to-protect-the-public-core-of-the-internet.pdf>.



The ‘Definition of the Public Core’ document<sup>23</sup> was based on a survey done among experts on communications infrastructure and cyber defence to assess which infrastructures were deemed most worthy of protection. The participants were asked to rank 11 categories on a scale of 0 to 10, with 0 being ‘unworthy of special protection’ and 10 being ‘essential to include in the protected class’; all surveyed categories ranked between 6.02 and 9.01. From this the commission defined ‘the public core of the Internet’ to include packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, and physical transmission media. In its report the GCSC went into more detail about what constitutes those categories. In Table 1, we compare some definitions from the global commission with the definitions that came out of the Clingendael non-paper.<sup>24</sup> What we see is that the GCSC document went into much more precise technical detail than the Clingendael non-paper. We also see that the GCSC report does not define integrity but talks about the cryptographic mechanisms that are needed to provide integrity protection and other security services such as authenticity and confidentiality.

In both documents the public core is defined to include non-tangible elements such as protocols and even operational and standardisation processes.

Whether that amount of detail is needed within the cyber-diplomacy processes is not clear. Details will help with understanding whether a violation of the norm has taken place or may prevent violation of certain types of infrastructure in the first place. But these lists of detailed technologies cannot remain stable as the environment evolves. In fact, the GCSC report contained an explicit disclaimer that ‘this definition may be broadened in the future’. Besides, there exists a tension between the technical precision of lists of technologies and the digital ambiguity needed to get closure in the diplomatic process.

<sup>23</sup> Global Commission on the Stability of Cyberspace, ‘Definition of the Public Core, to which the Norm Applies’, May 2018. <https://hcss.nl/wp-content/uploads/2022/08/Definition-of-the-Public-Core-of-the-Internet.pdf>. The final GCSC report contains the same expansion on the definition of the public core as the earlier document: see <https://cyberstability.org/report.html#item-11>.

<sup>24</sup> The comparison is illustrative: we do quote the definition of all terms.

Table 1. Examples of detailed technical description of the elements of the public core

	Integrity	Forwarding	Naming
Clingendael	The integrity of data is, at its most basic, its property of being identical to and unmodified in any way from that which was created by its original author. In computer science and telecommunications, the service of data integrity is dependent not upon the coincidence of data having been transmitted in unmodified form, but upon the ability to prove that it has been transmitted so. This is typically achieved through the creation of a cryptographic signature ‘over’ the data, which allows anyone to subsequently verify or disprove that a copy of the signed data is identical to the data over which the signature was originally affixed. The creation of the cryptographic signature does not imply or impose confidentiality of the data.	The forwarding of data is the service of its transmission in accordance with the End-to-End Principle: that data introduced into the network by a sender should be forwarded promptly and uniquely to its intended recipient in unmodified form. Elements of the forwarding infrastructure include, among others: key routers and switches, Internet Exchange Points, radio-frequency and free-space optic transmission links, and terrestrial and undersea copper and fibre-optic cables. Forwarding paths are established through routing and switching protocols. Internet Service Providers (ISPs) are the principal organisational agents of forwarding in the Internet.	Naming is the system of ‘service discovery’ whereby something that can be named by one person may be found and communicated with by another person. Naming services typically translate between human-readable natural-language names (such as email and web addresses, or even keywords or search terms) and the machine-readable addresses required by the forwarding infrastructure (such as Internet Protocol version 4 (IPv4) or version 6 (IPv6) addresses, or Ethernet Media Access Control addresses). The denial of naming services renders the forwarding infrastructure largely unusable by humans and most automated processes, while the usurpation of naming services misdirects communications to unintended recipients. The Domain Name System (DNS) is the ubiquitous naming system on the internet.

Table 1 continued

	Cryptographic mechanisms	Forwarding	Naming
GCSS	The cryptographic mechanisms of security and identity include, but are not limited to: the cryptographic keys that are used to authenticate users and devices and secure Internet transactions, and the equipment, facilities, information, protocols and systems that enable the production, communication, use and deprecation of those keys. This includes PGP key servers, Certificate Authorities and their Public Key Infrastructure, DANE and its supporting protocols and infrastructure, certificate revocation mechanisms and transparency logs, password managers, and roaming access authenticators. It also includes the integrity of the standardisation processes and outcomes for cryptographic algorithm and protocol development and maintenance and the design, production and supply chain of equipment used to implement cryptographic processes.	Packet routing and forwarding include, but are not limited to: the equipment, facilities, information, protocols and systems that facilitate the transmission of packetised communications from their sources to their destinations. This includes Internet Exchange Points (the physical sites where Internet bandwidth is produced) and the peering and core routers of major networks that transport that bandwidth to users. It includes systems needed to assure routing authenticity and defend the network from abusive behaviour. It includes the design, production and supply chain of equipment used for the above purposes. It also includes the integrity of the routing protocols themselves and their development, standardisation and maintenance processes.	Naming and numbering systems include, but are not limited to: systems and information used in the operation of the Internet's DNS, including registries, name servers, zone content, infrastructure and processes such as DNSSEC used to cryptographically sign records, and the whois information services for the root zone, inverse-address hierarchy, country-code, geographic and internationalised top-level domains and for new generic and non-military generic top-level domains. It includes frequently used public recursive DNS resolvers. It includes the systems of the Internet Assigned Numbers Authority and the Regional Internet Registries which make available and maintain the unique allocation of Internet Protocol addresses, Autonomous System Numbers and Internet Protocol Identifiers. It also includes the naming and numbering protocols themselves and the integrity of the standardisation processes and outcomes for protocol development and maintenance.

### From technical precision to diplomatic ambiguity

The lack of consensus in the 2017 GGE had little to do with the precision in the technical definition,<sup>25</sup> and while the norm to protect the public core of the Internet has found its way into other processes such as the Paris Call,<sup>26</sup> the remnants of the original idea appeared in the 2021 final report of the Open-Ended Working Group (OEWG),<sup>27</sup> in which states '[endeavour] to ensure the general availability and integrity of the Internet', and in the 2021 GGE Report with similar wording in Norm 13.f:<sup>28</sup> 'Critical infrastructure may also refer to ... the technical infrastructure essential to the general availability or integrity of the Internet.'

The astute reader of the OEWG and GGE texts will notice that a further definition of what makes up the Internet is missing from the documents. Besides, clarifications such as 'infrastructure may be owned, managed or operated by the private sector, may be shared or networked with another State or operated across different States' in the OEWG report suggest that the infrastructure is mostly tangible hardware and the intangibles that were so clearly part of the original public core idea are not referred to. The GGE report only refers to technical infrastructure, which also seems to suggest tangibles.

That is unfortunate because the Internet does not operate only because of the availability of subsea cable, switches at Internet Exchange Points, servers for the DNS, hardware signing machines (HSMs) for public key infrastructures and other types of hardware. The Internet, as a network of networks, exists because of voluntary adoption of a number of technical standards, (multi-)stakeholder managed resources (e.g. ICANN for the DNS, the Regional Internet Registries for IP addresses) and decentralised collaboration between networks.

The public core idea also captured these intangibles because damaging the trust in those intangibles can cause delayed and long-term damage to the general availability and integrity of the Internet and potentially lead to fragmentation. For instance, if cryptographic standards are undermined, they may not be deemed usable in large parts of the world, causing interoperability problems.

<sup>25</sup> See, for instance, Christian Ruhl, Duncan Hollis, Wyatt Hoffman and Tim Maurer, 'The UN GGE', in *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads*, ed. Christian Ruhl, Duncan Hollis, Wyatt Hoffman and Tim Maurer (Washington, DC: Carnegie Endowment for International Peace, 2020), pp. 4–6.

<sup>26</sup> <https://pariscall.international/en/principles>.

<sup>27</sup> United Nations General Assembly, A/AC.290/2021/CRP.2. <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>.

<sup>28</sup> United Nations General Assembly, A/76/135. <https://documents.un.org/doc/undoc/gen/n21/075/86/pdf/n2107586.pdf>.

Another way to think of the intangibles is through the lens of the Critical Properties of the Internet,<sup>29</sup> a framework developed by the Internet Society in the context of its Internet Impact Assessment Toolkit.<sup>30</sup> The Internet Society identifies five critical properties (CPs). These are, in no particular order:

- an accessible infrastructure with a common protocol
- an open architecture of interoperable and reusable building blocks
- decentralised management and distributed routing system
- common global identifiers
- a technology-neutral general-purpose network.

We refer to the original ISOC papers for a detailed explanation of these. We<sup>31</sup> make the case that damaging these critical properties is likely to be irreversible and will lead to fragmentation of the Internet. A number of these critical properties depend on the trustworthiness of the actors. For instance, in the context of the CP *distributed and decentralised routing system* there are expectations that most actors work towards global connectivity; in the context of CP *Open Architecture of interoperable and reusable building blocks* the weakening of cryptographic primitives through a standards process would be seen as undermining the CP; and in the context of CP *common global identifiers* interfering with root zone registration would be seen as damaging that CP. Within the Impact Assessment Toolkit we further look at enablers for openness, globality, trustworthiness and security that also relate to general availability and integrity of the Internet.

I am not arguing that there is a one-to-one mapping between the Impact Assessment Toolkit and the call to protect the public core; that wouldn't be likely since they are written for different purposes: one as a proposed norm for international stability, the other as an operational toolkit for policy making. But I do try to illustrate that the intangibles are an important consideration in other Internet frameworks.

Back to the OEWG report.

With the OEWG report the UN members clearly take a step forward in recognising that the Internet is different enough from critical infrastructure and critical information infrastructure to warrant its own protection – this is a nuanced difference from the 2021 GGE report, where technical infrastructure essential to the general availability or integrity of the Internet is provided as an example of what critical infrastructure may refer to. The wording in the OEWG report is results-oriented: as such, the definition of all the elements, tangible or not, with great technical precision may not be needed to assess whether general availability or integrity of the Internet has been impacted. That type of damage will be easy for anybody to see.

<sup>29</sup> Internet Society, *The Internet Way of Networking: Defining the Critical Properties of the Internet*. <https://www.internetsociety.org/wp-content/uploads/2020/09/IWN-IIAT-Defining-the-critical-properties-of-the-Internet.pdf>.

<sup>30</sup> Internet Society, *Internet Impact Assessment Toolkit*. <https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit>.

<sup>31</sup> This author has been a major contributor to the Internet Society's papers.

However, for states that want to operationalise their promise to protect the general availability and integrity of the Internet, the public core definition, with a relatively detailed description of the elements, may inform them how to operationalise their positive obligations. In fact, the GCSC's call to protect the public core was a call for action for a broader community of state and non-state actors. As such, initiatives such as the Mutually Agreed Norms for Routing Security (MANRS<sup>32</sup>) and the recent attention of the US government to routing security<sup>33</sup> could be seen as aspects of operationalising the call.

Within the context of the UN first committee discussions, it remains to be seen whether a more detailed description of the technical elements will make a difference if and when the current wording about the 'general availability and integrity of the Internet' evolves into international normative and/or legal obligations. That evolution is a responsibility more for experts on international law and diplomats than for a member of the technical community. I am convinced that involvement of the technical community and other stakeholders in that discussion will lead to better outcomes, even though during that process technical precision will necessarily be diluted for diplomatic progress towards an outcome document.

Regardless of the UN outcome, the technical community and the many private entities that operate the networks and infrastructure that allow us to internetwork will take the technical measures to improve the security of the Internet – first committee UN documents will probably not change their pace.

<sup>32</sup> MANRS, 'Protect the Internet'. <https://manrs.org>.

<sup>33</sup> See Reply *Comments of the National Telecommunications and Information Administration*, FCC Dkt 22-90 (filed 10 May 2022). See also NTIA, 'Secure Internet Routing' (<https://www.ntia.gov/blog/2023/secure-internet-routing>) and references for more casual background.

## 3. EU policy and the public core of the Internet: an ever more strategic relationship

Paul Timmers

EU policy in relation to the public core of the Internet<sup>1</sup> has been developing over at least two decades. This analysis illustrates the evolving and ever wider scope of what is regarded in EU policy as the public core of the Internet. In line with the growing importance of ‘digital’ in geopolitical, economic, social and democratic life, EU policy for the public core of the Internet has become ever more strategic. Yet this policy could and probably should become more comprehensive, focused and complete in order to meet the EU’s aspirations for the future Internet, based on values, resilience and strategic autonomy.

### Introduction

The EU has had a long involvement in the public core of the Internet. Over the past few years this became even more intense due to rising concerns about cybersecurity, incidents of geopolitical importance, and the expanding scope of EU cybersecurity and data protection legislation and policy. This paper first gives some historic elements of the EU’s involvement in the public core and then zooms in on cybersecurity and the recent hotspot of concerns about security and resilience of undersea cables, before concluding with some other relevant policies. From a reflection on history and current status, the somewhat paradoxical conclusion is that despite an ever more comprehensive and stronger EU policy approach to the public core of the Internet, the goal of an all-inclusive, global, unfragmented and peaceful Internet seems further away than ever.

### A short history in highlights

#### Opening up global governance

From 1998 onwards and for about a decade and a half, the EU got deeply involved in a limited part of international governance of the public core of the Internet, namely the organisation of domain name management (focusing on the organisational layer of the public core<sup>2</sup>). The EU was seeking to reform ICANN<sup>3</sup> and loosen it from US control. This was partially successful, but even in 2014 the European Commission (EC)<sup>4</sup> complained that ICANN remained incorporated in the USA

1 The shorthand ‘the public core’ is also used here.

2 Dennis Broeders distinguishes logical, physical and organisational layers in the public core of the Internet. See Dennis Broeders, ‘Aligning the International Protections of “the Public Core of the Internet” with State Sovereignty and National Security’, *Journal of Cyber Policy*, vol. 2, no. 3 (2017), pp. 366–376.

3 ICANN is the international organisation coordinating and managing the Internet global domain name system, where actual systems management is limited to the root zone file, which contains a list of all top-level domains (TLDs) and the corresponding IP addresses of the name servers that host them.

4 The European Commission is the executive branch of the European Union, responsible for proposing legislation, implementing decisions, upholding the EU treaties and managing the day-to-day business of the EU.

and under Californian law. The EU also pushed for greater multistakeholder and international governmental involvement, and was largely successful. An important instance of this success was the transition of Internet Assigned Numbers Authority (IANA) stewardship from the US government to ICANN.<sup>5</sup> Finally, the EU advocated that ICANN would be principles-based, which was partially achieved. ICANN’s principles are for a ‘stable, secure, and unified global Internet’ whereas the EU’s principles for the Internet are ‘single, open, free, unfragmented, inclusive, transparent and accountable multistakeholder, respect for human rights, fundamental freedoms, democratic values, linguistic and cultural diversity, and care for vulnerable persons’.<sup>6</sup>

EU policy and law does not provide a definition of the public core of the Internet even if it does refer to specific physical, logical and organisational elements when the public core is discussed: for instance, the physical Domain Name System (DNS) and its governance, or, as we discuss below, physical core connectivity infrastructure such as undersea cables. Data is also in scope, but only insofar as directly related to these elements (generally, EU data legislation is ‘horizontal’, i.e., not usage-specific).<sup>7</sup> An example is the EU data protection law, the General Data Protection Regulation (GDPR), as applied to the DNS system, as discussed next.

#### The far reach of EU data protection

Although the push for reform of ICANN abated, interaction between the EU and ICANN was very intense from 2016 onwards, specifically on personal data protection. The question was how to deal with the challenging issue of making WHOIS<sup>8</sup> compatible with EU data protection law, the GDPR. To some extent, ICANN is still struggling with GDPR-induced fragmentation, namely the fact that responsibility for personal data related to domain registration must be with registrars at a national or local level. In response to the GDPR and to deal better with law enforcement requests, ICANN has developed new functionality to handle domain name information, including personal data (as part of RDS – Registration Directory Service, formerly known as WHOIS).

#### Cybersecurity rises to the top of the agenda

The other issue that rose in importance and is nowadays at the top of agendas is cybersecurity. Cybersecurity became an important concern in the EU around 2012 and then developed into one of the most active areas of EU digital policy development, with an ever-extending reach that touches the public core to a significant extent – and ever more so, the wider the definition of ‘public core’ becomes.

The main EU cyber laws are the Network and Information Security (NIS) Directives. The first edition, NIS1, was applicable from 2016 and was succeeded from October 2024 onwards by the more extensive NIS2. These Directives<sup>9</sup> prescribe cybersecurity risk management with a view to increasing the resilience of critical infrastructures within the EU’s Single Market.

5 <https://www.Internetsociety.org/iana-transition>.

6 European Commission, *Internet Policy and Governance – Europe’s Role in Shaping the Future of Internet Governance*, COM(2014)72 (2014).

7 See also ‘Governing the Public Core of the Internet: A Snapshot of the Netherlands’ Practices’ by Jan Aart Scholte and Bibi van den Berg in this collection.

8 The WHOIS system is a protocol to query the databases that link a registration of a domain name to an IP address.

9 EU Directives need transposition into national law; EU Regulations are directly and uniformly applicable law.

NIS1 and even more so NIS2 are highly relevant for the public core. NIS1 is directly applicable to the public core, namely to Internet exchange points (IXPs), DNS service providers and top-level domain (TLD) name registries. They are ‘operators of essential services’ (OESs). These are ‘designated’, i.e. identified, by the EU Member States, who have to ensure that these OESs comply with obligations for risk-management-based cybersecurity and incident notification.

Interestingly, DNS, TLD and IXP providers were not in the NIS1 category of digital service providers (DSPs), which consists of providers of cloud computing services, online search engines and online marketplaces. DSPs in NIS1 had uniform requirements across the EU, unlike OESs. The reason for the different treatment originates in the balance of competence between the EU and its Member States in matters close to national security. National security is – in principle – solely under the control of the EU Member States, since Article 4(2) of the Treaty on the European Union states: ‘The Union ... shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order, and safeguarding national security. National security remains the sole responsibility of each Member State.’

The NIS2 Directive is a major revision in this respect. In NIS2 there can still be some national variations, but far fewer, and DNS/TLD in particular are mentioned as needing harmonised rules as they are of a cross-border nature.<sup>10</sup> For instance, there can no longer be variation in the identification of NIS-relevant DNS, TLD and IXP providers as for those there is now a uniform size cap rule, in essence bringing all medium-sized<sup>11</sup> and larger providers into the NIS fold. DNS root name server operators are not in scope (which is a clarification on NIS1).<sup>12</sup> The extraterritorial reach is maintained, i.e. foreign providers are also under NIS obligations where they deliver services into the EU (they need to have a legal representative in the EU).

NIS2 is even more relevant than NIS1 to the public core as it added a whole set of requirements beyond NIS1. For instance, NIS2 explicitly states that EU Member States shall adopt policies to sustain ‘the general availability, integrity and confidentiality of the public core of the open Internet’. Furthermore, additional TLD registries requirements were considered necessary on the ground of combating DNS abuse. TLD registries have obligations for access under criminal law, incident prevention and response, and verification of domain name registration data. The implementation of these must progress as best practice develops, including in secure electronic identification.

10 Detailed requirements are fixed by an implementing act that is added to NIS2. This allows the European Commission to ensure an EU-wide identical (i.e. harmonised) approach to cybersecurity risk management.

11 E.g. 250+ employees. For the precise rules see the law itself.

12 Recital (32) of NIS2 says: ‘Upholding and preserving a reliable, resilient and secure domain name system (DNS) are key factors in maintaining the integrity of the Internet and are essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to top-level-domain (TLD) name registries, and DNS service providers that are to be understood as entities providing publicly available recursive domain name resolution services for Internet end-users or authoritative domain name resolution services for third-party usage. This Directive should not apply to root name servers.’ Root name servers were included in the initial NIS2 legal proposal. ICANN successfully argued that ‘12 independent organizations ... provide root name service for the greater good of all Internet users, not for revenue. If undue, and in 10 of 12 cases, extra-territorial, regulatory oversight were to be applied by the EU, it is possible such voluntary service would no longer be feasible, resulting in a potential fundamental restructuring of how root name service is provided with unknown long-term consequences.’ (ICANN, ‘ICANN Org Provides Feedback on the Proposed NIS2 Directive’ (2021). <https://www.icann.org/en/announcements/details/icann-org-provides-feedback-on-the-proposed-nis2-directive-19-3-2021-en>.) The final legal text of NIS2 excludes root name servers.

Resilience is also to be supported by diversification of DNS resolution services, although that is a soft requirement in the law. The complement to this is that a public and secure European DNS resolver service, DNS4EU, is to be put in place from 2025 onwards, when the startup phase will get support from EU funding. The use of DNS4EU is voluntary and thus would not risk fragmenting the Internet.<sup>13</sup> NIS2 also extends the scope to ISPs (which may provide DNS services). NIS2 also moves into ICT supply chain security, setting up mechanisms for security risk assessment of critical supply chains. This part of NIS2 is, however, formulated with softer wording such as ‘may’ rather than ‘should’, and supply chain obligations on providers are not direct but go via their EU Member State.

Potentially, whatever reasonable definition of ‘public core of the Internet’ there may be,<sup>14</sup> it is likely that NIS2 will touch it. NIS2 includes specific requirements on DNS and TLD management. But if ‘public core’ is understood more widely by EU law to also include basic communications infrastructure,<sup>15</sup> then this also falls under NIS2 (public communications providers or telecoms and publicly available electronic communications services such as over-the-top chat services are all included). Similarly if it is understood even more widely, to include certain cloud activities such as for virtualised telecommunication services. Where ISPs play a role, the same outcome will apply,<sup>16</sup> and also where security services are included, such as trust services for two-factor authentication and e-identification. Clarification is however necessary where private networks get involved, as these are only indirectly covered by NIS2. NIS2 does not directly impose obligations on private networks but rather addresses cloud service providers and public telecommunications providers. NIS2 carved out cybersecurity from EU telecoms legislation (the European Electronic Communications Code). Private telecoms networks were always exempt from EU telecoms legislation. Public telecoms providers or cloud providers may depend in their supply chain on private networks. The NIS2 obligations on these public telecoms or cloud service providers may get translated into contractual obligations on private networks, but this is not imposed. However, precisely these private networks today form a large part of the backbone that enables the Internet as a global network of networks.<sup>17</sup> Therefore, potentially there is a challenge in this respect in terms of cybersecurity and resilience (see also the section on undersea cables below).

13 ISOC states: ‘As long as the use of DNS4EU remains voluntary, this does not pose a great risk of fragmentation. The creation of redundancies in the DNS infrastructure is not a negative development.’ See ISOC, ‘Moderating Content Can’t Be a Blunt Instrument’, *Internet Society* (2023). <https://www.internetsociety.org/resources/internet-fragmentation/dns4eu>. The DNS4EU project states that ‘To ensure net neutrality and freedom for internet users, the usage of DNS4EU is voluntary for EU citizens, and they are always free to choose a different DNS provider.’ See DNS4EU, ‘Is DNS4EU mandatory for EU citizens, and does it enable censorship by the European Commission?’ (2023). <https://www.joindns4.eu/about>.

14 See also ‘Technical Precision and Diplomatic Ambiguity’ by Olaf Kolkman in this collection.

15 The EU Cyber Act (CA) inter alia assigns tasks to ENISA, which include to support the security and resilience of the public core, which is described (in a recital) as the main Internet protocols and infrastructure, while NIS2 explicitly refers to the public core as including undersea cables. By implication it can be construed that the public core in EU law includes undersea cables.

16 Provided they are above a certain size.

17 Volker Stocker, Guenter Knieps and Christoph Dietzel, ‘The Rise and Evolution of Clouds and Private Networks – Internet Interconnection, Ecosystem Fragmentation’, SSRN Scholarly Paper ID 3910108 (2021). doi:10.2139/ssrn.3910108.

## Undersea cables: suddenly a core concern

Still, the situation on the ground develops faster than law can keep up with, notably geopolitically. This rather abruptly manifested itself when undersea cables became an issue – even if it can be argued that these were always included in the public core of the Internet.<sup>18</sup> Europe and the world were confronted with several incidents of disruption of undersea cables. In March 2024, a key cable connecting West Africa across the Atlantic was severed, with repairs taking several weeks and limited or no Internet availability in a number of countries. Before that, in February 2024, several cables in the Red Sea were damaged, possibly due to the sinking of a ship by Houthi rebels. In October 2023 a data cable and a gas pipeline in the Baltic Sea between Finland and Estonia were cut due to a ship, possibly under the Chinese flag, dragging an anchor for many kilometres across the seabed. In this incident, Finland activated the EU Hybrid Toolbox mechanism<sup>19</sup> to share information with EU partners.<sup>20</sup> In 2022 undersea cables connecting Faroe and Shetland islands were damaged, and undersea cables in the south of France were sabotaged. The high-profile underwater incident in 2022 was the destruction of the Nord Stream 1 and 2 pipelines.<sup>21</sup>

More than 60% of international traffic transits through submarine cables, which do not belong to public telecoms providers that would otherwise fall under NIS2.<sup>22</sup> Much traffic goes via the own-backbone networks of cloud/platform operators, which are unregulated private networks. These networks also reach deep into the public telecoms networks.<sup>23</sup> In the EU, countries such as Malta, Cyprus and Ireland are extremely dependent on submarine cables. In turn, these cables and their landing stations are installed and maintained by a small number of suppliers, while seafaring repair capacity is fairly limited. This creates a risk of bottlenecks and of economic insecurity in cases where foreign suppliers are not from a like-minded country.

Such points of risk for resilience are of a structural nature and consequently the European Commission envisages structural measures. These were suggested in February 2024 in the White Paper ‘How to Master Europe’s Digital Infrastructure Needs?’, for which a public consultation is currently running. The proposed interventions are given in Table 1.

Other policy papers directly relevant to submarine cables are the report on the cybersecurity and resilience of the EU communications infrastructures and networks of the NIS Cooperation Group of EU Member States (the ‘Nevers Report’), the European Commission and Council conclusions

18 See argumentation related to EU law in this paper, as well as the definition of the public core by the Global Commission on the Stability of Cyberspace: ‘[the public core includes] packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, and physical transmission media’. ‘Global Commission Proposes Definition of the Public Core of the Internet’, GCSC (2018). <https://cyberstability.org/news/global-commission-proposes-definition-of-the-public-core-of-the-internet.html>.

19 Council conclusions of 21 June 2022 on a Framework for a coordinated EU response to hybrid campaigns.

20 Finnish Government, ‘Ministerial Committee on European Union Affairs Discussed EU Hybrid Toolbox’, Valtioneuvosto, 20 October 2023. <https://valtioneuvosto.fi/en/-/10616/ministerial-committee-on-european-union-affairs-to-discuss-eu-hybrid-toolbox>.

21 See Georg Serentschy, ‘Digital Infrastructure Resilience and Security Policy Implications and Mitigation Measures’ (2024); Dennis Broeders and Arun Sukumar, ‘Core Concerns: The Need for a Governance Framework to Protect Global Internet Infrastructure’, *Policy & Internet*, vol. 16, no. 2 (2023), pp. 411–427.

22 European Commission (2014). This is actually more subtle, as the argument is not only about private networks but also about extraterritoriality. NIS2 is explicit about its extraterritorial applicability to specific service providers but its extraterritorial application to infrastructure operators such as of undersea cables in international waters does not appear to be included. See Art 26(3) in combination with Art 26(1) of the NIS2 Directive.

23 Stocker et al., ‘Rise and Evolution of Clouds and Private Networks’.

on the development of the EU’s cyber posture, and the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.<sup>24</sup> The aforementioned NIS2 obligation of EU Member States to adopt policies to sustain the cybersecurity of the public core specifies in the same sentence ‘including, where relevant, the cybersecurity of undersea communications cables’. In addition, the EU and NATO collaborated in a joint taskforce on critical infrastructures and NATO established a permanent Critical Undersea Infrastructure Coordination Cell.

Table 1. Undersea cables: EU actions

Area	Action	Hard/Soft intervention
Regulatory	NIS2, Cyber Act, Critical Entities Resilience Act <sup>25</sup>	Hard since this is EU law
Monitoring	EU-wide cable mapping and assessment (risks, vulnerabilities, dependencies)	Soft
Investment	Identifying EU and global cable projects for investment; public funding to boost private funding; state aid for strategic cable projects	Soft in general, hard for strategic cable projects by law in Connecting Europe Facility funding programme
Public procurement	Purchase cable transmission capacity for public use	Soft, as no EU mandate
Research and innovation	Leadership intention, new cable technologies	Soft as intentional, hard if in EU R&D funding programme
Incident handling	Information sharing Shared repair	Soft as EU Hybrid Toolbox; hard if shared repair facility is part of EU emergency assistance
Coordination/Cooperation	Joint EU governance of cable infrastructures	Possibly hard for risk assessment, criteria for new/upgraded cables; CPEI list; pooled funding; repair capacity
International	Best-in-class standards, Cooperation with NATO	Soft, as international cooperation. Hard if followed by EU certification

24 Respectively Council of the European Union, Council Conclusions on the Development of the European Union’s Cyber Posture (2022); NIS Cooperation Group, Report on the Cybersecurity and Resiliency of the EU Communications Infrastructures and Networks (2024).

25 See also footnote 15.

## Other policies related to critical infrastructures

Generally, where the public core involves critical infrastructures, these would fall under the Council Recommendation of 2022 on an EU-wide approach to strengthen the resilience of critical infrastructure. This non-binding joint Act of the EU Member States was triggered by the Nord Stream pipelines sabotage in 2022. Key elements of this Recommendation are enhanced preparedness, response, and international cooperation where there is cross-border relevance. EU–NATO cooperation is also included in this Recommendation.

The EU has also – over many years – been very supportive of R&D to advance the Internet and underlying communications infrastructure such as mobile communications (currently 5G and 6G, supported by the Horizon Europe funding programme). Likewise, the EU has a long tradition in international cooperation on principles, norms and values, as well as capacity-building. For instance, the EU and its Member States are very active in the UN Group of Governmental Experts (GGE) and the UN Open-Ended Working Group (OEWG), which both generally emphasise the importance of protecting the integrity, stability and security of the Internet, including its core infrastructure. The UN GGE and OEWG have managed to achieve broad agreement, albeit at a high level and non-binding.<sup>26</sup>

The EU has, also for a long time, taken a globally inclusive approach. However, since 2017, increasingly the EU engages in partnerships with like-minded countries also in public core matters. This is a consequence of rising geopoliticisation of the digital world and concerns about the EU's ability to safeguard its sovereignty. The EU seeks to increase its strategic autonomy (capability, capacities and control necessary for sovereignty<sup>27</sup>), while staying open to the world ('open strategic autonomy'). One such recent partnership initiative is the 2022 Declaration for the Future of the Internet, by 60 countries including the EU and the US,<sup>28</sup> which supports multistakeholder Internet governance and protection of the technical layer of the public core of the Internet.<sup>29</sup> This Declaration was reconfirmed by the European Commission at the 2023 Internet Governance Forum (IGF), largely reiterating earlier stated principles ('an Internet that is open, free, secure, global, reliable, inclusive and interoperable; an Internet that not only kindles innovation but also upholds democratic values and universal human rights') and rejecting attempts to fragment the Internet: an oblique reference to China's push for 'new IP'. The broader digital policy framing of the EU is the Digital Decade, towards 2030 policy.<sup>30</sup>

26 UN GGE, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (2021); UN OEWG, *Final Substantive Report of the UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security* (2021). See also Pavlina Pavlova, 'United Nations OEWG on ICT Security', *Directions* blog, 5 April 2024. <https://directionsblog.eu/united-nations-oewg-on-ict-security>.

27 Paul Timmers, 'The Technological Construction of Sovereignty', in *Perspectives on Digital Humanism*, ed. Hannes Werthner, Erich Prem, Edward A. Lee and Carlo Ghezzi (Cham: Springer, 2022), pp. 213–218; Dennis Broeders, Fabio Cristiano and Monica Kaminska, 'In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions', *Journal of Common Market Studies*, vol. 61, no. 5 (2023), pp. 1261–1280.

28 European Commission, 'Declaration for the Future of the Internet', *European Commission – Press Corner* (28 April 2023). [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_2695](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2695).

29 Respectively 'Protect and strengthen the multistakeholder system of Internet governance, including the development, deployment, and management of its main technical protocols and other related standards and protocols' and 'Refrain from undermining the technical infrastructure essential to the general availability and integrity of the Internet.'

30 European Commission, *2030 Digital Compass: The European Way for the Digital Decade*, COM/2021/118 final (2021).

## Conclusions

The EU's undersea cable infrastructure policy seems a fairly comprehensive package of measures. However, much of it is still rather soft policy. Moreover, it could be complemented by enhanced international work on undersea critical digital infrastructures, bilaterally<sup>31</sup> and also in the UN on norms for responsible state behaviour in cyberspace<sup>32</sup> as well as on international cyber-capacity building, linked to the EU's Global Gateway policy.<sup>33</sup>

It is probably fair to say that concerns about undersea cables were 'discovered' as a shock due to the series of incidents. However, this trigger should be an invitation to revisit the various layers of the public core of the Internet, and certainly the technical layer. When this is done, it is evident that there are areas of concern other than undersea cables. A concern should also be security vulnerabilities of satellite systems (think of the cyber attack on the ViaSat ground stations<sup>34</sup>). By implication, since satellite services can be disrupted, and also considering GPS-jamming and GPS-spoofing as seen at scale in Russia's war against Ukraine, there must be serious consideration of ground-based location services as an alternative or fallback to satellite-based GPS. Furthermore, cyber *and* physical security of the Internet of Things (IoT) must be taken into account. This especially holds within the telecom system, where it concerns remote monitoring, sensing and control of towers, street cabinets, routers and switches. Here both the EU NIS2 Directive and the EU Cyber Resilience Act (a Regulation) would be applicable. It does not need to be mentioned here that cloud services now also play a role for the public core of the Internet. Recently, SIDN, the Dutch ccTLD registrar, decided to migrate from its legacy software to the cloud, and proposed this to be managed by a non-EU cloud provider, AWS, in a foreign country, Canada. This led to a spotlight being turned on sovereignty requirements next to cybersecurity concerns, raising questions in the Dutch parliament.

A recommendation for a 'security X-ray' of the extended technical layer of the public core follows from the above, namely a comprehensive and coherent, whole-system and end-to-end security analysis. This also needs to address evolution of the digital infrastructure towards edge cloud, which may, for instance, increase IoT vulnerabilities yet also increase local resilience. Elements of such a comprehensive security X-ray of the public core are already being made available by the European Union Agency for Cybersecurity (ENISA), which at an early stage analysed 5G cyber-physical vulnerabilities and security of undersea cables, and recently cybersecurity of Low Earth Orbit (LEO) constellations providing telecommunications services (LEO satcom).<sup>35</sup> ENISA has also done some work on IoT cybersecurity 'good practice'.

31 See e.g. references to undersea cables and resilient connectivity in third countries in a recent declaration on Republic of Korea–EU digital partnership, in European Commission, 'EU and Republic of Korea Reaffirm Their Partnership for an Inclusive and Resilient Digital Transformation', *European Commission – Press Corner*, 26 March 2024. [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_24\\_1708](https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1708).

32 In the UN OEWG on security of and in the use of information and communications technologies ('ICT security').

33 European Commission, 'Backbone Connectivity for Digital Global Gateways', updated 23 October 2024. <https://digital-strategy.ec.europa.eu/en/activities/backbone-connectivity>.

34 Viasat, 'KA-SAT Network Cyber Attack Overview', *Viasat*, 30 March 2022. <https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview>.

35 ENISA is the EU's Cybersecurity Agency. References are respectively: ENISA, *ENISA Threat Landscape for 5G Networks Report*, 14 December 2020. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks>; ENISA, 'Undersea Cables', 31 August 2023. <https://www.enisa.europa.eu/publications/undersea-cables>; ENISA, 'Low Earth Orbit (LEO) SATCOM Cybersecurity Assessment', 15 February 2024. <https://www.enisa.europa.eu/publications/low-earth-orbit-leo-satcom-cybersecurity-assessment>.

From this short analysis of the history of EU policy on the public core (no doubt incomplete and not doing justice to all past efforts), it also appears that EU policy contains quite a number of soft actions, and that involvement in governance could to some extent be described as ‘start, stop and restart’.

Generalising from the previous analysis of the public core of the Internet, it appears that still further steps need to be taken. This leads to *a recommendation for a truly comprehensive and proactive EU policy for the public core of the Internet*. This is relevant not only for resilience of the Internet in Europe but also to increase the EU’s international legitimacy in promoting the protection of the public core of the Internet.<sup>36</sup>

It is also clear that the scope of the public core of the Internet for the EU is ever growing, in several ways. First of all, technically: we have seen this with the undersea cable challenge and suggested a number of other technical areas, from satellites to cloud. Physical security, and indeed hybrid security, comes ever more into play.

Secondly, the scope of governance is growing (the organisational view of the public core) in terms of organisations, laws and norms. Ever more organisational arrangements that involve the EU relate to the public core. Examples are trans-Atlantic cooperation and the Declaration for the Future of the Internet, as well as the EU–NATO Taskforce. Ever more EU laws relate to the public core, from the early decision to set up the domain .eu to telecoms regulation, to data protection, to cybersecurity. It is then natural to wonder what the relation will be of another major piece of legislation, the EU Artificial Intelligence Act, to the public core of the Internet? One suggestion in this respect: ICANN must evolve its fight against abuse of the global DNS and increasingly has to respond to law enforcement, while at the same time having to handle more fragmented domain name governance. It can then be anticipated that ICANN will explore AI to find vulnerabilities, detect misuse, etc. and possibly also use AI to respond to threats. This, however, will imply that it needs to assess such AI against the EU AI Act, where such AI may well land in the high-risk category of the Act. At the same time, other AI policy and regulatory frameworks are developing across the globe which ICANN will also have to comply with. In short, it may be the right time, even for just that one aspect of public core management, to engage with AI policy and regulation.

Thirdly, in the functional view on the public core an extension is also happening and already advanced. Public core management now includes all steps of cybersecurity risk management – identify–protect–detect–respond–recover – which ideally happen within common public core cybersecurity governance. The latter needs to advance and continue to evolve internationally.

Yet as regards international dialogue and response to EU policy for the public core of the Internet, it must be recognised that this is not a free-standing policy area for the EU. It is linked to larger areas of concern, notably cybersecurity, the future Internet and, as mentioned above, economic security and strategic autonomy. It is telling that the European Commission, as EU policy and law initiator, has no dedicated organisational unit for the public core of the Internet, whereas it has several organisational entities for cybersecurity or telecoms.

<sup>36</sup> As a shared position of likeminded countries, rather than a Brussels-effect-by-intent (see Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (New York: Oxford University Press, 2020); Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (New York: Oxford University Press, 2023)).

Consequently, when the EU discusses its policy on the public core of the Internet with international counterparts, it is within these large concerns. For instance, as regards cybersecurity, on the one hand many countries can find a degree of alignment in the UN settings mentioned above on high-level and non-committing norms and values for state behaviour in cyberspace. As regards the future Internet, the Declaration for the Future of the Internet also finds wide endorsement, even if many countries from the Middle East, Africa and Asia have not (yet) signed up and authoritarian states such as China and Russia will not endorse its commitments to fundamental freedoms.

In particular, over the years, the US and EU positions on the public core of the Internet have become highly aligned (e.g. the positive reception of the IANA transition and the joint Declaration on the Future of the Internet). This is despite the fact that the US retains some de jure control as ICANN remains incorporated under Californian law, and, more significantly, significant de facto control since much of the core of the Internet is provided and run by US-based large companies.

On the other hand, ultimately, international differences are large. For instance,<sup>37</sup> it is not possible to reconcile the kind of state and party control of digital infrastructures (including on the public core) of China with EU NIS2 requirements to assess digital supply chains’ security risks, including on government interference for politically adverse purposes.<sup>38</sup> From the perspective of cybersecurity and given rising geopolitical tensions, fragmentation is real and may become even worse. Concerns about strategic autonomy when US cloud providers play a major role in national domain name services in the EU have been mentioned above, although EU unease manifests itself rather in the larger context of digital strategic autonomy or digital sovereignty.<sup>39</sup>

In summary, in a paradoxical way, the EU experience is an illustration of the quest for a system-wide, society-wide and internationally wide perspective on public policy for the public core of the Internet, while the goal of an all-inclusive, global, unfragmented and peaceful Internet seems further away than ever.

<sup>37</sup> It is beyond the scope of this paper to provide a complete analysis of international responses to the EU’s position on the public core. We limit ourselves to a few examples.

<sup>38</sup> Article 22 of NIS2, of which a precursor is the common EU approach to 5G security (see European Commission, ‘Commission Recommendation (EU) 2019/534 of 26 March 2019: Cybersecurity of 5G Networks’, *Official Journal* L(88/42): 6, 26 March 2019).

<sup>39</sup> See for instance Paul Timmers, ‘Telecoms Resilience and Security’, in *The Future of European Telecommunications: In-Depth Analysis* (Brussels: CERRE, 2024), pp. 118–165, and the EU REMIT project, which investigates the relation between geopolitics, technology and multilateralism. <https://www.remit-research.eu>.



## 4. Why multistakeholderism? Ruling the Internet without multilateralism

Byoung Won Min

The emergence of the Internet has posed many issues for economic and political management systems across the world. One of them is the ruling principle of the Internet as a global commons or a public core.<sup>1</sup> The principle of multistakeholderism has become the most preferred norm in dealing with new technological standards in cyberspace. Internet Corporation for Assigned Names and Numbers (ICANN) meetings and Internet Governance Forum (IGF) conferences have taken this principle as the main framework in discussing issues in Internet governance in recent decades. It seems that the principle has become quite a good compromise in regulating the Internet as a global commons. In this sense, it seems to have become one of the significant elements in discussion of the public core of the Internet.

A challenge to this overall trend may be posed. This paper asks in a critical manner why the ICANN and IGF participants have shared the flag of multistakeholderism. Particularly, the paper looks at whether the IGF should have applied this principle, because it represents state actors and so has good reasons for supporting the principle of multilateralism rather than multistakeholderism. I think that the contrast between multilateralism and multistakeholderism reveals our trouble in endorsing principles for the Internet among countries. Since almost all states and non-state actors are interested in ruling and regulating material infrastructures and technical standards of the Internet, it becomes more and more important for us to take an overarching principle for many other public issues regarding the Internet. Multistakeholderism and multilateralism are the two of those competing principles. Is multistakeholderism more democratic than multilateralism? If not, what has made international institutions take the principle of multistakeholderism as their catchword? This paper tries to explicate the history of the principles of Internet governance in a political context and to show that these principles do not represent real-world political relations very well.

### The Internet and multistakeholderism

Multistakeholderism is currently shaping the framework for international agreements on Internet address resource issues, and has been one of the most frequently proclaimed principles for ICANN and the IGF meetings. It is a new governance model that emerged in opposition to the Anglo-American *shareholderism*, which seeks to maximise the interests of shareholders who own stakes in corporate management. Like the tradition of shareholderism, the model of multistakeholderism assumes the existential multiplicity of stakeholders within a company. So it is considered that a company aims to foster the collective interests of various actors participating in corporate activities.

1 Dennis Broeders and Arun Sukumar, 'Core Concerns: The Need for a Governance Framework to Protect Global Internet Infrastructure', *Policy and Internet*, vol. 16, no. 2 (2024), pp. 411–27.

In capitalist societies, stakeholders engage in or have interests in the business that corporations or institutions encompass. Workers and shareholders are main interest groups, but suppliers, consumers, managers and external groups are also included in the corporate activities. Governments are also included in stakeholder groups with regulatory power, as well as non-governmental organisations advocating social concerns.<sup>2</sup> In this context, external groups join business activities not only by social contracts but also with the motivation to manage externalities. While corporate activities are aimed at generating economic profits in a narrow sense, thereby enhancing the wealth of shareholders, they can also be seen as serving the broader function of supporting the entire society through *self-organised* processes. Within this organic entity, various actors interact to carry out desirable economic activities for the overall society. As such, corporations function not only to maximise the interests of shareholders but also as arenas mediating the socio-economic interactions of diverse actors.<sup>3</sup>

The notion of stakeholders assumes the relationship of *contract* within corporations. Due to the dispersed ownership structure of most large corporations, responsibility and control were delegated to managers, who tried to maximise shareholder interests as the ultimate goal of business activities. This perspective, which emphasises the functional aspects, is referred to as *functionalism*. The perspective that a corporation's value and managerial success are often reflected in its stock prices is rooted in the *efficient market hypothesis*. According to this hypothesis, the value of capital is created by providing appropriate public information, thus generating future value and building trust in contractual relationships. Functionalism and the efficient market hypothesis have formed the basis for traditional liberal market economic theories and *shareholderism*.<sup>4</sup> Since the 1980s, neoliberalism has risen in response to the perceived erosion of Keynesian economics, welfare platforms and socialist ideologies. It has advocated for a revival of classical liberal ideas around the principle of shareholderism. The interests of shareholders, rather than those of workers or subcontractors and others, have come to the fore due to the neoliberal catchphrases. On the other hand, there has been a growing backlash against and criticism of neoliberal economic philosophy.

### Multilateralism within coordinated capitalism

Considering corporations solely as actors maximising the interests of shareholders in an efficient market within a highly complex society is a very simple view. Corporations engage in much more complex activities, and there are growing concerns over this new reality. From an alternative viewpoint, attention has been drawn to the fact that corporations not only pursue the interests of shareholders but also reflect overall social and political demands.<sup>5</sup> In the process of maximising shareholders' economic interests, corporations encounter various obstacles, which implies that the role of corporations as actors goes beyond economic functions to include the social role of mediating and coordinating conflicting interests. Corporate governance should be understood not merely in economic terms but as *embedded* within a broader context of social and political communities.<sup>6</sup>

2 Norman Bowie and Meg Schneider, *Business Ethics for Dummies* (Indianapolis, IN: Wiley, 2011).

3 Edward Freeman, *Strategic Management: A Stakeholder Approach* (Boston: Pitman, 1984).

4 Gerald F. Davis, 'New Directions in Corporate Governance', *Annual Review of Sociology*, vol. 31 (2005), pp. 143–62.

5 Mark Granovetter, 'Economic Action and Social Structure: The Problem of Embeddedness', *American Journal of Sociology*, vol. 91, no. 3 (1985), pp. 481–510.

6 Davis, 'New Directions'.

The perspective that corporate activities are *embedded* within society carries implicit meanings in several aspects. When we consider the broader concept of *society* beyond the economic realm, we recognise that various actors such as organisations, governments and individuals exert influence on corporate activities. For example, labour unions apply pressure to prevent corporations from solely maximising the interests of shareholders. Governments regulate corporate activities to prevent adverse effects on the nation or society as a whole. NGOs monitor corporate ethics and service activities for consumers while complementing the roles of governments. In corporate activities, therefore, a variety of actors interact with each other so that they make an economy *embedded* in a social nexus. The basic model of corporate governance, in this context, should be redefined in this way, taking account of its roles for and relations to human factors beyond a purely economic sense. Liberal economic ideas and corporate activities today can no longer be entirely economic, but tend to be more politically and socially *embedded*.

Given the *embeddedness* of corporations within society, social demands have increased so much that a purely shareholder-centred capitalism seems no longer feasible. In particular, in terms of relationships with governments, consumers, NGOs and collaborative partners, corporate activities have reached a point where they are no longer possible without considering external entities. Multistakeholderism, rather than shareholderism, contributes to creating mutually corresponding situations by enabling corporate managers to respond to the demands of various types of participants. In the end, traditional shareholderism, in a narrow sense, reflects a governance model based only on the liberal market principle. On the other hand, multistakeholderism reflects the principle of coordinated capitalism, which considers the complex relationships among various production factors and stakeholders while adhering to the principles of liberal market order, aiming to resolve conflicts and issues among them. As a new principle of *coordinated capitalism*, multistakeholderism has exposed a tendency to expand the role and responsibility of corporations as economic, social and political actors. While it shares the goal of prioritising corporate interests with shareholderism, it differs in that it considers stakeholders more than just shareholders, so it can create comparative advantage in a complex economy of this era.

Historically, multistakeholderism has its origins in continental Europe, where corporate ownership was concentrated, which led to concentrated decision-making power being granted to a small number of shareholders. Countries such as France and Germany, recognising the harm caused by this excessive shareholder dominance over corporations' social roles, have devised institutional corrections to limit shareholders' authority. In contrast to a pure type of shareholderism, the newly conceived *multistakeholderism* and efforts to curb opportunism and power struggles among shareholders have been a characteristic feature of corporate governance in modern Europe. Economic institutionalism served as a theoretical basis to correct the shareholder-centred liberal market economic model, and *multistakeholderism* has become the guideline for institutionally implementing these motivations.

In the US, due to the frequent dispersion of corporate ownership, discussions on corporate governance structures tended to prioritise the relationship between shareholders and management over the social role of corporations. In particular, managers, acting as agents, were granted a significant degree of autonomy, and the focus was on how to protect the interests of shareholders in operating the corporation.<sup>7</sup> However, many cases of *market failure*, such as the Enron scandal

7 Martin Gelter, 'Taming or Protecting the Modern Corporation? Shareholder–Stakeholder Debates in a Comparative Light', *NYU Journal of Law and Business*, vol. 7 (2011), pp. 641–730.

in 2001, vividly demonstrated the significant pitfalls of shareholderism. These issues represented the failure of existing neoliberal economic theories to properly grasp the core of corporate governance and to understand the increasing complexity of the economy.<sup>8</sup> The emergence of multistakeholderism concerning Internet governance can be understood in this context of market principles. The US, which had dominated in setting the standards of the Internet, has also reflected these opportunities in economic principles in its future plan to govern Internet technologies.

Internet governance has long been recognised as a serious issue in the anarchic international politics, as it concerns the management of the Internet, which is to be considered a *commons*. This concept of *commons* sheds light on two aspects of Internet governance issues. One is the question of how to embrace all stakeholders from an egalitarian perspective. The other is how much tolerance should be allowed given inequality among those stakeholders. Multistakeholderism can be interpreted as a compromise between the entrenched inertia of the unequal structure highlighted in the historical context of regulated capitalism, and the new demands for equality. It can also be seen as a middle ground between individualistic pursuit of interests, characteristic of liberal freedom, and fostering collective interests represented by commons.<sup>9</sup> Therefore, multistakeholderism seems not to be an ideology that truly represents the entire Internet community.

This consideration tells us that today's multistakeholderism of Internet governance has become a *rhetoric* that excessively empowers core actors endorsed by the US government and existing Internet communities. In relation to this, Habermas has proposed important criteria for *democratic processes* through his theory of the *public sphere*, which includes stakeholders' interdependence, information sharing, mutual learning and collective problem-solving through negotiation.<sup>10</sup> However, we know this model is just an *ideal type*. In reality, many marginalised actors are excluded from governance due to the excessive asymmetry of knowledge and exclusivity of power. This includes numerous developing countries, Internet users and potential stakeholders who have yet to access Internet resources, all of whom are under the heavy influence of information big tech and great powers. While multistakeholderism aims to implement the concept of *public sphere* and pursue an idealistic goal, it still cannot fully escape the shadow of liberal pluralism, which supports traditional superpowers' *market-first* strategies.<sup>11</sup> Therefore, it falls short of becoming the principle of true *participatory democracy* for managing global commons.

In this context, we need to recognise the gap between the ideals and the realities of multistakeholderism, which has become a standard principle in today's Internet governance. It is clear that the principle should serve as the ultimate orientation in democratically addressing the issues of global commons. However, great powers like the US hesitate to translate these principles into concrete and effective action plans. In this regard, it is necessary to understand multistakeholderism as an *extension* of the logic of corporate management, which has been proposed as an alternative in response to the changing environment of capitalism, so that it can be expanded to political governance. The shift from the past shareholder-centric corporate

8 Thomas Clarke, 'Accounting for Enron: Shareholder Value and Stakeholder Interests', *Corporate Governance*, vol. 13, no. 5 (2005), pp. 598–612.

9 Rolf Weber, *Shaping Internet Governance: Regulatory Challenges* (Berlin: Springer, 2010).

10 Shawn Powers and Michael Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom* (Urbana, IL: University of Illinois Press, 2015).

11 David Edmunds and Eva Wollenberg, 'A Strategic Approach to Multistakeholder Negotiations', *Development and Change*, vol. 32, no. 2 (2001), pp. 231–53.

governance to multistakeholderism may be understood as a kind of *compromise* in the situation of increasing socio-political complexity and conflicts of interest in the market. As such, it is not surprising that the neoliberal US has emphasised the principle of multistakeholderism in governing the Internet as a *global commons*.

### Multilateralism: its state-centric approach and political delegation

The Internet, initially emerging from US technological advances, started out with characteristics of a *private good* but gradually began to be recognised as a *public good*, which has led to the establishment of the Internet governance framework. However, the most ideal form of managing public goods, known as libertarian multilateralism, has yet to be properly implemented, for various reasons. One is the structural factor of international politics, particularly the *anarchic* nature of the international system. The *strategic* approach of the US has contributed to aggravating this situation. The US government initiated its plan to establish the ICANN for delegating the authority of Internet management to an official intergovernmental organisation, thereby aiming to minimise the influence of other countries. Even when transferring the IANA (Internet Assigned Numbers Authority) functions to the ICANN, the US government tried to evade any possibility of other countries' intervention in governing the Internet. Why not an authoritative international regime or organisation for this?

Multilateralism has a long history in the modern international political system. Its origins are traced back to the Peace of Westphalia in 1648, where nations agreed to norms recognising each other as sovereign and equal entities, while accepting principles of non-intervention from outside. The *multilateral* principles in this system have remained intact and relevant until today. The universal principle of multinationalism has transformed to institutions such as the League of Nations and the United Nations, and the tradition of maintaining order and of resolving issues through agreements among European great powers. The 19th-century *Concert of Europe* and the principle of *balance of power* have laid the foundation for contemporary cooperation among major powers, such as the United Nations Security Council and the G7. This tradition of *multilateralism*, built over centuries, prioritises collaborative problem-solving among multiple countries rather than unilateral action by any specific hegemony. It is rooted in the spirit of cooperative agreements and consensus-building, forming the basis of multilateral approaches to the problem of governing global commons.<sup>12</sup>

Today, multilateralism has emerged as a significant norm in the international community under the tradition of liberalism. Major international organisations such as the United Nations embody the spirit of multilateralism and uphold it as a core principle in resolving diverse issues facing the global community. Multilateralism can also be implemented through various forms of informal mechanisms alongside institutions such as international regimes. Despite the diversity in its forms, multilateralism in international politics can be defined as 'a relationship involving cooperation among three or more countries based on principles'.<sup>13</sup> Multilateralism makes sense as an institutional mechanism for addressing global issues as it is characterised by generic norms

12 Friedrich Kratochwil, 'The Genealogy of Multilateralism: Reflections on an Organizational Form and Its Crisis', in *Multilateralism under Challenge? Power, International Order, and Structural Change*, ed. Edward Newman et al. (Tokyo: United Nations University Press, 2006).

13 John Gerard Ruggie, 'Multilateralism: The Anatomy of an Institution', in *Multilateralism Matters*, ed. John Gerard Ruggie (New York: Columbia University Press, 1993).

shaped into institutional forms, grounded on the understanding that participating countries form a community. This attribute, referred to as *indivisibility*, emphasises that the collective interests of society transcend individual national concerns. Also, it exhibits *diffuse reciprocity*, wherein all actors should benefit over the long term. This principle governs both the obligations and the rights of members.

Multilateralism and its mechanisms, which have been maintained as fundamentals of international politics, evolved into international organisations, various forms of international regimes and informal cooperation mechanisms in the 20th century. Moreover, due to imbalances in contributions among countries, multilateralism has transformed into various forms of small-scale multilateralism. However, reflecting on the US's position since the emergence of the Internet, it is difficult to observe a sufficient spirit of multilateralism being implemented. This is because, as mentioned earlier, the US has explicitly stated that it would not delegate authority over Internet address resources to international or intergovernmental organisations. If the US's stance on Internet governance is not based on formal intergovernmental multilateralism, what scenario might be envisaged regarding the transfer of related authority to the global community?

### Multilateralism and American strategy for the Internet

Criticism and reflection on the unilateralist foreign policy of the US following the 9/11 terrorist attacks have been ongoing, but discussions about the necessity of multilateralism have also persisted. The US has proclaimed the necessity of multilateralism in international relations. This perspective was rooted in a pragmatic view that multilateralism aids in managing long-term American interests and power. Therefore, even during the period of criticism of unilateral foreign policy during the 'War on Terror', efforts to pursue multilateralism continued. These efforts by the US aimed to exercise hegemonic power while also enhancing legitimacy through strategic restraint, intending to implement effective foreign policies.<sup>14</sup> Beyond the pragmatic view that sees multilateralism as a tool for specific purposes, it can also hold significant value as a procedural practice for sustaining future cooperation, essentially serving as a template for ongoing collaboration.<sup>15</sup>

In the late 2000s, the Obama administration also recognised the Internet as an indispensable infrastructure for the economic recovery of the US. Interconnected cyberspace served as a symbol of innovation and openness necessary for generating core American interests and had to be maintained flexibly and securely. Therefore, the Obama administration emphasised the need to protect the Internet space as a tool for economic growth, job creation, enhancing global competitiveness and improving quality of life. The US particularly feared excessive interference or control over the Internet space by countries such as Russia and China, and authoritarian regimes in the Middle East. The economic interests of the US had been considered to be based on principles of freedom, human rights and democracy. The Internet, as an infrastructure and a tool, was crucial for spreading these core values worldwide. Therefore, it was imperative to protect it from threats posed by authoritarian states. At least nominally, there was a sense of duty among Americans to make the Internet a space for free flow of information and political discourse.<sup>16</sup>

14 John Ikenberry, 'Is American Multilateralism in Decline?', *Perspectives on Politics*, vol. 1, no. 3 (2003), pp. 533–50.

15 Vincent Pouliot, 'Multilateralism as an End in Itself', *International Studies Perspectives*, vol. 12, no. 1 (2011), pp. 18–26.

16 Robert K. Knake, *Internet Governance in an Age of Cyber Insecurity*, Special Report 56 (New York: Council on Foreign Relations, 2010).

Historically, the US has assumed responsibility as a hegemon to provide public goods required by the international community, such as the North Atlantic Treaty Organization (NATO) for a security alliance or the Bretton Woods system for managing the international economic order. Since the decline of this hegemonic status since the 1970s, the US has maintained the international order by establishing various alternatives of global governance. However, in the case of Internet governance, the US retreated from the principle of multilateralism while emphasising that of multistakeholderism. Of course, multilateralism is most democratic when members possess equal rights. However, the US has pursued a dual-strategic approach by maintaining the pretext of global democracy while pursuing its own interests. Instead of intergovernmental organisations, the US has sought an alternative representative mechanism for global civil society, the Internet community and supranational corporations in conceptualising Internet governance, sometimes in ways where they could be overrepresented.

The ongoing controversy surrounding the democratic nature of the ICANN originated from this situation. The US government initially established the ICANN as a private entity within its own territory, but the government has authorised this entity as a kind of global multistakeholder-centric organisation. We should not ignore the fact that the US government did not use the term *multilateral* to describe the ICANN; on the other hand, the word *multistakeholderism* has been used thereafter. As we discussed above, multistakeholderism has been an economic doctrine to complement the mechanisms of a market economy. Therefore, it fails to adequately implement the core values of democracy, such as *legitimacy* and *accountability*, within the ICANN. Ultimately, the delegation of the IANA by the US government is likely to perpetuate the problem of *democratic deficit* regardless of the composition of the ICANN board.

Countries nowadays have increasingly delegated numerous functions they need to conduct to international organisations, which is natural in complex international relations. However, in protecting fundamental rights such as economic interests or human rights, it becomes more difficult for international organisations to satisfy all the demands from individual member countries. In other words, some countries may perceive themselves as relatively disadvantaged by delegating specific functions to international organisations because the level at which their domestic laws operate may not align with the jurisdiction of those organisations. When such a *jurisdictional gap* occurs, individual member countries can raise *accountability* issues regarding the functions of international organisations. In practice, these justifications are frequently utilised when great powers refuse to cooperate with multilateral international organisations.<sup>17</sup> In the realm of Internet governance as well, the principles of multilateralism in international relations have frequently been distorted by asymmetric power relations and the obstinate will of great powers.

### Great power politics and its limits

As such, multilateralism symbolises the spirit of cooperation among the global community to address its issues, but in real-world practices it faces significant constraints. Foremost among these is the *imbalance* of power among members, reflecting the intention of powerful countries to disguise power politics as democratic mechanisms. What appears on the surface to be a multilateral solution in reality often ends in the *unilateralism* of powerful countries. So it is valid to say that the mechanisms of multilateralism in international politics are still

<sup>17</sup> August Reinisch, 'Securing the Accountability of International Organizations', *Global Governance*, vol. 7, no. 2 (2001), pp. 131–49.

under the heavy influence of powerful countries, with much less consideration of smaller ones.<sup>18</sup> Therefore, it is necessary to understand international institutions not merely as symbols of cooperation but also as symbols of conflicts. The premise that international institutions will enhance the welfare of all countries and global citizens is still dubious from a realist perspective. What we observe within multilateral institutional frameworks is not so much the realisation of collective cooperation and welfare enhancement as a *distorted* form of multilateralism centred around powerful countries. Ultimately, despite diversity in historical backgrounds and objectives, various forms of international institutions serve as arenas for unequal power distribution. While multilateralism still functions as a mechanism for cooperation in contemporary international politics, the prevailing phenomenon in reality is the frequent occurrence of power imbalances and unilateralism by strong powers.

In the context of multilateralism, where the power of major countries operates asymmetrically, how do smaller or discontented countries respond? If we limit our discussion to Internet governance, in recent decades there has been a noticeable challenge to the dominance of the US, observed in a more aggressive form since the World Summit on the Information Society in 2003 and 2005. With this trend intensifying, voices demanding adherence to democratic principles and participation in international organisations have grown louder. In response, the US has, to some extent, partially accepted such demands while predominantly adopting a unilateral approach. This is evident in its determination to maintain the robustness of the ICANN system while maximising the values it prioritises and its economic interests. What enables such *go-it-alone* actions by the US despite criticism and opposition from other countries?

It can be reasonably speculated that the US is able to maintain a unilateral attitude, disregarding the spirit of multilateralism, primarily due to its overwhelming dominance in technology and national power. It should be noted that the US has the power to change the *rules* of the game. For example, let's assume that China and Russia collaborate to create a new Internet to replace the existing ICANN. Even if these countries have enough technological capabilities, the problem of path dependence remains. That is, the world is still dependent on the history of the existing Internet and will not be able to overcome its legacies soon. It is not easy to swiftly create an alternative system in responding to dissatisfaction with existing regimes. Even if it were possible, countries or forces opposing the US would likely prefer to fight within the Internet governance game rather than outside it. This is because it would be more advantageous for them to *remain* within the game, raising their voices as *internal enemies*, rather than being labelled as *external enemies* against the winning group in the game.<sup>19</sup> The fact that the disputes surrounding Internet governance have not led to extreme fragmentation of the Internet can be attributed to this strategic thinking.

<sup>18</sup> Fen Hampson, 'Deconstructing Multilateral Cooperation', in *International Cooperation*, ed. William Zartman and Saadia Touval (Cambridge: Cambridge University Press, 2010).

<sup>19</sup> Lloyd Gruber, *Ruling the World: Power Politics and the Rise of Supranational Institutions* (Princeton, NJ: Princeton University Press, 2000).

In the process of participating in global multilateralism such as Internet governance, the US has leveraged its power to achieve desired outcomes, revealing patterns of power dynamics in international relations. In international relations, power is divided into *coercive* power, which is exercised directly by actors, and *institutional* power, which is exercised indirectly. This reflects the difference in whether the target of power feels the strength of the other party directly or indirectly from the perspective of the affected subject. However, a more sophisticated exercise of power occurs at the *structural* dimension. Great powers seek to achieve their desired outcomes by changing the structure of institutions or the rules of the game. This approach focuses on influencing the structure in which the game takes place rather than limiting power to actors. In particular, it may include new actors or change the rules of interaction to indirectly reflect the great power's preferences in the institution.<sup>20</sup>

In conclusion, the mechanisms of global cooperation, including Internet governance, predominantly reflect the tradition of international organisations and multilateralism represented by intergovernmental organisations, which have strong ties to historical precedents. However, given that the Internet, as a *global commons*, inherently possesses the potential for new types of possibilities based on emerging technologies, the US has strategically sought to manage Internet governance differently. Rather than handing over the authority of managing the IANA to intergovernmental organisations, which represent the multilateral principle of international relations today, the US has pursued unconventional solutions such as the ICANN. So it must be acknowledged that the spirit of multilateralism as an alternative to multiparty stakeholders has been hampered by the US and allies' preference for multistakeholderism. Ultimately, instead of true multilateralism in international relations, an alternative liberal concept, multistakeholderism, has been adopted as a mechanism for liberal cooperation in Internet governance. However, this is merely a *modus vivendi* – a temporary solution to the shortcomings of current capitalist market economies – rather than representing the entire community.

### Conclusions: the South Korean position on multistakeholderism

The US has supported the development of the principle of multistakeholderism, but it has been the target of many challenges as the Internet could not be protected only by technological property rights. The Internet, since the early 1990s, has provided so many opportunities for states and big tech that we have to regard it as a global commons or a public core element. This implies that we need to devise a new kind of governance system for the Internet. No further application of the traditional state-centric paradigm seems to work efficiently. How can we find a better system of governing the infrastructure or the public core of the Internet? What is the right principle to underpin the Internet, between multistakeholderism and multilateralism?

The principle of multistakeholderism seems a good starter for satisfying new demands. The US government has initiated this since its establishment of the ICANN in the late 1990s. This paper asks a challenging question about the relevance of the principle for regulating the whole Internet as a global commons. In reality, multistakeholderism contradicts the conventional approach of multilateralism, which has been recognised as a standard method among equal sovereign states in international society. States, whatever ways they have emerged, represent a whole country in international society. States still hold the spirit of Westphalia in respecting and trusting other

<sup>20</sup> Michael Barnett and Raymond Duvall, 'Power in International Politics', *International Organization*, vol. 59, no. 1 (2005), pp. 39–75.

state members. On the other hand, the principle of multistakeholderism does not depend on this assumption of state agency, so diverse actors join and share their authority. So, should we take it as the fundamental principle in governing the Internet or its public core?

This paper tries to understand this incongruous situation in the field of Internet governance by illuminating the roles of the US as the leading power in Internet technology since its early stages and the current game-setter. The principle of multilateralism has not been preferred by the US, as it did not want to allow authoritarian countries to intervene in Internet governance. As such, the US did not intend to delegate the IANA to any international organisation. The ICANN, even though it was not a perfect solution, was chosen as the second-best option for the US government to reach a compromise between its political motivations and economic strategies. So the ICANN has welcomed the principle of multistakeholderism, rather than that of multilateralism, as the principal orientation in governing the Internet. This history and its political implications seem to push us to become eager for an alternative Internet governance model with more political legitimacy and economic efficiency in dealing with a new global commons.

The discussion of the limitations of the principle of multistakeholderism also reveals the same positional contradictions of the South Korean government in its approach to Internet governance. While South Korea has devised a semi-governmental institution, the Korean Internet Security Agency (KISA), which has been authorised to regulate the Internet since the early 1990s, it has taken the US position around the ICANN and the IGF for any overall principles of Internet governance. So multistakeholderism has echoes in government, civil society and academic society as the most promising model for participants in Internet governance. This seems not so much desirable as expected in terms of global interests in the public core. Considering the low development of civil consciousness and participation, the mechanism of multistakeholderism seems not be fully implemented in South Korean society. What this implies is that any policy and discussion of the Internet may follow governmental guidelines for the time being. We may have to wait for more identifiable and participatory multistakeholderism to emerge in South Korea, which is more voluntary and more independent from hegemonic influence in regulating the Internet public core.

## 5. Governing the Public Core of the Internet: A Snapshot of the Netherlands' Practices

Jan Aart Scholte and Bibi van den Berg

This paper reviews governance practices in the Netherlands vis-à-vis the public core of the Internet. The discussion proceeds in three steps. First, we briefly set out our understanding of the concept of 'the public core' as covering the underlying technical infrastructure of the Internet. Second, we describe the general approach in the Netherlands to governing the public core of the Internet as 'polycentric', meaning that processes of making and implementing rules for the public core are spread across multiple sites. This governance is *transsectoral*, in that it involves actors from both the public and the private domains, sometimes combined in so-called 'multistakeholder' arrangements. The governance is also *transscalar*, in that it involves actors with global, regional, national and local remits. Third, we highlight certain consequences of this polycentric approach to governance, both promises (such as enhanced opportunities for creative policy experimentation) and pitfalls (such as greater scope for confusion, duplication and incoherence).

### The public core

In 2015 Dennis Broeders introduced the notion of the 'public core' of the Internet.<sup>1</sup> In a report and accompanying policy brief, both written for the Netherlands Scientific Council for Government Policy (WRR), Broeders underlined that *the functioning and integrity of the Internet as an infrastructure [have become] a vital necessity for the future*.<sup>2</sup> Given the Internet's crucial importance for economy and society, its key infrastructure ought to be considered a so-called global public good.<sup>3</sup> National governments should adhere to a norm of non-intervention vis-à-vis these fundamental elements.<sup>4</sup>

The foundational infrastructure of the Internet integrates all users into a single worldwide digital communications network. Without the proper functioning of this technical layer, the Internet 'breaks'. In terms of hardware, the technical infrastructure involves devices that connect to the Internet (computers, smartphones, etc.) as well as the communication lines that connect those devices to one another (cables, routers, exchange points, satellites, broadcast transmitters). In terms of software, the technical infrastructure involves the Internet address system (particularly TCP/IP and the Domain Name System), cryptographic mechanisms, packet routing and forwarding, and other protocol parameters for the transmission of digital data between devices. For the Internet to be a mode of communication that is open to all, these technical features must be

1 Dennis Broeders, *The Public Core of the Internet: An International Agenda for Internet Governance* (WRR-Policy Brief 2) (The Hague: Netherlands Scientific Council for Government Policy, 2015); Dennis Broeders, *The Public Core of the Internet: An International Agenda for Internet Governance* (Amsterdam: Amsterdam University Press, 2015).

2 Broeders, *Public Core of the Internet*, WRR-Policy Brief 2, p. 3.

3 Broeders, *Public Core of the Internet*, Amsterdam University Press; Dennis Broeders, 'Defining the Protection of "the Public Core of the Internet" as a National Interest', *ORF Issue Brief*, 190 (2017), pp. 1–8.

4 Dennis Broeders, 'Aligning the International Protection of "the Public Core of the Internet" with State Sovereignty and National Security', *Journal of Cyber Policy*, vol. 2, no. 3 (2017), pp. 366–76.

accessible to everyone who wants to connect. Moreover, the Internet is a *global* public good, in that its user population (today numbering some 5.5 billion individuals) is spread across the planet.

The concept of 'public core' does *not* extend to data around Internet use or the content that flows through the Internet. Regarding data, it is not necessary (and in some cases not desirable) for the whole public to have access to information about users and their use of the Internet. Indeed, data protection rules generally seek to limit access to this information for reasons of privacy and safety. Likewise, it is not necessary (and in some cases not desirable) for the whole public to have access to all content on the Internet. Hence regulations may restrict access to certain digitised texts, images and sounds that flow on the Internet, for reasons of intellectual property, cultural sensitivity and political judgements.

### Polycentrism

By 'governance' we mean any and all processes for making and implementing order in society through the creation, implementation and enforcement of rules.<sup>5</sup> The question for this paper is how measures that (seek to) bring regularity and ordered adjustments to the public core of the Internet are constructed and administered (with particular reference to the Netherlands). Such regulatory activities may lie with the state, and to that extent Internet governance involves government. However, rules for the Internet can also be handled – and in practice often are handled – through private or non-state channels, and to that extent Internet 'governance' is wider than 'government'.<sup>6</sup>

As a general description of governance of the public core of the Internet in the Netherlands, we invoke the term 'polycentrism'.<sup>7</sup> This word suitably conveys the idea of 'many centres': that is, regulation spread over multiple sites. Those sites are located on different levels (local, national, regional and global) and in different sectors (public, private and mixed). The overall process of governing the public core thereby becomes quite complicated and messy. At the same time, the many actors and their interactions generally follow certain unifying norms (e.g. a commitment to technical security and stability) and practices (e.g. cycles of regular meetings).

### Multi-level public governance

Governance of the Internet's public core in the Netherlands is not centralised in one office of the state. There is no single 'Department for Internet Affairs'. Rather, government concern for the public core of the Internet is diffused across several ministries and bureaux, and is intertwined with related themes, such as digital security and cybercrime, the protection of physical infrastructures, digitisation and economic growth, and digital skills for the population.

5 Guy Hermet, Ali Kazancigil and Jean-François Prud'homme, *La Gouvernance: Un Concept et Ses Applications* (Paris: Karthala, 2005); Robbie Waters Robichau, 'The Mosaic of Governance: Creating a Picture with Definitions, Theories, and Debates', *Policy Studies Journal*, vol. 39, no. 1 (2011), pp. 113–31.

6 Lee A. Bygrave and Jon Bing (eds), *Internet Governance: Infrastructure and Institutions* (Oxford: Oxford University Press, 2009); Eric Brousseau, Meryem Marzouki and Cécile Méadel (eds), *Governance, Regulation and Powers on the Internet* (Cambridge: Cambridge University Press, 2012); Jamie Collier, 'Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom', in *Ethics and Policies for Cyber Operations*, ed. Mariarosaria Taddeo and Ludovica Glorioso (Cham: Springer, 2017), pp. 187–212; Adam Segal, 'Bridging the Cyberspace Gap: Washington and Silicon Valley', *PRISM*, vol. 7, no. 2 (2017), pp. 67–78; Roxana Radu, *Negotiating Internet Governance* (Oxford: Oxford University Press, 2019).

7 Frank Gadinger and Jan Aart Scholte (eds), *Polycentrism: How Governing Works Today* (Oxford: Oxford University Press, 2023); Carolina Aguerre, Malcolm Campbell-Verduyn and Jan Aart Scholte (eds), *Global Digital Data Governance: Polycentric Perspectives* (Abingdon: Routledge, 2024).

Various ministries have (partial) responsibilities for these themes, with the Ministry of Justice and Security (JenV) having the formal final responsibility and a coordinating task, in addition to its central role in regulatory interventions regarding digital security and cybercrime. The National Coordinator for Security and Counterterrorism (NCTV) is the main policy body within this ministry, which also houses the National Cyber Security Center (NCSC). Other important ministries are the Ministry of the Interior (BZK) (for digitisation broadly and also home to the Netherlands General Intelligence and Security Service (AIVD)), the Ministry of Infrastructure and Water Management (IenW, for the protection of physical infrastructures), and the Ministry of Economic Affairs (EZK, for digitisation and economic growth). With respect to the protection of the public core, the Ministry of Economic Affairs provides the Netherlands' representative to the Government Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN). The Ministry of Defence hosts Defence Cyber Command (DCC), handles cyber-related aspects of border control through the Military Police, and houses the Military Intelligence and Security Service (MIVD). Last but not least, the Ministry of Foreign Affairs (BZ) contributes to international cyber-diplomacy policies and practices, especially through a team of cyber diplomats led by an ambassador-at-large for security and cyber.

This overview shows that the Dutch government approaches cyberspace and its public core as a shared cross-ministerial responsibility rather than an issue that is vested in a single department.<sup>8</sup> Note, moreover, that the Dutch government has different entities for the development of policies and regulations, their implementation, and oversight functions. In practice this means that responsibilities for the public core are spread across an even larger set of government actors. Such wider entities include the Dutch Authority for Digital Infrastructure (RDI), which oversees the operations of digital infrastructures in the Netherlands, and the Netherlands Authority for Consumers and Markets (ACM), which oversees the 30 Internet service providers (ISPs) that operate in the Netherlands.

Moreover, since the Netherlands is part of the European Union (EU), many of its laws and norms concerning the protection of cyberspace are related to, if not dictated by or translated from legislation at the European level. While EU 'regulations' are legally binding for all member states (and hence take effect directly), 'directives' and 'codes' must be translated into national legislation by each government individually (and so take effect indirectly).<sup>9</sup> Examples of European measures in the digital realm that apply in the Netherlands include the EU Cyber Resilience Act (CRA)<sup>10</sup> (directly), as well as the Network and Information Systems Directive<sup>11</sup> (NIS2) and the General Data Protection Directive<sup>12</sup> (GDPR) (both indirectly). The EU also brings sector-specific regulations such as the Digital Operational Resilience Act<sup>13</sup> (DORA) targeted at the financial sector (directly),

8 Parto Mirzaei and Els De Busser, 'The New F Word: The Case of Fragmentation in Dutch Cybersecurity Governance', *Computer Law and Security Report*, vol. 55, 106032 (2024).

9 European Union, 'Types of Legislation'. [https://european-union.europa.eu/institutions-law-budget/law/types-legislation\\_en](https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en).

10 European Commission, 'EU Cyber Resilience Act'. <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>.

11 European Commission, 'Directive on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive)'. <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>.

12 European Commission, 'Data Protection in the EU'. [https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu\\_en](https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en).

13 European Insurance and Occupational Pensions Authority, 'Digital Operational Resilience Act (DORA)'. [https://www.eiopa.europa.eu/digital-operational-resilience-act-dora\\_en](https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en).

as well as the Electricity Network Code<sup>14</sup> (Netcode) for the energy sector and the Radio Equipment Directive<sup>15</sup> for the placement of radio equipment on the EU market (both indirectly). Also relevant for the Netherlands at a regional level is the Council of Europe, particularly its Budapest Convention on Cybercrime.

At the global intergovernmental level, the International Telecommunication Union (ITU) currently has only minor regulatory impact on Internet-enabled devices, Internet communication lines, Internet names and numbers and Internet protocols. An exception is the ITU's rules for radio broadcasting frequencies and satellite telecommunications. Also at the global level, the United Nations (UN) has convened a Group of Governmental Experts (GGE) and an Open-Ended Working Group (OEWG), both of which discuss general norms for Internet governance that are relevant to the Netherlands.

### *Multi-actor (semi-)public and private governance*

'Governance' also extends beyond 'government' when it comes to regulating the public core of the Internet in the Netherlands. The private sector (both profit and not-for-profit) fulfils a considerable regulatory function in this field. Examples include the Amsterdam Internet Exchange (AMS-IX), the European Internet Exchange (Euro-IX) and the global Internet Exchange Federation (IX-F). Internet address allocation (IPv4 and IPv6) is executed and regulated through RIPE NCC, which has its head office in Amsterdam. In addition, Netherlands-based professionals participate in global nongovernmental forums such as the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), the Internet Research Task Force (IRTF) and the World Wide Web Consortium (W3C), particularly through the Netherlands chapter of the Internet Society (ISOC). The Netherlands Network Operator Group (NLNOG) is a mechanism for communication and mutual learning, interlinked in turn with the Global NOG Alliance. Private firms also take a frontline role in everyday cybersecurity operations in the Netherlands.

Furthermore, in the Netherlands considerable emphasis is placed on the so-called 'multistakeholder' principle for the governance of the public core of the Internet.<sup>16</sup> In this case rules are made and administered through collaboration among participants from various functional sectors, including business, civil society, government and technical circles. The multistakeholder principle is also reflected in so-called 'public-private partnerships', which arise when government entities cannot realise their policy goals in isolation but need (and want) to collaborate with semi-public and private organisations.<sup>17</sup> There are different degrees of

14 European Commission, 'Electricity Network Codes and Guidelines'. [https://energy.ec.europa.eu/topics/markets-and-consumers/wholesale-energy-market/electricity-network-codes-and-guidelines\\_en](https://energy.ec.europa.eu/topics/markets-and-consumers/wholesale-energy-market/electricity-network-codes-and-guidelines_en).

15 European Commission, 'Radio Equipment Directive (RED)'. [https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red\\_en](https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en).

16 Jovan Kurbalija and Valentin Katrandjiev (eds), *Multistakeholder Diplomacy: Challenges and Opportunities* (Geneva: DiploFoundation, 2006); Sergei Boeke, 'National Cyber Crisis Management: Different European Approaches', *Governance*, vol. 31, no. 3 (2018), pp. 449–64; Jann Aart Scholte, *Multistakeholderism: Filling the Global Governance Gap?* (Stockholm: Global Challenges Foundation, 2020).

17 Nationaal Cyber Security Centrum (NCSC), *Cybersecurity Beeld Nederland (CSBN) 2016* (The Hague: Ministerie van Justitie en Veiligheid, 2016); Cyber Security Raad, *Integrale aanpak cyberweerbaarheid*, No. 2021-2 (The Hague: Cyber Security Raad (CSR), 2021). <https://www.cybersecurityraad.nl/binaries/cybersecurityraad/documenten/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid/CSR+Adviesrapport+%27Integrale+aanpak+cyberweerbaarheid%27.pdf>; Jorgen Schram, Henk den Uijl and Mark van Twist, *Actuele kwestie, klassieke afweging: Een verkenning naar de governance van het Nederlandse digitaliseringsbeleid* (The Hague: NSOB, 2021).

public–private collaboration. In some cases, responsibilities within public–private partnerships are more equally spread, as is the case for instance in the Dutch sectoral Information Sharing and Analysis Centers (ISACs), where government representatives share information and engage in vulnerability analyses with, inter alia, the energy, finance and health sectors. Moreover, in ICANN, actors from Dutch business, civil society, government and technical circles collectively participate, including as a former chair of the board.

In other cases, multistakeholder arrangements for the Internet in the Netherlands are nearly entirely focused on private parties, with government entities only providing funding or maintaining oversight at a distance. This happens mostly in areas where a high level of expertise encourages the government to defer to specialist semi-public and private organisations. For example, the Foundation for Internet Domain Registration (SIDN) is a semi-public organisation, which oversees the country code .nl on behalf of the Ministry of Economic Affairs. SIDN participates globally in the Country Code Names Supporting Organisation (ccNSO) at ICANN, as well as regionally at the Council of European National Top-Level Domain Registries (CENTR). The Netherlands has some 90 domain name registrars, and several hundred Internet registries offer services there. Some of these registrars and registries participate in policy development through the Generic Names Supporting Organisation (GNSO) at ICANN. In other examples of delegation to semi-public and private entities, various Netherlands-based engineers have participated in the technical advisory committees at ICANN, RSSAC and SSAC, while academics and civil society associations have participated in the At Large Advisory Committee (ALAC) and the Non-Commercial Stakeholder Group (NCSG). Finally, Dutch non-state actors are also active in the Internet Governance Forum (IGF), including the Netherlands national edition of the IGF, the European Dialogue on Internet Governance (EuroDIG), and the annual global IGF. A further multistakeholder initiative with major Netherlands input is the Global Commission for the Stability of Cyberspace (GCSC), set up in 2017 through The Hague Centre for Strategic Studies and the EastWest Institute.

Finally, it should be noted that certain parts of the public core of the Internet are not governed by institutionalised arrangements at all, but rather left to the market completely. In particular, no regulatory authority, public or private, currently oversees the laying, repair and maintenance of submarine Internet cables that serve the Netherlands. That said, disruptions to undersea cables have recently prompted increased policy attention at the EU. In addition, the North Atlantic Treaty Organization (NATO) in 2023 established a Maritime Centre for the Security of Critical Undersea Infrastructure in the UK and a Critical Undersea Infrastructure Coordination Cell at NATO headquarters in Brussels.

In sum, governance of the public core of the Internet in the Netherlands is a polycentric process that moves across scales and sectors. This complex governance is both diffuse (scattered) and fluid (constantly evolving). The many sites involved sometimes have overlapping mandates (with several actors addressing the same issues) and often have ambiguous hierarchies (so that it is unclear who has authority over whom). Polycentrism also means that there is in effect no final decision point for policy on the public core of the Internet in the Netherlands.

## Promises and pitfalls of polycentrism

Polycentrism is embraced by some and decried by others.<sup>18</sup> In practice the scorecard is mixed. This mode of governing has both positive and negative potentials. Polycentrism is not inherently more (or less) effective, more (or less) democratic, or more (or less) fair than other ways of regulating. That said, polycentrism has certain built-in promises and risks, as borne out by experiences of governing the public core of the Internet in the Netherlands.

Regarding effective policy, polycentrism with its involvement of many participants increases opportunities for rich and diverse inputs of information, insights, experiences and expertise. Multiple actors bring different data, rationalities, interests and perspectives, thereby expanding possibilities of multipronged and creative regulatory strategies. Indeed, agencies in a situation of polycentrism are often competing to invent preferred regulatory measures and frameworks. One example is the Internet Cleanup Foundation, a collective of volunteers that aims to make the Internet more secure in the Netherlands by scanning to what degree basic security measures are in place for key Dutch organisations, including municipalities, provinces, water boards, national government organisations, political parties, (higher) education institutions, the healthcare system, the financial sector and key private companies. While this initiative is run by volunteers, it works with government subsidies and has also spurred government and private actors into action to increase collaboration and regulations for improved cybersecurity.

Another potential contribution to effectiveness lies in polycentric governing's flexibility and adaptability. When many actors are pursuing many approaches – including through competition with one another – the overall regulatory system for the Internet is less likely to be rigid and stuck with a single misguided policy line. When circumstances change – including when crises arise – polycentric regimes tend to offer a range of solutions: from different ministries, from different scales, from different sectors.

One example in this regard from the Netherlands is the Cyclotron project. This government-initiated collaboration for information sharing among many private and semi-private actors seeks to improve the Netherlands' position with respect to resilience and security in/of cyberspace. Both public and private organisations often benefit by having more and better access to information on threats, vulnerabilities and incidents, yet they can be reluctant to share this information for fear of reputation damage or through a lack of trust. The Cyclotron project takes down these barriers to collaboration and creates mechanisms to foster trust. Moreover, information sharing is adjusted to fit different scales (central government, local government, large and international companies, small companies, etc.) and different maturity levels and information needs so that organisations are optimally served.

As for democracy and fairness, polycentric governing of the public core of the Internet can increase opportunities for wider and deeper participation in and deliberation on policy. More people from more sectors are involved in the policy-making process, including non-state actors and citizens. It means that, in principle, more voices can be heard and more influences can be exerted. This pattern is visible in the Netherlands in the ways that new policies, agendas and strategies for all elements of the digital realm are consistently instigated and executed through extensive

18 Gadinger and Scholte, *Polycentrism*.



stakeholder consultation with relevant experts from the private sector, from academia, from NGOs and from the local and federal government organisations. One example from the Netherlands is the creation of the National Cybersecurity Strategy (NLCS) in 2022, in which a ‘triple helix’ of public organisations, private bodies and academia collaborated closely to develop policy principles and regulatory goals for the next six years.

On the negative side, however, polycentrism can, with a multitude of actors and inputs, breed confusion, duplication, inefficiency and limited coordination in the governance of the public core of the Internet. No one has a full picture of the whole, which may lead to insufficient coordination in some areas. The lack of guidance on the goals and management of (new) submarine cables mentioned above is an example. With little government or collective direction of this infrastructure, there are risks not only of inefficiency and duplication, but also of shortages and underperformance in the (near) future.

Critics also note that, in practice, voice and influence in polycentric governing are more narrowly concentrated than the enthusiasts suggest.<sup>19</sup> Substantial and sustained impact tends to lie with small insider circles who have the greater experience and resources needed to intervene most impactfully in the policy process. This power elite in polycentric Internet governance tends to be disproportionately wealthy, male, white, middle-aged, based in the Global North and English-speaking.<sup>20</sup> To this extent polycentrism falls well short of its purported democratic qualities. One line of criticism on the aforementioned stakeholder consultation for the National Cybersecurity Strategy is that while many parties were consulted, on closer inspection large public, academic and private organisations from the geographical vicinity of the government centre of the Netherlands were overrepresented.

Next to skewed participation, the democratic potentials of polycentric governing of the public core of the Internet are undermined by weak public transparency and accountability. While the Internet deeply affects everyone in the Netherlands, most of the population (including most elected members of parliament) have little or no awareness of the complex regulatory networks that govern their online lives. Invisibility also allows the rulers of the public core to escape adequate accountability. Informal transgovernmental networks, private governance and multistakeholder mechanisms rarely answer directly to the people whom they affect. This risk became visible in the Netherlands with a citizen-initiated national referendum in 2018 regarding a revision of the law regulating the competencies, capabilities and modus operandi of the Dutch General Intelligence and Security Service (AIVD).<sup>21</sup> This law had been created in the political centre of the country, in attempted collaboration with relevant stakeholders. However, Dutch citizens railed against it for lack of transparency and fear of privacy violations. Protection of civil liberties in relation to the infrastructural core of the Internet in the Netherlands was a key part of this debate.

19 Maria Koinova, Maryam Deloffre, Frank Gadinger, Zeynep Sahin Mencutek, Jan Aart Scholte and Jens Steffek, ‘It’s Ordered Chaos: What Really Makes Polycentrism Work’, *International Studies Review*, vol. 23, no. 4 (2021), pp. 1988–2018.

20 Hortense Jongen and Jan Aarte Scholte, ‘Inequality and Legitimacy in Global Governance: An Empirical Study’, *European Journal of International Relations*, vol. 28, no. 3 (2022), pp. 667–95.

21 BBC, ‘Dutch Referendum: Spy Tapping Powers “Rejected”’, 22 March 2018, <https://www.bbc.com/news/world-europe-43496739>.

In sum, polycentrism as a mode of governing the public core of the Internet has both advantages and disadvantages in the Netherlands. To reduce confusion in the regulatory complex, one might in the future institutionalise a coordinating mechanism where delegates from the various main sites of public core governance regularly consult together. For digital security, such a mechanism already exists in the form of the Dutch Cyber Security Council, a triple-helix body of private parties, public representatives and academics that collectively advise government and the cabinet on all matters related to cybersecurity. It would be helpful to replicate this initiative for other areas of the digital agenda. Moreover, the creation of (semi-)formal network organisations could improve interconnectedness and increase communication. For digital security this process is well under way in the Netherlands. Academics are organised in ACCSS, the Academic Cyber Security Society, while Dutch cybersecurity companies,<sup>22</sup> ISPs and cloud services<sup>23</sup> and IT companies<sup>24</sup> all have their own branch organisations. Meanwhile the chief information security officers (CISOs) of a wide array of public and private organisations have collectively created the CISO platform to represent their profession. By creating such centres of gravity, more voices may be heard and more influence exerted on current and future policies and regulations, thus fortifying the strong points of a multistakeholder approach in the governance of cyberspace.

### Conclusion

This paper has described and assessed governance of the public core of the Internet in the Netherlands through the conceptual lens of polycentrism. Such a perspective helps to identify governance of this vital infrastructure as a complex process involving the interplay of many sites of regulation across scales (local to global) and sectors (public to private). The resulting institutional messiness holds both promise and perils for effective, democratic and fair governance. The challenge for all involved is to maximise the positive potentials and limit the negative possibilities.

Our paper has related the concept of polycentrism to the specific context of the Netherlands. Yet governance of the public core of the Internet also shows transscalar and transsectoral qualities in other countries across the world. Of course, the precise forms and extents of polycentrism vary from one context to another, as do the positive and negative consequences. Perhaps polycentric governing is generally more pronounced in Europe than in other world regions, but it is also present in East Asia, where Internet governance is likewise spread across multiple governmental bodies, incorporates various quasi- and nongovernmental elements, and engages a range of transnational processes. Further research can helpfully explore other contexts in greater detail, and comparative analysis may then identify larger patterns in the benefits and costs of polycentrism as a mode of governing the Internet’s public core.

22 <https://cyberveiligenederland.nl>.

23 <https://dutchcloudcommunity.nl>.

24 <https://www.nldigital.nl>.

## 6. The public core from the perspective of Internet governance

### Jung Sup Park

The Internet has become an essential part of daily life. As its importance increases, efforts at systematic management and stable operation become necessary. The Global Commission on the Stability of Cyberspace (GCSC) has indicated the importance of ensuring the stability of the public core and emphasized the need of global cooperation to maintain it. Although there may be some differences in Internet issues and related governance as discussed in Korea, it is essential to understand and develop a consensus on the concept of the public core as a vital element for Internet operation.

Governance of the public core in Korea can be examined in four areas, as follows.

1. In terms of packet routing and forwarding, major Internet service providers (ISPs) autonomously comply with it and policies based on participation of relevant stakeholders are established and operated through laws and regulations such as those of the Telecommunication Technology Association (TTA).
2. The naming and numbering system is stably operated through the Korea Internet & Security Agency (KISA) and Korea Network Information Center (KRNIC), and a governance system is established domestically and internationally through related agencies and the Internet Address Resources Act.
3. In the cryptographic mechanism field, development, verification and utilisation are carried out through the government (Ministry of Science and ICT (MSIT), National Security Agency (NSA)), specialised institutions (KISA, National Security Research Institute (NSR)) and related private expert groups. In the identity field, coordination between 23 private platforms and specialised institutions is maintained for operation.
4. In the area of physical transmission media, collaboration between the government and ISPs creates a structure where market management based on legislation and unilateral government intervention is difficult, aiming for efficient and stable network services.

Nevertheless, participation of investigative and security agencies and cooperation with overseas government agencies such as the National Institute of Standards and Technology (NIST) and international organisations such as Forum of Incident Response Security Team (FIRST) and Computer Emergency Response Team (CERT) are essential for network security and stability maintenance.

In the early days of Internet development, setting technical principles and expanding network connectivity were top priorities. However, nowadays the top priorities have changed to global

cooperation and policy development regarding information-disadvantaged groups and regions where the Internet is not connected, so that the interests of not only current but also future generations are guaranteed.

### Understanding the concept of the public core and trends in Korea

As the internet becomes a part of our everyday lives, the stability of its use is becoming increasingly important. However, interest in Internet governance is very low.

Regarding the four major areas of the public core, many experts in Korea, including KISA, are directly or indirectly conducting work related to the four areas of the public core, and those in charge of the work and key experts are also acknowledged for their consultation role. However, considering the level of technological development and the special characteristics of the region, a separate detailed redefinition is necessary, and many experts have said that Korea needs detailed coordination for each of the four areas. Table 1 explains Korea's classification of and response organisation for Internet-related issues.

Table 1. Major discussion topics in Korean internet governance and key participating international and domestic organisations

Internet address resource management	ICANN (Internet Corporation for Assigned Names and Numbers), IETF (Internet Engineering Task Force)	KISA (Korea Internet Security & Agency), KRNIC
Technical standards	ITU (International Telecommunication Union), IETF, W3C (World Wide Web Consortium), GSC (Global Standards Collaboration), ISO (International Organization for Standardization)/ IEC (International Electrotechnical Commission)	ETRI (Electronics and Telecommunications Research Institute), TTA (Telecommunication Technology Association)
Security	UN, ITU, IGF (Internet Governance Forum), COE (The Council of Europe), ICANN, OECD (Organisation for Economic Cooperation and Development), APEC (Asia-Pacific Economic Cooperation), APCERT (Asia-Pacific Computer Emergency Response Team), AVAR (Asia-Pacific Association of Anti-Virus Asia Researchers)	KISA (KISC, KRNIC), National Intelligence Service (NIS), Ministry of the Interior and Safety, Ministry of National Defense, National Police Agency, etc.

Table 1. Continued

<b>Intellectual property rights protection</b>	WIPO (World Intellectual Property Organization), UNESCO (United Nations Educational, Scientific and Cultural Organization), UNCTAD (United Nations Conference on Trade and Development), US Private Organisations (IPC (Inter-Process Communication) & IIPA (International Intellectual Property Alliance), CIC (Creative Incentive Coalition), DFC (Digital Future Coalition)	KISA Internet Address Dispute Resolution Committee, Korea Copyright Commission, Copyright Registration Management Organization, NIS (National Intelligence Service)
<b>Personal information protection</b>	OECD, UN (United Nations), EU (European Union), APEC	Personal Information Protection Commission, Korea Association for Information, Protection
<b>Content regulation</b>	OECD-ICCP (The Information and Communication Policy Committee of OECD), UNESCO, INHOPE (International Association of Internet Hotlines)	Broadcasting and Telecommunications, Review Committee

In summary, the definitions and key stakeholders or participants in the four areas of the public core are as shown in Table 2. Specific governance structures according to relevant legal systems, in addition to the participants, will be examined in detail in the following section.

Table 2. Key stakeholders and participants in the four areas of the public core

Area	Contents	Management and Implementing Agency
<b>Packet routing and forwarding</b>	<ul style="list-style-type: none"> <li>A series of processes and technologies that determine the path of data packets and transmit them to their destinations.</li> <li>Routing, BGP (Border Gateway Protocol), etc.</li> </ul>	<ul style="list-style-type: none"> <li>ISPs</li> <li>KISA</li> <li>MSIT</li> </ul>
<b>Naming and numbering systems</b>	<ul style="list-style-type: none"> <li>Systems responsible for the unique identification of resources such as domain names (DNS), IP addresses/AS numbers used on the Internet.</li> <li>Domain registration management, IP address/AS number allocation management, public DNS.</li> </ul>	<ul style="list-style-type: none"> <li>KISA</li> <li>ISPs</li> <li>Domain registration agents</li> <li>MSIT</li> </ul>

Table 2. Continued

<b>Cryptographic mechanisms of security and identity</b>	<ul style="list-style-type: none"> <li>Technologies related to encryption, identification systems, and ensuring the confidentiality, integrity, and authentication of data.</li> <li>SSL/TLS, Resource Public Key Infrastructure (RPKI), etc.</li> </ul>	<ul style="list-style-type: none"> <li>KISA</li> <li>Telecommunications Technology Association (TTA)</li> <li>Electronics and Telecommunications Research Institute (ETRI)</li> <li>MSIT</li> <li>NSR</li> <li>NSA</li> </ul>
<b>Physical transmission media</b>	<ul style="list-style-type: none"> <li>Physical wired and wireless media used for data transmission.</li> <li>Fibre optic cables, wireless communication technologies, scientific research networks, etc.</li> </ul>	<ul style="list-style-type: none"> <li>ISPs</li> <li>MSIT</li> <li>National Security Agency(NSA)</li> <li>Korea Institute of Science and Technology Information (KISTI)</li> <li>National Information Society Agency (NIA)</li> </ul>

In Korea, the management organisation for ccTLDs (country code top-level domains) is KISA, specifically through its department known as KRNIC. The actual operation of KRNIC began when the Network Information Center (NIC) in the United States registered the .kr domain area in the root domain name system (DNS) in 1990. With increasing demand for registration, KRNIC was established within the Korea Advanced Institute of Science and Technology (KAIST) in 1993 to standardise and manage Internet addresses domestically.

In July 1991, under the leadership of Professor Jeon Gil-Nam, the Academic Network Council (ANC) was formed to coordinate domestic academic and research network activities. It served as a coordinating body with committees and technical working groups, playing a crucial role in early Internet governance in Korea. Subsequently, with the enactment of the Internet Address Act in 2004, the management of Internet address resources was institutionalised according to legal regulations (see Table 3).

Table 3. Changes in Internet address resource-based governance in Korea

Management Organisation	1986–1983 KAIST	1994–1998 NCA	1999–2003 KRNIC	2004–2008 NIDA	2009–2011, 2012– KISA
<b>Policy making</b>	KAIST	1991–1996 ANC	1997–1998 Internet Council (KRIA)	Name and Number Committee (NNC)	Internet Address Policy Committee
<b>Policy discussion</b>				Internet Address Policy Working Group	Internet Development Council KIGA

## Current status of governance in Korea based on the concept of the public core

### Governance related to packet routing and forwarding in Korea

In Korea, the sector of packet routing and forwarding adheres to standards through major telecommunications companies such as KT (Korea Telecom), SKB (SK Broadband), LG U+ and 90 small and medium-sized ISPs. To promote cooperation and mutual understanding among these ISPs, the Korea Internet Service Provider Association (KISPA) was established in 2000. KISPA focuses on market cooperation and policy discussions aimed at enhancing the quality of Internet services and fostering fair competition in the related market.

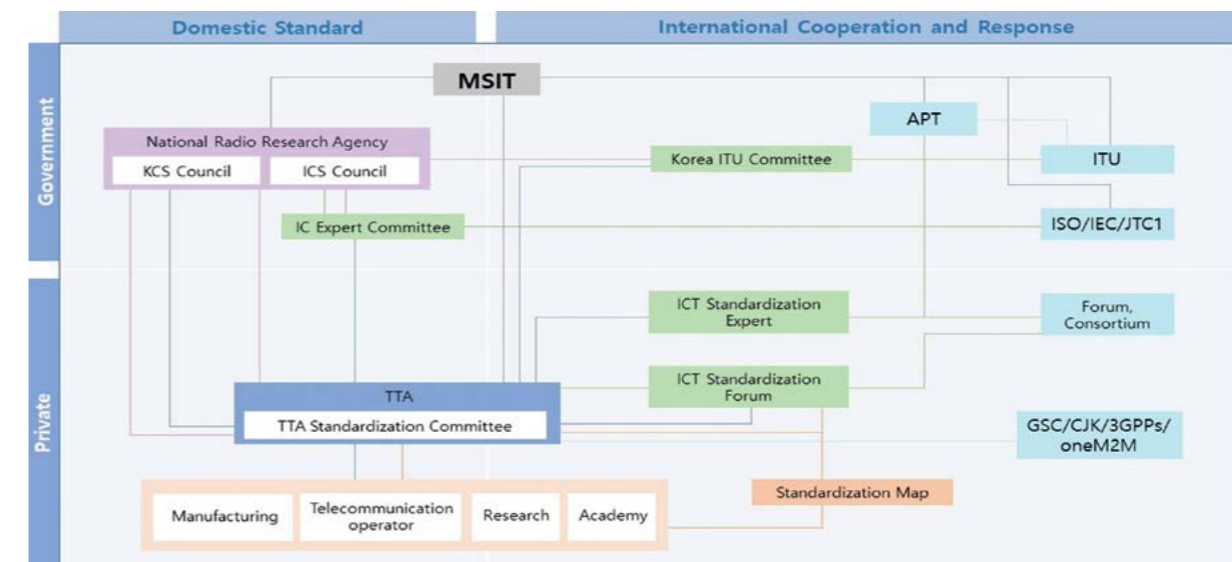
As in other countries, as the influence of the Internet on people's lives and the national economy grows, the government in Korea ensures stable provision and operation of Internet-related infrastructure and services through legislation and supervision. Under the MSIT and the Telecommunications Business Act, the financial status, technical qualifications and policies for the protection of citizens or users of these operators are reviewed and supervised. Measures are taken not only for the registration and qualification of operators but also to minimise confusion and user harm during outages, and to supervise various fair competition issues.

Standards related to packet routing and forwarding, as well as other protocols, products and service standards, evolve alongside technological advancements and the introduction of new services. It is natural that new technologies and services may bring unforeseen side-effects or issues. If vulnerabilities are discovered, specialised research, development and incident response analysis are conducted to review new standards. International standardisation efforts related to Internet standards and protocols are carried out through organisations such as the Internet Engineering Task Force (IETF) or ITU-T. Initially, during the early days of the Internet, the IETF, supported by the technical community Internet Society (ISOC), played a central role.

Standards for products and services in Korea's Internet and information communication sector are established through the Telecommunications Technology Association (TTA). TTA's standardisation process involves various stages – proposal, drafting, gathering feedback, deliberation/adoption, issuance/revision of existing standards – all of which are conducted based on the participation of relevant industries, research institutions and academia. These stakeholders participate as members of various organisations such as the TTA Standardization Committee, ICT Standardization Forum, ICT International Standardization Expert Group and Korea ITU Research Committee. As of March 2024, TTA was operating a pool of over 250 experts who engage in domestic and international activities, supported by the organisation.

For the development and application of standards in the domestic public and government sectors, oversight is provided by the national Radio Research Agency (RRA), a subsidiary of the MSIT established on 19 August 2011. To gain a comprehensive understanding of Korea's standardisation system, please refer to Figure 1.

Figure 1. The standardisation system in Korea's Internet and information communication sector



(KCS) Korea Communications Standard; (ICS) Internet Computing Service; (IC) Internet Computing; (JTC1) Joint Technical Committee; (GSC) Global Standards Collaboration; (CJK) China, Japan, Korea; (3GPPs) Third Generation Partnership Project; (oneM2M) One Machine to Machine.

Given that KISA is responsible for the allocation and management of Internet address resources and the stable operation of DNS, it can be considered a major participant in the field of packet routing and forwarding. In particular, recent emphasis on the adoption of RPKI and the strengthening of BGP monitoring at the national level has led to enhanced collaboration with ISPs.

### Governance related to the naming and numbering system in Korea

In the field of naming and numbering systems, KISA, which performs the function of KRNIC, fulfils a pivotal role in South Korea. Specifically, KISA serves as the National Internet Registry (NIR) in cooperation with APNIC (Asia-Pacific Network Information Centre), one of the five Regional Internet Registries (RIRs) worldwide. Under KISA's management, three major ISPs and over 900 other management agencies receive IP address allocations for network operations. Additionally, around 100 independent users manage their IP address allocations.

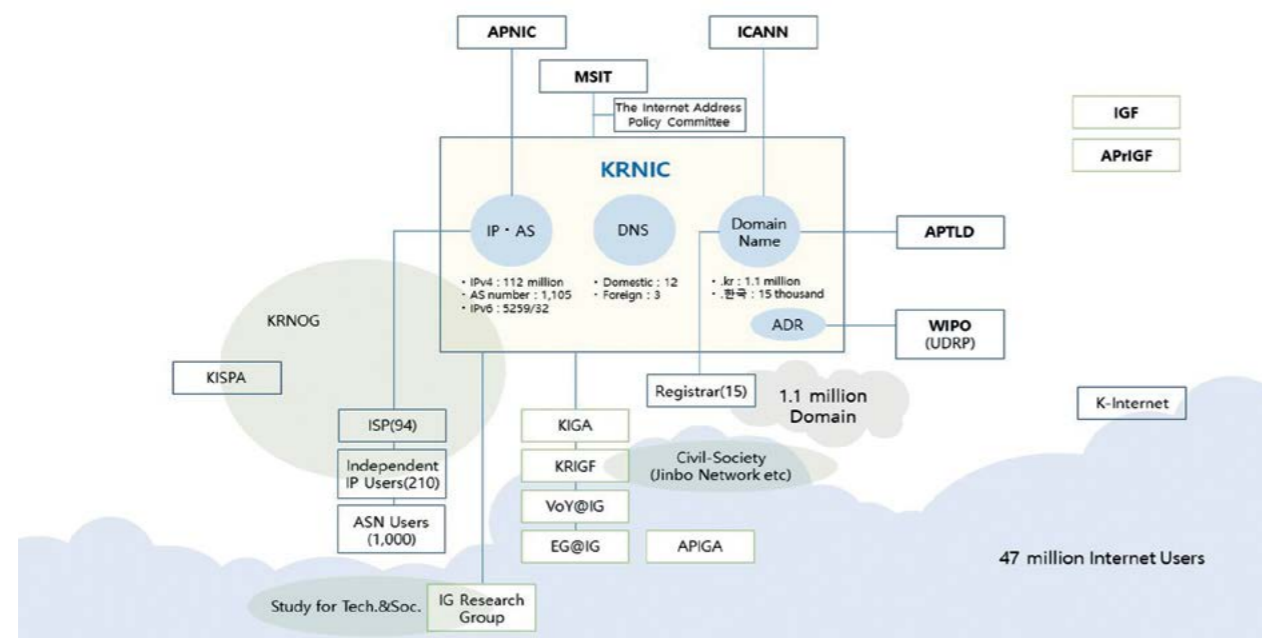
As of December 2023, TTA oversaw seven technical committees, each focusing on specific areas of expertise, with a total of 58 project groups. These committees and project groups facilitate collaboration among industry experts, academia and researchers to develop and maintain standards in various ICT domains.

South Korea holds approximately 112.5 million IPv4 addresses, ranking sixth globally in IPv4 address holdings. As of March 2024, over 1,050 AS (Autonomous System) numbers were allocated and operational, and approximately  $5,276 \times 296$  IPv6 addresses were secured. KISA also operates the domain name registration management system and the national top-level DNS servers. The national DNS is mirrored in 12 domestic locations and three overseas locations (Brazil, Germany, China). After the onset of the COVID-19 pandemic, it was processing approximately 2.3 billion queries per day, with the volume increasing annually. From the end of 2022, it was handling an average of around 3.5 billion queries per day, and recently it has reached up to 8.8 billion queries per day.

The increase in query volume is attributed to a significant rise in malicious queries targeting government agencies and public domains related to South Korea's parliamentary elections. Given the ceasefire situation with North Korea and adversarial relationships with China, Russia, Japan and the United States, there is a recognition among both the public and the government of the potential for various attacks and intrusions via the Internet at any time. Despite these challenges, there is a consensus on the need to advance Internet and digitalisation efforts. To ensure a stable Internet environment, efforts are being made to upgrade relevant equipment and facilities. Additionally, measures such as RPKI implementation and BGP monitoring are being actively pursued.

Furthermore, KISA oversees the registration and management of .kr and .한국 domains through accredited registrars, totalling 15 companies. Currently, approximately 1.1 million .kr and .한국 domains are in use, with an estimated 3 million additional domains under gTLDs such as .com, .net, .org and .edu likely registered and utilised by Korean entities. Given the increasing cybersecurity threats and the government's push for digital transformation through initiatives such as the Digital Platform Government, South Korea is actively considering the adoption of public DNS services to ensure the stability and security of critical infrastructure. Similarly to countries such as the UK and the US, South Korea aims to enhance the management and monitoring of DNS services for government, local authorities, public institutions, financial institutions and educational organisations (Figure 2).

Figure 2. Overview of governance in South Korea regarding the naming and numbering system



(KRNOC) Korea Network Operators' Group; (KISPA) Korea Internet Service Promotion Association; (ASN) Autonomous Server Number; (KIGA) Korea Internet Governance Alliance; (VoY@IG) Voice of Youth at Internet Governance; (EG@IG) Expert Group at Internet Governance; (ADR) Alternative Dispute Resolution; (APTLTD) Asia-Pacific Top Level Domain Association.

KRNIC, operated by KISA, not only manages Internet resources but also shows interest in understanding and addressing changes and international issues related to Internet governance. To enhance awareness and participation among Internet-related companies, academic and research communities and general users, KRNIC is considering programmes such as VoY@IG (Voice of Youth at Internet Governance) and EG@IG (Expert Group at Internet Governance). Additionally, it collaborates with the academic community, including six universities in South Korea, to develop and operate mentoring-based programmes aimed at enhancing the next generation's Internet governance capabilities.

Furthermore, KRNIC cooperates with organisations such as ICANN, APNIC, ISOC and DotAsia to run the Asia Pacific Internet Governance Academy (APIGA). APIGA offers specialised Internet governance education, primarily attended by students from the Asia-Pacific region and particularly targeting youth, to help people understand the origins and history of the Internet, grasp concepts like the multistakeholder model and learn about Internet standards and policy-making processes. Around 350 individuals have received education on Internet governance through APIGA since 2016. Some Korean participants continue their engagement by staying updated on developments in their areas of interest through EG@IG and receiving mentoring from experts (professors). They also present their research and ideas at events like the Korea Internet Governance Forum (KrIGF) and Asia Pacific Internet Governance Forum (APrIGF), with three teams in 2022 and five in 2023 presenting at APrIGF.

#### Governance related to cryptographic mechanisms of security and identity in Korea

##### Development and activation of cryptographic modules

In the interconnected Internet where information and services are exchanged at the speed of light, it is crucial to have clear identification of senders and receivers, as well as the ability to verify information between identified and qualified senders and receivers. In Korea, various laws and administrative systems, such as the Basic Act on Intelligent Information Society, the Act on Promotion of Information and Communications Network Utilization and Information Protection, the Electronic Government Act and the Cyber Security Work Regulation, are used to verify the security of cryptography. Through these measures, efforts are made to develop cryptographic algorithms used by the public and private sectors and to establish a secure usage infrastructure to protect data and services distributed and stored on the Internet.

In the sector of security and identity encryption mechanisms, roles are divided into the development and generation of encryption and supporting and verifying its practical application in the market or field. The aspect of developing, generating and managing encryption is handled by the National Intelligence Service (NIS) and the National Security Research Institute (NSR) under the jurisdiction of the Electronic and Telecommunication Research Institute (ETRI), and inspection of encryption mechanisms is carried out by the MSIT and KISA (Table 4).

Table 4. The cooperative system related to the development and promotion of encryption algorithms

	MSIT, KISA	NIS, NSR
Tasks	Activation of secure encryption usage and expansion of encryption technology applications	<ul style="list-style-type: none"> <li>• Operation of the Cryptographic Technology Safety Verification (KCMV) system</li> <li>• Development of domestic encryption algorithms such as post-quantum cryptography</li> </ul>
Scope	Private sector	Public critical infrastructure
Roles	<ul style="list-style-type: none"> <li>• Testing and evaluation of encryption modules, countermeasures against cryptographic technology misuse such as ransomware and quantum computing</li> <li>• Survey of encryption usage practice</li> </ul>	<ul style="list-style-type: none"> <li>• Operation of encryption module verification and evaluation systems</li> <li>• Development of domestic encryption algorithms such as post-quantum cryptography</li> <li>• Response to the revision of domestic encryption standards</li> </ul>

As various new Internet services such as big data and Internet of Things (IoT) are being developed and disseminated, there is an urgent need for the development and dissemination of cryptographic technology that can effectively respond to potential new security threats. Furthermore, with the significant increase in computer processing speeds and the advent of the quantum computing era, current cryptographic algorithms are very vulnerable. In such a situation of hyperconnectivity and the advent of super quantum computing, the importance of the development, systematic management and utilisation of encryption cannot be overstated.

In Korea, national public institutions are required to utilise verified cryptographic modules, and even private enterprises are encouraged to use these modules. For national public institutions, it is mandatory to install only verified cryptographic modules for database encryption, single sign-on authentication, document encryption (Digital Rights Management), virtual private networks (VPNs), software security, secure USB and others.

The major cryptographic technologies both domestically and internationally are standardised by organisations such as ISO/IEC and IETF. These standards are applied across various industries where digital and Internet technologies are utilised, including networks, terminals, services and products. Symmetric key cryptography, hash functions, digital signatures and other cryptographic methods developed domestically are internationally recognised and applied for interoperability across different systems.

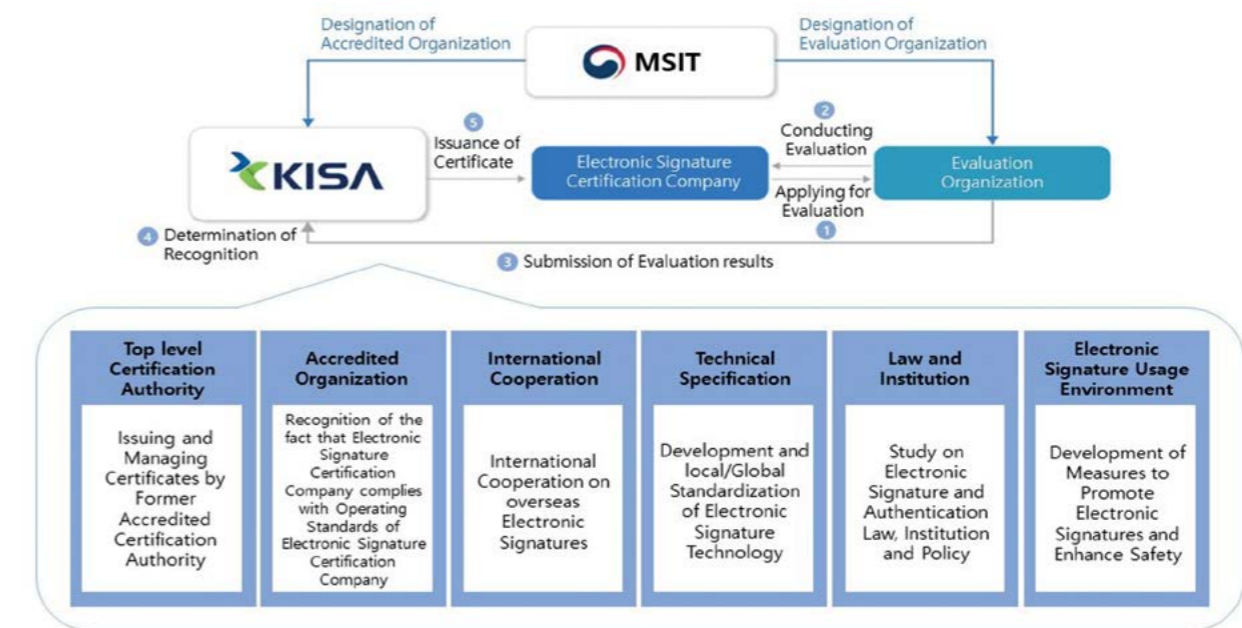
*User authentication based on electronic signatures*

With the proliferation of Internet usage and the advancement of digital technology, digital transformation has become a pervasive challenge in most countries. Many offline transactions, such as document verification and contract exchanges, have been digitised through the Internet, increasing the need to verify authenticity or identity, much like signatures or seals. Consequently, there is a growing demand for systems that are tamper-proof and can prove one’s identity.

In response, Korea has introduced and implemented an evaluation and certification system to enhance the reliability of electronic signatures. Based on the Electronic Signature Act, the MSIT plays a leading role, while KISA serves as the top certification authority and accrediting body. The MSIT establishes a separate professional evaluation organisation to assess and evaluate the qualifications of institutions or companies wishing to become electronic signature certification authorities. However, the final determination of qualification recognition is made by KISA, the accrediting body.

As of March 2024, there are four evaluation organisations: TTA, Korea Financial Security Institute, Deloitte Anjin Accounting Corporation and Samjeong Accounting Corporation. Additionally, 23 electronic signature certification authorities are recognised to conduct business (see Figure 3).

Figure 3. Recognition and evaluation system for electronic signatures



*Governance related to physical transmission media in Korea*

In South Korea, physical transmission media, including cables and wireless base stations used for broadcasting, telecommunications and electricity transmission, are operated or leased by various private or public companies to conduct business. These services have a significant impact on public welfare in the digital age and the national economy, thus they are subject to various obligations and responsibilities under different laws. Under the Telecommunications Business Act, these services are categorised based on whether they involve the installation of circuit facilities, such as telecommunications lines.

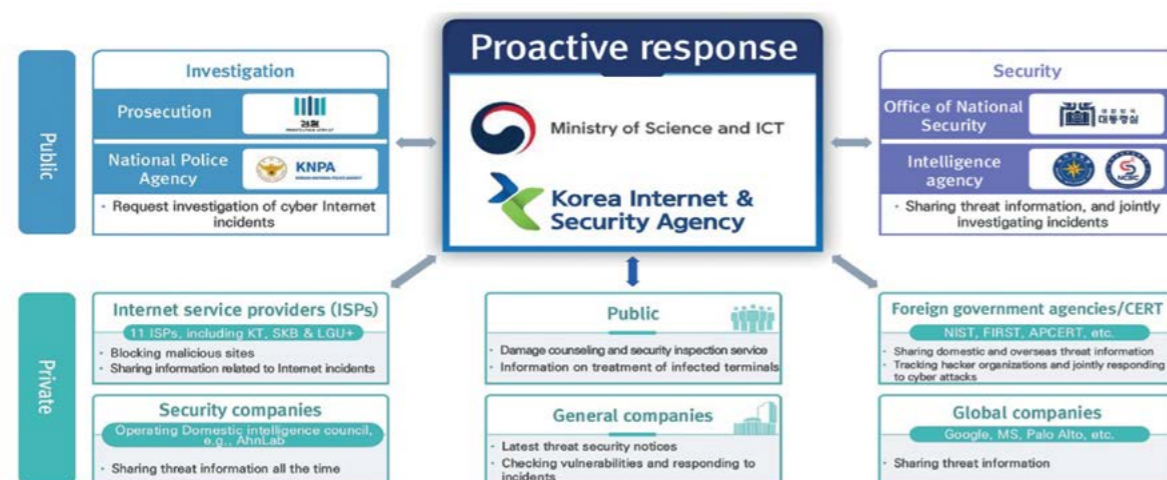
Telecommunications businesses that install and operate circuit facilities encompassing exchange equipment and lines to provide telecommunication services are referred to as telecommunications carriers. Entities wishing to operate telecommunications carriers must register with the MSIT, meeting requirements such as financial and technical capabilities, user protection plans and registration criteria outlined in the Enforcement Decree of the Telecommunications Business Act.

As of January 2024, Korea Electric Power Corporation (KEPCO) obtained the status of a telecommunications carrier by submitting an operational plan for electrical facilities and related communication facilities. There are over 90 registered telecommunications carriers in South Korea. Additionally, there are ‘specific telecommunications businesses’, which provide information communication services in specific areas or for specific services using the circuit facilities of telecommunications carriers, and ‘value-added telecommunications service providers’, which operate businesses such as portals, content, e-commerce and hosting by leasing circuit facilities from telecommunications carriers.

South Korea has over 1,000 network service providers, including over 90 telecommunications carriers, interconnected through four Internet Exchange Points (IXPs). Furthermore, the country is connected to overseas networks via submarine cables, including those linking Japan, China and other regions.

As mentioned in the section on packet routing and forwarding governance in Korea, the network is operated through various operators, including 90 ISPs such as KT (Korea Telecom), SKB (SK Broadband), LG U+ and over 1,000 operators allocated with IP addresses and AS numbers. Also, efforts have been made to secure new Internet address resources such as IPv6, in addition to implementing RPKI and BGP monitoring for stable operation and management of these networks. Furthermore, at the national level, a system has been established to differentiate between public and private sectors for network security and to respond to various network intrusions and threats, from identifying causes to responding and assessing security situations in case of incidents. Given the ongoing state of tension in the country, it is crucial to clearly identify whether network intrusions are caused by hostile forces. However, the main focus remains on ensuring the safe operation of the Internet, preventing network intrusions, minimising damage in the event of incidents and preventing their spread (see Figure 4).

Figure 4. Korea’s Internet incident response system



Korea has established separate governance to secure the stability of critical infrastructure and its ICT, providing essential services in areas such as administration, telecommunications, finance and energy. As these critical infrastructures are digitised using the Internet and ICT, they are susceptible to electronic intrusions, which can not only inconvenience citizens but also affect national security. Similar to other response systems, governance is established through legislation.

Under the Information and Communication Infrastructure Protection Act, ‘major information and communication infrastructure’ is designated, taking account of factors such as national and societal importance, reliance on information and communication, interconnectivity with other facilities, expected scale of damage in the event of intrusion, likelihood of intrusion occurrence, and ease of recovery in the event of an intrusion. Facility designation is carried out through the Information and Communication Infrastructure Protection Committee established under the Prime Minister’s Office, with participation from relevant agencies and private experts. Operations in the private sector are centred on the MSIT, while those in the national and public sectors are centred on the National Intelligence Service.

Once something is designated as a major information and communication infrastructure, vulnerability analysis must be conducted annually and, based on the results, protective measures must be formulated and submitted to the Information and Communication Infrastructure Protection Committee. Various organisations such as KISA, National Security Research Institute and other specialised information security service companies support these activities. As of January 2024, a total of 439 institutions and facilities had been designated as major information and communication infrastructure and were being managed accordingly.

### Governance of the public core in Korea and implications

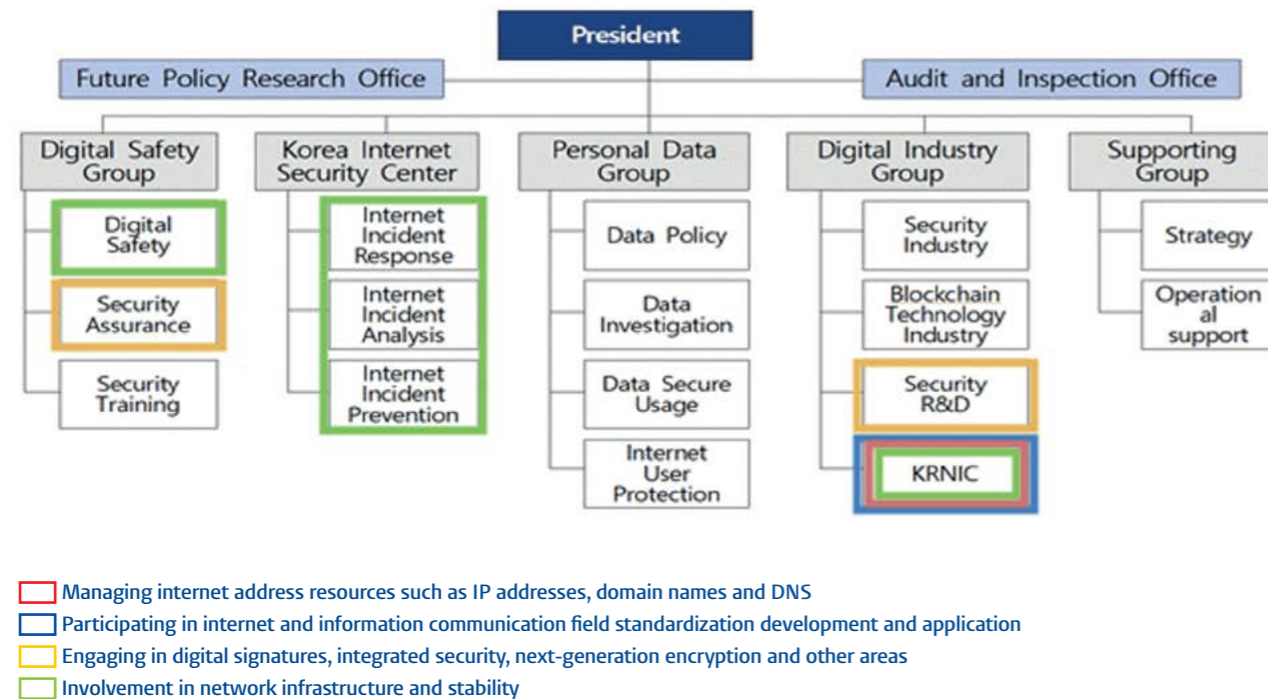
#### Establishment of Internet governance in Korea based on legislation

Korea, following the United States, is the second country to successfully establish Internet connectivity, rapidly adapting to and transitioning into the digital realm. Citizens, businesses and the government all exhibit a high level of interest in the stable operation of the Internet. Similarly to how democratically oriented societies manage public interests and common concerns through laws based on social consensus, Korea formulates legislation through gathering opinions and engaging in public discourse from various stakeholders on a case-by-case basis. Through this process, the objectives and governance of managing specific issues are established, and various procedures and oversight mechanisms are put in place.

In addition to legislation, specialised institutions are established and operated to ensure the effectiveness of the relevant laws. As previously mentioned, government agencies such as the MSIT, responsible for the jurisdiction of the laws, exist, and specialised institutions such as TTA, NIA and KISA are established and operational for the performance of related tasks. KISA, for example, encompasses departments responsible for managing Internet address resources such as IP addresses, domain names and DNS; participating in Internet and information communication field standardisation development and application; engaging in digital signatures, integrated security, next-generation encryption and other areas; and involvement in network infrastructure and stability (Figure 5). Virtually all departments are directly or indirectly interconnected. Furthermore, MSIT and KISA maintain close networks with the research community, academia and industry throughout the process of performing

these tasks and have established governance mechanisms to gather domestic and international policy trends and the opinions of Korean users through various institutional arrangements such as the Internet Address Policy Committee, the Information and Communication Standards Committee and the Information and Communication Infrastructure Protection Committee.

Figure 5. Organisational chart of KISA



In essence, a clear governance system has been established by law for the management of the Internet’s major infrastructure, particularly in the public core sector, significantly reducing the potential for government interference or unreasonable demands from specific individuals. Moreover, relevant stakeholders such as experts, users, policy makers and related industries are actively involved and their participation is systematised.

### Challenges for future research

As Internet usage becomes more widespread and digital transformation becomes a global priority, it is undeniable that the importance of the public core and the need to prevent unnecessary state intervention are paramount. However, there is a need to prepare contingency plans for situations where inevitable interventions may occur, leading to Internet disruption or disconnection in specific regions or countries. Such fragmentation, disruption or intentional infringements cannot be allowed to persist indefinitely, necessitating short-term coping mechanisms for such situations. These challenges are largely technical in nature, thus requiring technological solutions. These technical solutions need to be developed at various levels, including individual, corporate, critical infrastructure, national and global.

However, there seems to be controversy over whether a single-organisation-centric deliberative system, such as ICANN or the UN, based on the existing multistakeholder model would be efficient. The question arises as to whether the participation of stakeholders, who may be excluded due to the technology-intensive nature of Internet and ICT discussions, and the preservation of their interests can be ensured: for example, whether the interests of information-marginalised groups or communities and countries with slower technological advancement can be safeguarded within the current multistakeholder model.

Except for global Internet companies, few companies are directly interested in discussing Internet governance in the international arena, such as ICANN and IGF. The same is true of Korean companies such as Samsung, Hyundai, Naver and Kakao. This reality can be extended to individual users, civic groups and researchers. There seems to be room for the government to think about the advantages of multilateralism representing individuals, companies and regions.



## 7. Protecting the public core of the Internet: the Netherlands' security perspective

Paul A.L. Ducheine and Peter B.M.J. Pijpers

Within the human-made digital universe, defined as the full space characterised by three dimensions – processing power, storage capability and transmission speed – a conceptual space, i.e. cyberspace, was created that is functional for the communication of data and information.<sup>1</sup> This conceptual space defined as cyberspace comprises a virtual and a physical dimension. Virtual personas (identities) provide access to virtual objects (such as software and data) using hardware for storage, computations, communication, etc.<sup>2</sup> The communication infrastructure – both physical and digital – that connects the separate parts of cyberspace is referred to as 'the Internet'.

This brief paper deals with the protection of the public core of the Internet (and thus of cyberspace). It summarises the Netherlands' view on the security aspects of (including threats to) the public core of the Internet/cyberspace, describes the military aspects of the public core, and outlines the utility of international law in protecting it.

### Introduction

The inception of cyberspace has created numerous opportunities, and the days of cumbersome dissemination of information via pamphlets or radio broadcasts are over. The virtues of digitisation and social media are plentiful for financial and economic institutions, to find old friends and acquire new like-minded peers all around the globe. The speed and degree of penetration into societies combined with the low cost of entry provide opportunities not only in the commercial or societal realm but also for the political system to enhance free expression and access to information and to reach out to potential voters. Cyberspace, including the Internet, has become indispensable for individuals, organisations, companies and states: - at least, for those that are connected to the Internet.<sup>3</sup>

To emphasise the importance of cyberspace, in 1996, Barlow even issued a declaration of its independence,<sup>4</sup> arguing that cyberspace should not fall under the sovereignty of any state but would have a jurisdiction of its own. States but also academics swiftly argued that this notion was flawed since several aspects of cyberspace, including the hardware (computers, routers, cables, etc.) will always be situated within the sovereign territory of a state and data will be subject to intellectual property rights. Along its many merits, cyberspace could be used for malign purposes, raising the question of how to protect not only the elements of cyberspace but also people's use of it.

Cyberspace occasionally proves ill-fitted for existing conventions, including international law. While the ICT infrastructure, the hardware and software, entails tangible objects that naturally fall under the territorial aegis of a state, data (including protocols) and virtual personas (e.g. our virtual identity and representation) do not. Moreover, the bulk of cyberspace is owned by private actors, and while states are the main security actors in the physical world, they are not in cyberspace. Some of these private actors, e.g. the Magnificent Seven<sup>5</sup> and their CEOs, have access to instruments of powers that match, or even surpass, that of states.<sup>6</sup> These actors and the infrastructure they own sometimes play essential roles in the functional space, a fact that becomes perceptible once services are not available during Internet outages.<sup>7</sup>

Given the salience of the Internet and people's dependence on digital interconnectivity,<sup>8</sup> especially in states high on the Digital Economy and Social Index,<sup>9</sup> states are called upon not to interfere with the public core of the Internet and to apply a regime of restraint and diligence against serious attacks to the publicly accessible and neutral public core, as reflected in the conclusions of the final reports of the 2015 UN Group of Governmental Experts (GGE) and 2021 Open-Ended Working Group (OEWG).<sup>10</sup>

In this brief paper we aim to elaborate on the Netherlands' view of the public core of the Internet (and hence of cyberspace), especially from a security perspective. How are the vital aspects of cyberspace assessed, what are the threats to and vulnerability of the public core for the Netherlands' society, how can the public core be protected and what is the role of the Netherlands Ministry of Defence and the armed forces in that?

1 Roy van Keulen, *Digital Force: Disrupting Life, Liberty and Livelihood in the Information Age* (PhD thesis, Leiden University, 2018), Chapter 2, p. 18. <http://hdl.handle.net/1887/62050>.

2 Paul Ducheine, 'Military Cyber Operations', in *Handbook of the International Law of Military Operations* (2nd ed.), ed. Terry D. Gill and Dieter Fleck (Oxford: Oxford University Press, 2015), pp. 456–475: 457.

3 Currently more than 5 billion people are connected; some 2.7 billion not yet. See ITU (2003), 'Population of Global Offline Continues Steady Decline to 2.6 Billion People in 2023 (12 September 2023)'. <https://www.itu.int/en/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx>. See initiatives and business models to facilitate connectivity such as The Other 3 Billion: <https://www.ses.com/o3b-mpower>.

4 John P. Barlow, 'A Declaration of the Independence of Cyberspace', *Electronic Frontier Foundation*, vol. 48, no. 3 (1996), p. 2.

5 Apple, Microsoft, Amazon, Nvidia, Meta Platforms, Tesla and Alphabet; see Alex Sebastian, 'The Magnificent Seven Stocks: Still a Great Opportunity or Overpriced and Set to Fall?', *The Times*, 23 August 2024. <https://www.thetimes.com/money-mentor/investing/magnificent-seven-stocks>.

6 See the individual wealth of Elon Musk, Jeff Bezos and Mark Zuckerberg, and see the market capitalisations of their companies.

7 See e.g. incidents such as the Microsoft (or CrowdStrike) outage (July 2024), Google (14 December 2020), DYN (21 October 2016), Amazon Web Services (7 December 2021). See also the Log4j and Citrix incidents.

8 See *Security Strategy for the Kingdom of the Netherlands* (2023), p. 19: 'Digitalisation makes systems more interconnected, and as a result, vital and nonvital processes become more susceptible to cyber threats.' <https://www.government.nl/topics/security-strategy-for-the-kingdom-of-the-netherlands>.

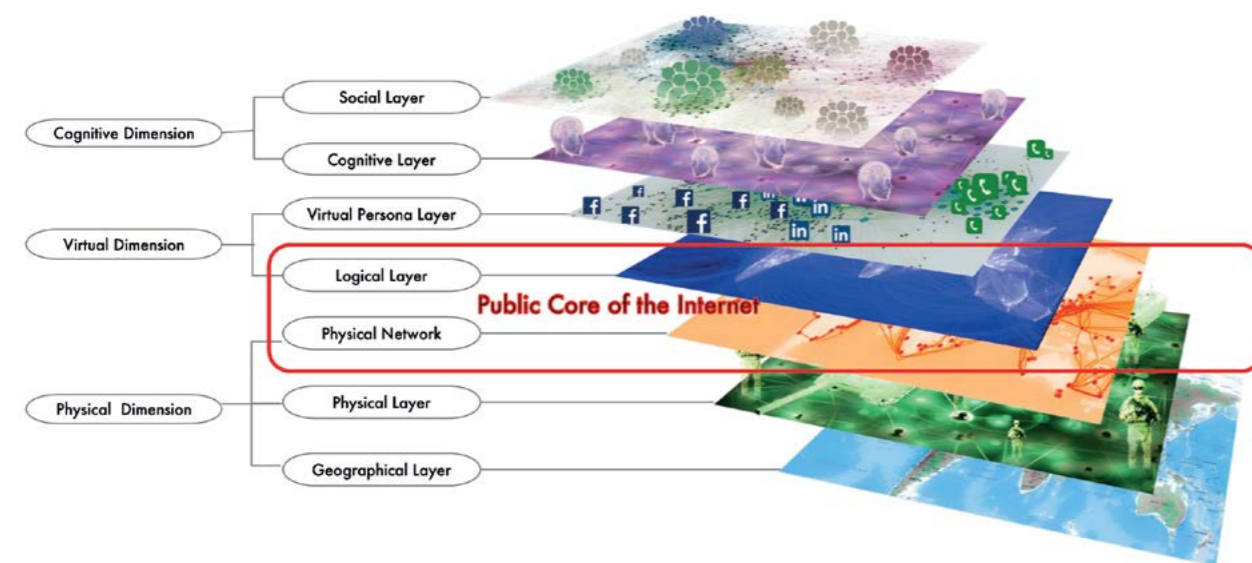
9 European Commission, 'The Digital Economy and Society Index (DESI)'. <https://digital-strategy.ec.europa.eu/en/policies/desi>.

10 See the work of Dennis Broeders, responsible for coining the term 'public core of the Internet'.

## On cyberspace and the public core of the Internet

The public core can be defined in a narrow or technical manner or approached as a broader functional issue. The technical approach links it to cyberspace, a human-made environment that is made up of physical and virtual dimensions. Cyberspace contains several layers: the physical network layer (computers, routers, cables); the logical layer (with its virtual objects such as data, protocols and software); and the virtual persona layer (email, social media accounts, URLs, IP addresses).

Figure 1. The public core of the Internet



The Global Commission on the Stability of Cyberspace (GCSC) defines the technical part of the public core of the Internet in terms of the physical transmission media combined with the systems and protocols for packet routing, naming and enabling cryptographic keys (including TCP/IP, DNS). Van Haaster, in his research on cyberspace, similarly argues that ‘the Internet’ entails the physical network layer and the logical layer that make communication possible, meaning the infrastructure (hardware) and the protocols and standards, including firmware, OS, apps, etc. (software).

The functional approach does not list the constituent elements of the Internet but focuses on the ‘general availability and integrity’ of the public core. While the technical approach is descriptive, the function of the Internet is a normative one that can depend on the political system, or perception of the Internet, of the state or community.

According to the Netherlands’ view,<sup>11</sup> the content itself is not part of the public core of the Internet but part of the logical layer and the virtual persona layer, and thus (the content of) websites, social media and instant messaging applications, e.g. WhatsApp are excluded from the public core.

11 Netherlands Ministry of Foreign Affairs, *International Cyber Strategy 2023–2028* (2023). <https://www.government.nl/documents/publications/2023/09/12/international-cyber-strategy-netherlands-2023-2028>.

Noting that the technical and functional views overlap, the public core of the Internet (and cyberspace) therefore rests within the logical and physical network layers (i.e. the technical view) while guaranteeing availability and integrity (the functional view) of data and communication (infrastructure and protocols).<sup>12</sup>

## On threats and vulnerabilities in a Netherlands context

In its annual cybersecurity assessments, the Netherlands’ government has named large-scale outages and tampering with global chains of ICT as two of the main cyber threats to national security. For years, it has signalled that digital processes are ‘the central nervous system of society’, and that ‘large-scale outages: situations in which one or more processes are disrupted due to natural or technical causes or unintentional human action’ are one of the major threats to national security.<sup>13</sup> In an effort to reduce risks to its cybersecurity, caused inter alia by outages, it is noted that ‘market dynamics complicate cyber risk management. Supply and demand for digital services, hardware (and components), software and networks converge on digital markets. These markets have a number of unique characteristics, such as the semi-monopolistic status of certain suppliers.’<sup>14</sup> The – often inevitable – dependency on these (semi-)monopolistic services or infrastructure suppliers is central to the idea that the public core of the Internet not only may suffer from technical failure,<sup>15</sup> but is also misused for geopolitical or criminal goals. In addition, ‘breaches of (the security of) cyberspace, such as through the misuse of global chains of ICT service providers, the exploitation of Internet protocols or the sabotage of cables’ are among the other main threats.<sup>16</sup>

The public core of the Internet is under (potential) threat when the technical aspects (the physical network and the logical layer) or the functional aspects (availability and integrity), including the organisations responsible for the functioning, are engaged with a malign intent.<sup>17</sup>

12 For an overview of the Netherlands’ interpretation and position on the public core, see Alexey Trepykhalin and Veni Markovski, *Country Focus Report: The Netherlands and the ‘Public Core of the Internet’* (ICANN, 2021). <https://itp.cdn.icann.org/en/files/government-engagement-ge/ge-008-28may21-en.pdf>.

13 NCTV, *Cyber Security Assessment Netherlands (CSAN) 2022* (2022), p. 15. <https://english.nctv.nl/documents/publications/2022/07/04/cyber-security-assessment-netherlands-2022>. See also *CSAN 2021*.

14 NCTV, *Netherlands Cybersecurity Strategy 2022–2028* (2022). <https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028>.

15 Whether or not caused by human failure, as was the case in the CrowdStrike outage (2024). See CISA, *Widespread IT Outage Due to CrowdStrike Update* (2024). <https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update>.

16 NCTV, *Cyber Security Assessment Netherlands (CSAN) 2023* (2023). <https://english.nctv.nl/topics/cyber-security-assessment-netherlands/documents/publications/2023/07/03/cyber-security-assessment-netherlands-2023>. The summary of assessed threats: (1) unauthorised access to information (and possibly its publication), in particular through espionage; (2) inaccessibility of processes, due to sabotage or cybercrime; (3) breaches of (the security of) cyberspace, such as through the misuse of global chains of ICT service providers, the exploitation of Internet protocols or the sabotage of cables; (4) large-scale outages: situations in which one or more processes are disrupted due to natural or technical causes or unintentional human action.

17 Leaving technical failure aside.

Attacks against the public core of the Internet can come in many guises. Lindsay and Gartzke provide an overview of cyber operations based on costs and rewards.<sup>18</sup> The public core is impaired if parts of it are not available for the public arena at large. Some states have the ambition to create a national Internet able to opt out of the World Wide Web at the will of the state,<sup>19</sup> which in itself is an undermining of the public core. A milder version of this lock-out is the ability to control parts or segments of the Internet. It is unlikely that, given the attributes of digital interconnectivity, a complete lock-out is feasible, and it needs to be taken into account that announcement of Internet fragmentation may have more symbolic than technical value.

The most frequent attacks against the technical public core are disruptions (e.g. large-scale ransomware attacks or wipers such as WannaCry, NonPetya) or tampering with the Border Gateway Protocol (BGP) or Domain Name System (DNS), or hacktivism including distributed denial of service (DDoS) attacks and website defacements that meddle with the logical layer of cyberspace. The impact of hacktivism is often limited to nuisance. The functionality of the Internet is under threat when main core services are not available, or when the integrity of the services cannot be guaranteed.

The public core is attacked or under threat when the technical physical network and the logical layer are undermined, or the functionality of the Internet is exploited. Most of the threats and attacks remain below the threshold of the use of force in terms of *ius ad bellum* (Art. 2(4) UN Charter)<sup>20</sup> and/or in terms of *ius in bello* (international humanitarian law, IHL) below an attack as in Art. 49 API.<sup>21</sup> Although it is evident that the Netherlands Ministry of Defence (MoD) and the armed forces are involved should these thresholds be crossed, the MoD also plays a role in providing protection below the threshold.

### How to protect the public core, and what is the role of the military?

‘Protecting the public core of the Internet’ is one of the Netherlands’ focal points in the strategic objective to maintain ‘a worldwide open, free and secure Internet’.<sup>22</sup> In parallel, the Netherlands aims to ‘combat cyber threats posed by states and criminals’ and to move ‘from a reactive to a proactive approach to cyber threats’ and ‘[reinforce and maintain] norms for responsible state behaviour’.<sup>23</sup>

18 Jon Lindsay and Erik Gartzke, *Coercion through Cyberspace: The Stability–Instability Paradox Revisited* (2016) [https://deterrence.ucsd.edu/files/LindsayGartzke\\_CoercionThroughCyberspace\\_DraftPublic1.pdf](https://deterrence.ucsd.edu/files/LindsayGartzke_CoercionThroughCyberspace_DraftPublic1.pdf).

19 Sometimes called the Balkanization of the Internet, or ‘SpllInternet’. See also Eneken Tikk and Mika Kerttunen, ‘The Alleged Demise of the UN GGE: An Autopsy and Eulogy’ (Cyber Policy Institute, 2017), p. 19. <https://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf>; Timmy Broderick, ‘Russia Is Trying to Leave the Internet and Build Its Own’, *Scientific American*, 12 July 2023.

20 Or armed attack (Art. 51, UN Charter). See Peter B.M.J. Pijpers, Hans Boddens Hosang and Paul A.L. Duchaine, ‘Dialects: Collective Cyber Defence in the EU and NATO’, in *A Language of Power? Cyber Defence in the European Union*, ed. Patryk Pawlak and François Delerue, Chaillot Paper 176 (November 2022), European Union Institute for Security Studies, pp. 72–81. <https://www.iss.europa.eu/content/language-power>.

21 Article 49 (1) of the 1st Additional Protocol to the Geneva Conventions of 12 August 1949 (ICRC, 1977).

22 Netherlands Ministry of Foreign Affairs, *International Cyber Strategy 2023–2028*, p. 4, ‘To maintain a global open, free and secure Internet, the Netherlands will protect the public core – in other words the technical layer – of the Internet, partly in order to prevent fragmentation.’

23 Netherlands Ministry of Foreign Affairs, *International Cyber Strategy 2023–2028*, p. 9.

In terms of combating threats, a number of roles have been defined. In the Netherlands digital telecommunication is a vital process, similar to the ability to transport energy or the embankments (dykes, weirs) that protect its citizens (and territory) from the water. It is vital as it supports core interests including our economic security and political and social stability. The ministry responsible for the Internet is the Ministry of Economic Affairs.

In protecting the public core, a difference can or should be made between protecting the physical aspects (hardware) versus the availability of the logical public core (software and protocols etc.). The physical aspects enjoy a deeper embedment of protection, not least by national and international law – the standards of sovereignty, non-intervention and *ius ad bellum* protect against attacks on cyber infrastructure. The non-tangible part of the public core is less easy to protect and will rely on the interpretation of states or groups of states on how to apply international law to the availability of the public core. While democratic states will value open and transparent societies, endorsing the freedom of speech to which the availability of the public core is vital, more authoritarian states, which use the Internet to suppress their population and prevent the diaspora from communicating alternative views inside the state, will take a more restrictive view.

The Netherlands’ view – a democratic view – is that digital attacks on the public core are not likely to reach the threshold of the use of force or (armed) attack, hence the military will not be the first responder. In reality, however, interfering with and attacking other states will be a combination of the use of multiple instruments of power in more than one domain, achieving effects not only in the physical but also in the virtual and cognitive dimensions. These hybrid attacks will require a whole-of-society defence and security doctrine.<sup>24</sup>

The response at the moment is layered. On the one hand, public and private organisations and dedicated private actors, including IT (security) firms, are the first line of defence, making sure their cybersecurity (firewalls, patches) is up to standards. This includes resilience of communication systems, inter alia by hardening, segregation or redundancy. In this vein, the Netherlands’ MoD offers a separate IT network to facilitate its own services and communication, while it is also made available for other governmental organisations and services.<sup>25</sup>

On the other hand are the governmental bodies. Firstly, nationally oriented agencies including the National Coordinator on Terrorism and Security (NCTV) (which encompasses the National Cyber Security Coordinator) and law enforcement services will assume responsibility. MoD organisations such as the Defence Cyber Security Centre, military constabulary (military police) and Defence Cyber Command may support these organisations with specialists, operating within the mandates of the supported entities (e.g. law enforcement).<sup>26</sup> A more assertive line of defence

24 See NCTV, *Netherlands Cybersecurity Strategy 2022–2028*, as well as Security Strategy for the Kingdom of the Netherlands (2023). <https://www.government.nl/topics/security-strategy-for-the-kingdom-of-the-netherlands>.

25 The so-called Netherlands Armed Forces Integrated Network (NAFIN), however, suffered from an outage for several days, hampering – apart from the MoD’s internal communications – civilian air traffic at Eindhoven Airbase, issuing of (emergency) passports, 2FA for national digital IDs and the C2000-communication system used by emergency services. See Ruben Brekelmans, ‘Cause of Defense Outage Still Unclear; Cyber Attack not Definitively Ruled Out: Minister’, *NL Times*, 28 August 2024. <https://nltimes.nl/2024/08/28/cause-defense-outage-still-unclear-cyber-attack-definitively-ruled-minister>.

26 Paul A.L. Duchaine and Peter B.M.J. Pijpers, ‘The Notion of Cyber Operations’, in *Research Handbook on International Law and Cyberspace*, 2nd ed., ed. N. Tsagourias and R. Buchan (Cheltenham: Edward Elgar, 2021), pp. 272–296.

is related to the two intelligence and security agencies.<sup>27</sup> These are mandated to actively further and protect our democratic rule of law, and our national vital interests in general. The activities of the intelligence and security agencies are governed by a formal act (legislation) permitting them to operate outside of an armed conflict and below the threshold of the use of force. Within their mandates, the above entities will assume responsibility on a permanent basis.

Secondly, the role of the armed forces<sup>28</sup> in protecting cyberspace – and the public core of the Internet – requires an ad hoc decision to act. For domestic situations, when they are supporting national police, this authority rests with the minister of justice and security. In general support of other public governmental bodies, the minister of defence may authorise assistance. However, in international situations, a cabinet decision is required.<sup>29</sup> After a cabinet decision, cyber specialists of the armed forces may be ‘deployed’ for a situation of intervention on invitation, in response to an armed attack, or once engaged (otherwise) in (armed) conflict, or during an expeditionary mission governed by the UN Security Council.

The norms and the legal framework related to the decision to deploy and engage cyber specialists in a conflict mode internationally, as well as the applicable legal regimes for their acts and operations, will be found in international law and agreements. The development of norms, their interpretation and their enforcement are an important avenue to reinforce responsible behaviour – but are not always a given. The Netherlands’ efforts to further norms can be found in its support of the UN GGE and OEWG, as well as in its material and organisational support to the ‘Tallinn Manual’ process. The process of norm seeking and creation is a continuous endeavour,<sup>30</sup> in which the Netherlands has been forward-leaning.<sup>31</sup> Within the sphere of *ius ad bellum*, well before NATO’s and the EU’s views coincided,<sup>32</sup> the Netherlands took the view that an armed attack launched in or through cyberspace could trigger the state’s right to self-defence, and might offer legal grounds to use armed force in response: ‘The government therefore endorses the finding ... that “a cyber attack that has comparable consequences to an armed attack (fatalities, damage and destruction) can justify a response with cyber weapons or conventional weapons ...”’. There is therefore no reason not to qualify a cyberattack against a computer or information system as an armed attack if the consequences are comparable to those of an attack with conventional or non-conventional weapons.’<sup>33</sup>

27 Military I&S Service (MIVD) and General I&S Service (AIVD). The MIVD does not report to the Chief of Defence (CHoD) but is subordinated to the Secretary-General and the Minister of Defence.

28 I.e. dedicated cyber operators of the armed services (navy, army, air force and military police in support of national police).

29 P.A.L. Ducheine, K.L. Arnold and Peter B.M.J. Pijpers, ‘Decision-Making and Parliamentary Control for International Military Cyber Operations by the Netherlands Armed Forces’, Amsterdam Law School. <https://ssrn.com/abstract=3540732>. Also available in *Military Operations and the Notion of Control Under International Law: Liber Amicorum Terry D. Gill*, ed. Rogier Bartels et al. (The Hague: TMC Asser Press/Springer, 2020), pp. 59–81.

30 See e.g. Ferry Oorsprong, Paul Ducheine and Peter Pijpers, ‘Cyber-attacks and the Right of Self-Defense: A Case Study of the Netherlands’, *Policy Design and Practice*, vol. 6, no. 2 (2023), pp. 217–239.

31 See inter alia the so-called Hague Process in support of the drafting of the Tallinn Manuals: Michael Schmitt, ‘The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis’, *Just Security*, 14 October 2019. <https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis>.

32 See Hans Boddens Hosang and Paul Ducheine, ‘Implementing Article 42(7) of the Treaty on European Union – Legal Foundations for Mutual Defence in the Face of Modern Threats’, in *The European Union’s Contribution to International Peace and Security*, ed. Stephen Marquardt and Steven Blockmans (Brill: Leiden-Boston, 2023), pp. 212–240.

33 Ministry of Foreign Affairs, *Annex to Letter to the Parliament on the International Legal Order in Cyberspace* (2019). <https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>.

Looking ahead, it will be most interesting to analyse future international criminal trials related to e.g. the war in Ukraine, as well as future criminal indictments related to assertive and offensive state(-supported) behaviour and to follow jurisprudence and legal doctrine in that respect.

## Conclusion

In sum, the public core of the Internet in the narrow sense entails a physical network layer and a virtual, logical layer of protocols. The broader definition also includes the availability of the public services provided by the technical aspects of the public core.

It should be taken into account that protection is a collective effort in which states are not the main actors, and the involvement of armed forces may be an option of last resort. In addition, protecting tangible aspects (computers etc.) and the availability of services may, given their distinctive attributes, require two different arenas but complementary approaches.

## 8. Evolving South Korea's cybersecurity strategy and implications for global critical Internet infrastructure

In Tae Yoo

The protection of the public core of the Internet has been called for by various stakeholders such as diplomatic, technical and civil society communities and has gained significant support, culminating in being mentioned in consensus reports and discussion agendas in global multilateral venues such as GGE and OEWG.<sup>1</sup> The public core of the Internet is critical Internet resources: packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, and physical transmission media.<sup>2</sup> Because of its inherent nature and operation, whereby it connects users across sovereign borders and is shared by them, the public core of the Internet *can be transnational* critical Internet resources. But it can also be regarded and used as *national* policy tools, especially where tangible hardware parts of the public core of the Internet are concerned, because in this case it is easier to determine who owns the property or that the property is under a particular sovereign. Because of the globally *public* nature of core Internet resources, how individual nations perceive the core parts of the Internet matters in the process of hammering out and shaping a common ground.

It is in this context that the Republic of Korea's (ROK) conception of the public core of the Internet is discussed in the present research. There is no reference to the public core of the Internet in official South Korean government documents. The closest analogue to the hardware aspect of the concept is 'critical information and communication infrastructure,' which is similar to the US's critical information infrastructure.<sup>3</sup> The ROK has a legal framework for the protection of critical information and communication infrastructure and is highly vigilant about cyber breaches of such facilities. According to the Information and Communications Infrastructure Protection Act, 'information and communication infrastructure' means electronic control and management systems related to national security, administration, defence, public security, finance, telecommunications, transportation, energy, etc. and information and communication networks pursuant to Article 2, Paragraph 1, Item 1 of the Act on Promotion of Information and Communication Network Utilisation and Information Protection. While the country has a well-developed legal and regulatory framework for other aspects of the public core of the Internet, it does not pay as much attention to cyberattacks by external actors on those aspects as it does to attacks on the critical information and communication infrastructure. Therefore, in the event of a conflict between states through cyberspace, that particular aspect of the public core of the Internet may be the primary area of focus by officials in the ROK.

1 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*, vol. 6, no. 3 (2021), pp. 277–97; Dennis Broeders, 'Aligning the International Protection of "the Public Core of the Internet" with State Sovereignty and National Security', *Journal of Cyber Policy*, vol. 2, no. 3 (2017), pp. 366–76.

2 Global Commission on the Stability of Cyberspace, *Definition of the Public Core, to Which the Norm Applies* (The Hague, 2018).

3 The National Intelligence Service, the Ministry of Science and ICT, the Ministry of the Interior and Safety, the Personal Information Protection Commission, the Financial Services Commission, and the Ministry of Foreign Affairs of the Republic of Korea, *National Cybersecurity White Paper* (Seoul, 2024).

In contrast, the *transnational* aspect of the public core of the Internet is seldom acknowledged in official Korean government documents. This aspect inevitably entails international collaboration between or beyond nations, with the Ministry of Foreign Affairs assuming the primary role in this regard. However, as previously stated, it appears that the public core of the Internet is not a prominent focus for the Korean government, and the international aspect of 'critical information and communication infrastructure' is not a significant concern for the ministries responsible for international cooperation. It is primarily recognised as an object of protection at the domestic level for national constituents. Consequently, the agencies with the greatest interest in 'critical information and communication infrastructure' are mainly the domestic agencies (not including agencies related to international cooperation), such as the National Intelligence Service, the Ministry of Science and ICT and the Korea Internet and Security Agency, while the Ministry of National Defence is responsible for the Internet only within the purview of national defence.

As previously stated, the components of the public core of the Internet are perceived in South Korea primarily in terms of the protection of domestic lives and properties. On the other hand, there has been no clear official government position on the transnational nature of 'critical information and communication infrastructure'. At least according to the National Cybersecurity White Paper, published jointly by the National Intelligence Service, the Ministry of Science and ICT, the Ministry of the Interior and Safety, the Personal Information Protection Commission, the Financial Services Commission and the Ministry of Foreign Affairs, and the Defence White Paper, published by the Ministry of National Defence, there is a lack of clarity regarding the utilisation of transnational critical infrastructure in the event of a conflict between states. While the South Korean government is in general agreement with and adheres to international norms and international law, there is a need for further discussion on how to interpret and implement international norms that are not necessarily globally accepted, and how to deal with countries that ignore them, especially when the ROK has to take actions on adversarial attacks through the public core of the Internet.

In this context, the following section presents an analysis of two national cybersecurity strategies as concrete evidence for the above arguments. The ROK published its inaugural National Cybersecurity Strategy (NCSS) in 2019, with a second iteration released in 2024. Neither of the cybersecurity strategies under consideration discusses the public core of the Internet in isolation. While the former strategy emphasises resilience of the critical information and communication infrastructure, recognising it as an object to be protected at the domestic level, the latter shifts the focus of the NCSS from a defensive to an offensive stance to some extent. Still, it is pertinent to enquire as to the stances adopted by these strategies with regard to the public core of the Internet and its interconnectivity with other countries. The strategies are relatively recent, and according to the author's research, which includes official disclosure requests for governmental documents, it appears that specific operational guidance based on the 2024 strategy is either lacking or undisclosed.

### *The National Cybersecurity Strategy of the Republic of Korea in light of the public core of the Internet*

The 2019 NCSS of the ROK states that its vision is to ‘create a free and safe cyberspace to support national security, promote economic prosperity, and contribute to international peace’.<sup>4</sup> The outlined vision closely aligns with that upheld by liberal democratic states and the norms and values established by other developed democratic governments. Following an exposition of the publication’s background in Chapter 1, the 2019 NCSS articulates this vision alongside three overarching goals in Chapter 2: namely, to ensure the stable operations of the state, respond to cyber attacks, and build a strong cybersecurity infrastructure. Additionally, it delineates three fundamental principles: balancing individual rights with cybersecurity measures, conducting security operations in accordance with the rule of law, and fostering a collaborative system of participation and cooperation.

From the stated vision and the goals, the 2019 NCSS aimed to be a comprehensive national security document in the realm of cybersecurity. Notably, it presents an inclusive compendium of national imperatives, reflecting the diverse interests of numerous governmental departments related to cyberspace in the context of national security. The strategic tasks outlined subsequent to the enunciation of vision, goals and principles within the document are exhaustive, encapsulating the agendas of various agencies spanning domains such as domestic security, industry, military, intelligence, diplomatic, cultural and social affairs. This breadth of coverage extends to multistakeholder engagements and stands in contrast to another NCSS published in 2024, which will be discussed further below.

Chapter 3 of the 2019 NCSS delineates six strategic tasks, each comprising distinct sections. The first section, particularly pertinent to our discussion, emphasises the safeguarding of ‘national core infrastructure’ as the primary imperative for realising the vision and objectives outlined in the document. This initial section is subdivided into three subsections.

The first subsection elucidates the protection of national information and communication networks. It encompasses security technologies and systems to protect the ICT environment, including mobile and cloud facilities. At this point, however, it is unclear what ‘national core infrastructure’ means, as mobile and cloud facilities may not be exclusively in government ownership, thus they are not inherently national assets. Cryptographic and confidential information security systems are also mentioned to ensure the protection of governmental confidential data against breaches and corruption, so it seems that the government perceives the demarcation between the public and private domains. In other words, physical core infrastructures are regarded as pivotal to national security, while data are distinguished based on levels of confidentiality. Lastly, emphasis is placed on international technical standards in constructing national informational communications networks in order to facilitate prompt response in the event of security incidents. Notably, this aspect prompts contemplation on the potentiality of international cooperation with regard to ‘core infrastructure’.

The second subsection of the 2019 NCSS delves into the environmental dimension of ensuring the safety of critical infrastructure. It aims to enhance schemes and guidelines to facilitate the

<sup>4</sup> National Security Office of the Republic of Korea, *National Cybersecurity Strategy* (Seoul, 2019).

government in swiftly designating and safeguarding critical infrastructure facilities. Additionally, governmental efforts extend to establishing departments and budgets dedicated to cybersecurity. Acknowledging the significance of private entities, the government pledges to cultivate an environment conducive to voluntary security assessments by the private sector, exemplified in inspector schemes and evaluation standards.

The concluding subsection addresses the subject of next-generation cybersecurity infrastructure. Central to the discussion is the concept of ‘security by design’ in ICT products and services, the establishment of high-assurance networks inherently resilient to cyber threats, and the development of next-generation security authentication infrastructure.

The Moon Jae-in administration, which promoted ‘comprehensive security’ as a national security policy, was characterised by its efforts to make a comprehensive survey on all issues related to national cybersecurity strategy and systematically organise them at the governmental level. This approach intended not only to respond to domestic governance needs but also to reflect the diplomatic strategy of ‘strategic ambiguity’ to some extent. That is, on the one hand, this feature arose because South Korea was pursuing balanced diplomacy or hedging between the US and China amid their strategic competition. On the other hand, it was due to a conciliatory stance toward North Korea.

However, this diplomatic strategy of South Korea shifted with the inauguration of the Yoon Suk-yeol administration in May 2022. Emphasising ‘strategic clarity’, the new administration pursued stronger alignment with the US, distanced itself from China through ‘values-based diplomacy’ and adopted a confrontational stance towards North Korea. This national security posture is also reflected in the cybersecurity strategy document published in 2024.

The freshly released 2024 NCSS continues many of the tasks outlined in its 2019 predecessor, albeit with significant alterations that underscore an active defence posture concerning cybersecurity, particularly in response to malevolent actions orchestrated by North Korea.<sup>5</sup> Following an exposition of the contextual backdrop surrounding the publication of the 2024 NCSS in Chapter 1, Chapter 2 delineates its vision and three primary objectives. The vision posits ROK as a global pivotal state, steadfastly championing the values of freedom, human rights and the rule of law within cyberspace while fulfilling its role and responsibilities to international society.

Although the alignment of the objectives with the pursuit of freedom, human rights and the rule of law as stated in the vision remains somewhat ambiguous, Chapter 2 articulates three goals: offensive cyber defence and response; amplifying global leadership; and fortifying robust cyber resilience. Furthermore, Chapter 2 introduces three guiding principles to underpin the attainment of these objectives: firstly, earnest consideration is given to striking a delicate balance between the core values of the state and the economic welfare of its citizens; secondly, acknowledging the paramountcy of cybersecurity, concerted efforts are to be made in order to foster a collective response involving all stakeholders, encompassing actors from the government, industry and academia; thirdly, cybersecurity-related endeavours are executed in adherence to established norms, thereby safeguarding individuals’ fundamental rights against encroachments such as privacy infringements through legitimate and lawful means.

<sup>5</sup> National Security Office of the Republic of Korea, *National Cybersecurity Strategy* (Seoul, 2024).

Three changes stand out in the 2024 NCSS compared to its 2019 predecessor. Firstly, the document underscores a national active and proactive stance in cyberspace, diverging from a purely defensive posture. It is prudent to exercise caution with specific terms utilised in news reports, such as ‘offensive’ and ‘preemptive’,<sup>6</sup> as they may not accurately depict the primary characteristics of ROK’s cybersecurity strategy. Elaboration on this matter is provided below. Secondly, the 2024 NCSS places significant emphasis on North Korea as a prominent cyber threat. Lastly, the document exhibits a heightened focus on the strategic security dimension, surpassing considerations that would have been raised by governmental departments associated with industry, economy, society and culture. Indeed, within Chapter 1, the document explicitly emphasises its national security aspect over the technical intricacies of cybersecurity.

Concerning the public core of the Internet, both the 2024 and 2019 documents acknowledge the significance of protecting critical infrastructure. However, there seems to have been a shift in priorities. The 2024 NCSS addresses critical infrastructure in the *third* subsection of Chapter 3, which outlines five strategic tasks and corresponding subsections. These tasks are: (1) bolstering offensive cyber defence activities; (2) establishing a global cyber cooperation system; (3) fortifying the cyber resilience of national critical infrastructure; (4) securing critical emerging technology; and (5) enhancing the foundational aspects of task performance.

Of particular relevance to the discussion on the public core of the Internet is the third section of Chapter 3. The section comprises three subsections: (1) fortifying the security of critical information systems; (2) reinstating the security system of a digital platform government; and (3) instituting a security and response system for the ICT supply chain at the national level. Notably, while there are several commonalities with the 2019 NCSS, the 2024 NCSS appears to incorporate concepts aligned with US cybersecurity strategies, such as zero trust, cybersecurity of the software supply chain, and the designation of trusted suppliers of ICT commodities and components.

In this context, the ROK has undoubtedly updated its NCSS by incorporating strategic cybersecurity concepts from its primary ally, the US, and aligning itself with like-minded states. The Five Eyes alliance members exhibit a high degree of similarity in their strategic cybersecurity orientations, with some actively embracing offensive cyber capabilities pioneered by the US.<sup>7</sup> Japan, a key ally of the US in the Indo-Pacific region alongside the ROK, has also charted a new course in its cybersecurity strategy as of 2022. The National Security Strategy of Japan approved by the cabinet in December 2022 explicitly states Japan’s intention to adopt active cyber defence, and potentially offensive cyber operations, ‘for eliminating in advance the possibility of serious cyberattacks that may cause national security concerns to the Government and critical infrastructures and for preventing the spread of damage in case of such attacks, even if they do not amount to an armed attack’.<sup>8</sup>

6 Haye-ah Lee, ‘Gov’t unveils Nat’l Cybersecurity Strategy with new focus on N. Korea’, *Yonhap News*, 1 February 2024, <https://en.yna.co.kr/view/AEN20240201007800315>; Joon Ha Park and Shreyas Reddy, ‘South Korea Unveils New Cyber Strategy to Counter North Korean Threats’, *NK News*, 2 February 2024, <https://www.nknews.org/2024/02/south-korea-unveils-new-cyber-strategy-to-counter-north-korean-threats>.

7 Josh Gold, *The Five Eyes and Offensive Cyber Capabilities: Building a ‘Cyber Deterrence Initiative’* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2020).

8 National Security Council of Japan, *National Security Strategy of Japan* (Tokyo, 2022), p. 33.

While some news media have translated *sunjaejeok* actions outlined in the 2024 NCSS as *preemptive* measures to be taken by the ROK government, it might be more apt to characterise them as *proactive*. This interpretation dovetails better with the contextual framework provided in the background chapter of the 2024 NCSS, which underscores the significance of the US–ROK alliance and trilateral cybersecurity cooperation involving the US, Japan and the ROK. Prior to Japan’s adoption of active cyber defence in 2022, the US had already introduced the strategic concept of persistent engagement and defending forward, and articulated its commitment to shift its cybersecurity ‘posture in cyberspace from reactive to *proactive*’ in 2018.<sup>9</sup> The concept of defending forward outlined in the 2018 DoD Cyber Strategy entails disrupting malicious cyber activities at their source, even those falling below the threshold of armed conflict. Further, it means ‘if a device, a network, an organization, or adversary nation is identified as a threat to U.S. networks and institutions, or is actively attacking them in or through cyberspace – it can expect the United States to impose costs in response’.<sup>10</sup> It is noteworthy that the US strategy document does not mention preemptive actions but rather proactive cyberattacks, if deemed necessary. Similarly, the Chief of the Cyber Operations Command of ROK has emphasised the need for operations grounded in the concept of defence forward, extending beyond purely defensive operations.<sup>11</sup>

However, it is disagreeable that the interpretations of the term *sunjaejeok* as proactive rather than preemptive and *gongsejeok* as defending forward rather than offensive as used in offensive realism are in accordance with the scope of conventional military operations long held by Section 1 of Article 5 in the Constitution of the ROK, which explicitly rejects wars of aggression, because the policymakers could have meant the cybersecurity strategy of the ROK to be preemptive and offensive at the *strategic* level. Nonetheless, it is more plausible to reason that those new characteristics added to the 2024 NCSS are meant to be applied to the *tactical* or *operational* level, because only defensive warfare is authorised by the Constitution, consistent with the principles outlined in the United Nations Charter. Thus, preemptive and offensive operations are deemed justifiable only in cases where the threat is imminent and when such operations are taken as deterrent and retaliatory measures proportional to the actual attack.

Still, it seems that the new strategy has not yet been reflected in operational guidelines. Thus, it remains to be seen how the 2024 NCSS will unfold in real-world application. The 2024 NCSS underscores that the shift toward an offensive cyber stance is largely motivated by the need to cope with the malicious cyber activities originating from North Korea. Thus, the new national cybersecurity strategy stance in the 2024 NCSS may be emphasising defensive measures or retaliatory offensive ones to resolve costs incurred by the North Korean cyberattack or prevent further cyberattacks at best.

The critical problem without clear red lines or rules of engagement in offensive cyber defence is that the line between defensive and offensive warfare often becomes ambiguous. For instance, the ROK government previously justified its involvement in the 2003 Iraq war, despite its being

9 Emphasis added. Department of Defense of the United States, *Department of Defense Cyber Strategy* (Arlington, VA, 2018); see also: <https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement>.

10 Department of Defense of the United States, *Cyber Strategy*.

11 See <https://e.chosunbiz.com/2023-%EC%82%AC%EC%9D%B4%EB%B2%84%EB%B3%B4%EC%95%88-%EB%B0%95%EA%B7%9C%EB%B0%B1-%EA%B5%AD%EB%B0%A9%EB%B6%80-%EC%82%AC%EC%9D%B4%EB%B2%84%EC%9E%91%EC%A0%84%EC%82%AC%EB%A0%B9%EA%B4%80-%EB%B0%A9/>.

perceived as an act of aggression by certain constituents. The deployment of ROK's Zaytun forces was contingent on strict conditions stipulating their role in supporting peace, security and reconstruction efforts, while abstaining from direct engagement in warfare. In cyberspace, it will become much harder to determine who started a conflict and who became the imminent threat first. This critical challenge is in line with the foggy line between the intelligent and disruptive purposes of cyber operations, especially when those operations are conducted against the public core of the Internet.

Another demanding problem stems from unresolved strategic alignment and operational guidelines in the alliance between the US and South Korea. It is not only about sharing information on cyber threats between the armies of the two countries.<sup>12</sup> The 2024 NCSS warrants further elucidation due to the potential interpretation of its adoption of an aggressive posture as a preparatory measure for conventional military operations, which might be requested by an ally. Clarity is needed to address concerns regarding intensifying tensions between the US and China and the growing possibility of the ROK becoming embroiled in a militarised conflict, particularly one instigated by China's potential invasion of Taiwan, amid ongoing strategic rivalry between these major powers. The US–ROK mutual defence treaty, formed in 1953, mandates the constitutional processes of each country to delineate the parameters of core national security.<sup>13</sup> The acknowledged interpretation of the parameters of the role of the ROK military is to protect the sovereign territory of the ROK. Given the recent framing of the nation's core interest as outlined in the strategic document of the ROK's Indo-Pacific Strategy, it could appear to extend beyond the Korean peninsula towards the Indo-Pacific region; clarification is imperative.

There is a nuanced line between offensive cyber operations motivated solely by strategic interests and those conducted in response to cyber attacks. The latter operations align with the Constitution, whereas the former would diverge from it. Transitioning from a reactive to a proactive posture does not necessarily denote a shift from defensive to offensive strategy; instead, it may entail moving from a cyber defence strategy without countermeasures to one incorporating retaliatory responses that would impose costs on the perpetrator. The former approach might equate to a cybersecurity strategy focused on deterrence by denial, whereas the latter involves a cybersecurity strategy based on deterrence by punishment, entailing the imposition of costs on cyber perpetrators. Indeed, the second section of Chapter 3, which immediately follows the first section on offensive cyber defence activities, suggests cyber *deterrence* through international cooperation and commits to making progress in cultivating norms for such cooperation.

The third section of Chapter 3 centres on national critical infrastructure and its cyber resilience. It outlines three key objectives: enhancing the security of critical information systems; reinstating the security management system for the realisation of digital platform government; and establishing a security policy and response system for the national ICT supply chain.

12 Erica D. Lonergan and Mark Montgomery, 'The Promise and Perils of Allied Offensive Cyber Operations', *14th International Conference on Cyber Conflict* (Tallinn, 2022), pp. 79–92; James E. Platte, 'Bilateral Alliances in an Interconnected World: Cyber Deterrence and Operational Control in the US Indo-Pacific Strategy', *Asian Perspective*, vol. 47, no. 1 (2023), pp. 75–99.

13 Article III of the US–ROK Mutual Defense Treaty states: 'Each Party recognizes that an armed attack in the Pacific area on either of the Parties in territories now under their respective administrative control, or hereafter recognized by one of the Parties as lawfully brought under the administrative control of the other, would be dangerous to its own peace and safety and declares that it would act to meet the common danger in accordance with its constitutional processes.'

Unlike some other states, such as the US, this chapter thus does not posit a public–private partnership. Instead, it aims to establish guidelines and standards for entities involved in critical infrastructure to adhere to. Given the aforementioned national deterrence stance, it seems logical that the third section, titled 'Enhancing cyber resilience of critical infrastructure', is placed after the emphasis on 'offensive cyber defence' activities in the 2024 NCSS, rather than in the first section of Chapter 3 as in the 2019 NCSS, given that cyber resilience is realised through undertaking defensive cyber operations, but not necessarily offensive operations. Thus, this shift reflects the 2024 NCSS's greater emphasis on offensive operations as retaliatory and thus deterring countermeasures. However, because the chapter does not explicitly designate critical infrastructure as red lines, which would serve as prerequisites for retaliatory cyber operations when crossed by an adversary, clarity on this matter is needed.



## Authors

### *Bibi van den Berg*

Bibi van den Berg is full professor of Cybersecurity Governance at Leiden University, and the head of the Cybersecurity Governance research group at the Institute of Security and Global Affairs of this university. Van den Berg has an MA and PhD in philosophy, both from Erasmus University in Rotterdam. Her research and teaching focus on several themes: (1) cybersecurity governance, (2) governance of security and safety and (3) regulating human behavior through the use of technologies (techno-regulation and nudging). Van den Berg is the chair of ACCSS, the Academic Cyber Security Society in the Netherlands. She is also a member of the Dutch Cyber Security Council (a Council that advises the Dutch cabinet on how to improve cybersecurity in the Netherlands). Aside from this, Van den Berg is a member of the ICT Advisory Board of the Central Bureau of Statistics in the Netherlands, the chair of the Advisory Board of ID&D, a member of the Advisory Board of ANVS, a member of the Committee Knowledge and Research of the Police Research Board, and a member of the Advisory board of dcipher, the Dutch platform for cybersecurity knowledge and innovation.

### *Dennis Broeders*

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.

### *Byoung Won Min*

Byoung Won Min is Professor of Political Science and International Relations at Ewha Womans University. He also has been Director of the Association of Internet Governance Researchers since 2023 with its collaboration with the Korean Internet Security Agency. His research interests are including international relations theories, global governance of the Internet, international security, and the complex systems theory. He has published *International Politics as a Complex System* (2005) and *The Network International Politics* (2023) in Korean and many other papers in academic journals. Min holds Ph.D. degree in Political Science at the Ohio State University (2002) and MA and BA degrees at Seoul National University. After working at the Sejong Institute for foreign policy and security in Seoul between 1988 and 1993, he spent two years at the Mershon Center for security studies as a research fellow in 1999 and 2000. He had taught for years at the Graduate School of Public Policy and Information Technology of Seoul National University of Technology between 2004 and 2011 before he moved to the current institution.

### *Paul Ducheine*

Brigadier-general Paul Ducheine is a Professor for Cyber Warfare at the Netherlands Defence Academy and a Professor in the Law of Military Cyber Operations at the University of Amsterdam. Ducheine started his military career in 1983 at the Royal Military Academy and joined the Engineer Regiment (as a combat engineer) in 1987. In 1998 he joined the Army Legal Service. Currently, he is the chair of the War Studies Department at the Netherlands Defence Academy. Prof. Ducheine holds degrees in Political Sciences (Amsterdam Free University, 1993) and Law (University of Utrecht, 1998). In 2008 he defended his PhD-thesis at the University of Amsterdam. During the *Tallinn Manual 2.0* process, he was a member of the International Group of Experts.

### *Olaf Kolkman*

Olaf Kolkman is the Principal Internet Technology, Policy, and Advocacy at the Internet Society. Olaf has two and a half decades of experience in Internet technology and policy matters, in particular those related to security and trustworthiness of the Internet. He is an executive level advisor to, and spokesperson of, the Internet Society. He strategises, formulates, reviews and advises on technical and policy issues. He serves on several advisory boards and is treasurer of the Global Forum on Expertise in Cyberspace. He served as IAB chair between 2007 and 2011 and was commissioner on the Global Commission on the Stability of Cyberspace.

### *Jung-Sup Park*

Jung-Sup Park is a Director of the KRNIC at Korea Internet & Security Agency(KISA). He was a manager of personal information team and Prevention Planning Team at KISA, and an Advisory in Gwangju City Hall in AI Policy. He has a Master's degree in Management Information System at Hankook University of Foreign Studies. He is highly interested in digital transformation which is caused by Internet. In the progress of digital transformation, he believes in the importance of individual participation based on a multi-stakeholder model. He places a high value on the process of learning and experiencing for individuals to discuss about their interests (thoughts), and reach out at some agreements.

### *Peter B.M.J. Pijpers*

Peter B.M.J. Pijpers Ph.D. is the Vice Dean of Education at the Faculty of Military Sciences of the Netherlands Defence Academy, Associate Professor Cyber Operations at the War Studies Department of the Faculty of Military Sciences, a researcher at the Amsterdam Centre of International Law, University of Amsterdam, and a non-resident fellow at the University of South Florida. His main area of research are the legal and military implications of cyber operations below the threshold of the use of force, with a special focus on digital influence operations (cognitive operations in cyberspace).

### *Jan Aart Scholte*

Jan Aart Scholte is Professor of Global Transformations and Governance Challenges at Leiden University since 2020. He leads Leiden's programme on Global Transformations and Governance Challenges (GTGC) (<https://www.universiteitleiden.nl/gtgc>), an interfaculty and interdisciplinary initiative to advance knowledge and practice on how we govern—and could govern—major world-scale changes in contemporary society. His own current research examines governing a global world both in general conceptual terms and with specific reference to internet governance. He has worked especially closely on research and policy regarding ICANN and the Regional Internet Registries. His books include *Globalization: A Critical Introduction* (Palgrave, 2005), *Encyclopedia of Globalization* (2007), *Building Global Democracy?* (Cambridge, 2011), *Legitimacy in Global Governance* (Oxford, 2018), *Global Governance: Fit for Purpose?* (SNS, 2023), and *Polycentrism: How Governing Works Today* (Oxford, 2023). Recent articles have appeared in *American Political Science Review*, *European Journal of International Relations*, *Global Governance*, *International Affairs*, *International Studies Review*, *International Theory*, *Regulation & Governance*, and *Review of International Studies*.

### *Arun Sukumar*

Arun Sukumar is Assistant Professor at the Institute of Security and Global Affairs (ISGA), Leiden University, and a researcher with The Hague Program on International Cybersecurity at Leiden. He is a lawyer by training, with a PhD in international relations from The Fletcher School at Tufts University. Arun served on the board of the Digital Public Goods Alliance in 2022-23, and was previously part of the World Economic Forum's Global Future Council on the Digital Economy and Society.

### *Paul Timmers*

Prof Dr Paul Timmers is research associate at the University of Oxford, Oxford Internet Institute, professor at KU Leuven and European University Cyprus, senior advisor EPC Brussels, President of the Supervisory Board Estonian eGovernance Academy, member of the EU Cyber Direct Advisory Board, research fellow of CERRE, and CEO of iivii (<https://iivii.eu>). He was Director at the European Commission with responsibility for legislation and funding for cybersecurity, e-ID, digital privacy, digital health, smart cities, and e-government; and cabinet member of European Commissioner Liikanen. He was software manager at a large ICT company and co-founded an ICT start-up. Physics PhD from Radboud University (Nijmegen, NL), MBA from Warwick University (UK), EU fellowship at UNC Chapel Hill (US), and a cybersecurity qualification from Harvard. His main interests are technology and geopolitics, publishing and advising on digital developments, technology and sovereignty, cybersecurity, industrial policy, and sectoral policies such as telecommunications, semiconductors and digital health.


### *In Tae Yoo*

In Tae Yoo is assistant Professor and Chair in the Department of Political Science and International Relations at Dankook University, and Director of the DKU Center for Advanced Political Research. Formerly, he was an assistant professor at Jeonbuk National University, research professor at Yonsei University, and Visiting Research Fellow at Waseda University. He has been a member for the Internet Governance Research Council at the Korea Internet & Security Agency (KISA). He has published a number of articles, book chapters and think-tank analyses, with regard to politics of cybersecurity, (international) political economy of (digital) trade, and Internet governance. Some of the topics of his work include “Cyber Deterrence and Offensive Cyber Operations,” “Bilateral Cyber Confidence Building Measures in Northeast Asia,” “Cybersecurity Crisscrossing International Development Cooperation: Unraveling the Cyber Capacity Building of East Asian Middle Powers Amid Rising Great Power Conflicts,” “Multistakeholderism in Global Internet Governance amid the US-China Strategic Competition,” “Internet Governance Regimes by Epistemic Community: Formation and Diffusion in Asia,” “The Five Eyes on Huawei: Middle Powers at the Crossroad amid Great Power Competition on Digital Hegemony,” “Is the Liberal International Trade Order Fragmenting or Diverging? Contested Digital Trade Regimes through Preferential Trade Agreements,” “The Emergence of Competitive Cybersecurity Multilateralism: From the 2004 UNGGE Through the 2021 OEWG”. Some academic journals where his works have appeared in multiple peer-reviewed English, Japanese, and Korean journals.

# Contact information

E-mail: [info@thehagueprogram.nl](mailto:info@thehagueprogram.nl)

Website: <https://www.thehagueprogram.nl>

 [@TheHagueProgram](#)

 [The Hague Program on International Cyber Security](#)

## *Address*

The Hague Program on International Cyber Security

Faculty of Governance and Global Affairs

Leiden University

Hague Campus

Turfmarkt 99

2511 DP The Hague

## Colofon

Published November 2024.

No part of this publication may be reproduced without prior permission.

© The Hague Program on International Cyber Security/Leiden University.

Graphic design: [www.pauloram.nl](http://www.pauloram.nl)



THE HAGUE  
PROGRAM  
on International  
Cyber Security



이화정치연구소  
EWha INSTITUTE OF POLITICS



Universiteit  
Leiden