Country Focus Report: The Netherlands and the “Public Core of the Internet”

Alexey Trepykhalin and Veni Markovski
28 May 2021
GE-008

TABLE OF CONTENTS

Introduction

This paper covers the national and international Internet-related initiatives undertaken by the Netherlands government. It is part of a periodic series of country-specific reports that provide an overview of activities relevant to the Internet ecosystem and ICANN's mission. Monitoring such initiatives demonstrate the commitment and responsibility of the ICANN organization's (ICANN org) Government and Intergovernmental Organizations Engagement (GE) team in keeping the broader ICANN community informed about issues of importance for the global, single, interoperable Internet and its unique identifier system.[1]

As in previous GE papers, the analyses are based on primary source texts related to Internet policies and technologies, such as the Domain Name System (DNS), Internet Protocol (IP) addresses, and protocol parameters, among others. Additionally, this paper relies on relevant texts and statements about positions of the Netherlands government on the same issues at the United Nations (U.N.). This ensures that the ICANN community has the necessary information to develop a better understanding of the deliberations taking place at the U.N.

Finally, this paper focuses on one term promoted by the Netherlands in private and public spaces – the "public core of the Internet." At the U.N., this term is used as part of the contributions made by the Netherlands to the United Nations General Assembly Open-Ended Working Group in the field of information and telecommunications in the context of international security (OEWG).[2,3]

Background: The "Public Core" Through the Years

In the last few years, the term "public core of the Internet" has been referenced several times in different settings. What follows are only selected examples of its use.

In 2015, the Netherlands Scientific Council for Government Policy presented to the Dutch Minister for Foreign Affairs, Bert Koenders, a report titled, "The Public Core of the Internet."[4]

In 2016, the Dutch Ministry of Foreign Affairs conducted a consultative workshop with members of technical and non-profit communities. During the workshop, the following was

[1] "ICANN Operating and Financial Plans," p. 47, ICANN organization, December 2020, https://www.icann.org/en/system/files/files/draft-op-financial-plan-fy21-25-opplan-fy21-20dec19-en.pdf
[2] "Kingdom of the Netherlands' response to the pre-draft report of the OEWG," General Assembly established an Open-Ended Working Group (OEWG), 2020, https://front.un-arm.org/wp-content/uploads/2020/04/kingdom-of-the-netherlands-response-pre-draft-oewg.pdf
[3] Netherlands' position paper on the UN Open-ended Working Group "on Developments in the Field of Information and Telecommunications in the Context of International Security" and the UN Group of Governmental Experts "on Advancing responsible State behavior in cyberspace in the context of international security" U.N. Open-ended Working Group, February 2020, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/letter-to-chair-of-oewg-kingdom-of-the-netherlands.pdf
[4] Broeders, Dennis, "The Public Core of the Internet. An International Agenda for Internet Governance," the Netherlands Scientific Council for Government Policy, January 2015, https://english.wrr.nl/publications/reports/2015/10/01/the-public-core-of-the-internet

stated: “protection of the public core was defined as the protection of the general availability of the core forwarding and naming functions of the global internet.”[5]

The Netherlands introduced this term to the 2016 – 2017 U.N. Group of Governmental Experts (GGE).[6] As the GGE did not issue a consensus report, it is unknown if the term would have made it into the final text.[7]

In 2017, the Dutch government supported the establishment of a private entity called the Global Commission on Stability in Cyberspace (GCSC).[8] In 2018, the GCSC published a definition which stated that the phrase “the public core of the Internet” includes “such critical elements of the infrastructure of the Internet as packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, transmission media, software, and data centers.”[9]

In 2017, the Netherland’s Ministry of Foreign Affairs outlined an international cyber strategy, which recognized that “given the nature of cyberspace and our dependence on it, it is necessary to exercise restraint when engaging in activities that can affect that public core.”[10] At the same time, this strategy also acknowledged that “to the greatest possible extent, the responsibility for maintaining and cultivating this public core should fall to the technology community, with the state playing a supporting role.”

During 2017 and 2018, a working group of the GCSC conducted a survey of experts on communications infrastructure and cyber defense “to assess which infrastructures were deemed most worthy of protection.”[11] As a result, the GCSC defined the “public core” as the “packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, and physical transmission media” (See Appendix III).[12]

In 2019, members of the GCSC introduced the term “public core” at the ICANN64 and ICANN65 meetings, in Kobe and in Marrakech, respectively. The term was first discussed in Kobe at a meeting of the Internet Service Providers and Connectivity Providers Constituency

---

[5] Broeders, Dennis, “Aligning the International Protection of ‘the Public Core of the Internet’ with State Sovereignty and National Security, Journal of Cyber Policy, Volume 2, Issue 4, November 2017, p. 369, https://www.researchgate.net/publication/321237654_Aligning_the_international_protection_of_'the_public_core_of_the_internet'_with_state_sovereignty_and_national_security

[6] “Group of Governmental Experts,” U.N. Office of Disarmament, May 2021, https://www.un.org/disarmament/group-of-governmental-experts/

[7] “Fact Sheet: Developments In the Field of Information and Telecommunications in the Context of International Security,” U.N. Office of Disarmament, July 2019, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf

[8] “Launch of Global Commission on the Stability of Cyberspace”, Global Commission on Stability of Cyberspace, 18 February 2017, https://cyberstability.org/news/launch-of-global-commission-on-the-stability-of-cyberspace/

[9] “Definition of the Public Core, to Which the Norm Applies,” Global Commission on Stability in Cyberspace, May 2018, https://cyberstability.org/wp-content/uploads/2018/07/Definition-of-the-Public-Core-of-the-Internet.pdf

[10] Ministry of Foreign Affairs, “Building Digital Bridges. International Cyber Strategy. Towards an Integrated International Cyber Policy.” Letter to the Parliament, 2017, https://www.government.nl/documents/parliamentary-documents/2017/02/12/international-cyber-strategy

[11] Louk Faesen, “Call to Protect the Public Core of the Internet,” Global Commission on the Stability of Cyberspace, December 2017, https://cyberstability.org/category/front/

[12] “Definition of the Public Core, to Which the Norm Applies,” Global Commission on Stability in Cyberspace, May 2018.

(ISPCP) of the Generic Naming Supporting Organization (GNSO).[13] Also, that same year, in Marrakech, the GCSC introduced its draft report to the broader Internet community as part of its outreach efforts. At the Marrakech meeting, the representative from the United Kingdom to the ICANN Governmental Advisory Committee (GAC) alerted the GCSC that "by introducing a term like the public core, which is not well understood or difficult to define, we may be causing more problems."[14]

Usage of the Term "Public Core" in Cyber-Related Discussions at the United Nations[15]

In 2020, the term "public core" appeared in some of the documents published on the official OEWG web page.[16]

In the first version of the Chair's pre-draft report, the term is found in point 38: "States, during discussions and through written submissions, also proposed suggestions for the "upgrading" as well as further elaboration of norms. Proposals included, inter alia, that States should affirm their commitment to international peace and security in the use of ICTs; that it should be reaffirmed that States hold the primary responsibility for maintaining a secure, safe and trustable ICT environment; that the general availability or integrity of the public core of the Internet should be protected[...]."[17]

In the second version of the Chair's revised pre-draft report, the term can be found in point 42: "States also made proposals for the enhancement as well as further elaboration of norms. Such proposals included, inter alia, that States affirm their commitment to a culture of restraint and to international peace and security in their use of ICTs; that States reaffirm their primary responsibility for maintaining a secure, safe and trustable ICT environment; that the general availability or integrity of the public core of the Internet should be protected[...]." [18]

In its February 2020 contribution to the OEWG, the Netherlands suggested that protecting the public core should be considered by both the OEWG and the GGE.[19] Several other

[13] "Transcription from the ISPCP Meeting," ICANN organization, March 2019, at 15:15 JST, (p. 22-23, 26), https://gnso.icann.org/sites/default/files/file/field-file-attach/transcript-gnso-ispcp-12mar19-en.pdf
[14] "GAC: Joint Meeting with the Global Commission on the Stability of Cyberspace (GCSC)," ICANN organization, 27 June 2019, (starts at 22:39), https://icann.zoom.us/recording/share/yW2zWMtn2QzqJTmj0u3sh-zWa6-FuQel7V72gUoFfaewIumekTziMw?startTime=1561633270000
[15] Before explaining where and how the term is being used at the different U.N. deliberations, it is important to point out that while this term exists in some legislation and policy, such as the Netherland's International Cyber Strategy or the EU Cybersecurity Act, the U.N. does not have the practice of taking texts from national laws and regulations and using them directly in their outcome documents.
[16] Open-Ended Working Group, U.N. General Assembly, May 2021, https://www.un.org/disarmament/open-ended-working-group/
[17] Chair's pre-draft report, March 2020, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-Pre-Draft-OEWG-ICT.pdf
[18] Chair's pre-draft report, May 2020, https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf
[19] "Netherlands' position paper on the UN Open-ended Working Group "on Developments in the Field of Information and Telecommunications in the Context of International Security" and the UN Group of Governmental Experts "on Advancing responsible State behavior in cyberspace in the context of international security," Open-Ended Working Group, U.N. General Assembly, March 2020,

member states also mentioned the term in their submissions, among them Germany, Switzerland, and the EU.[20,21,22] It was also mentioned in contributions by other stakeholders such as 12 non-governmental organizations, Microsoft Corporation, Global Partners Digital, and the Internet Society.[23,24,25,26,27] The latter gave this definition: "the Internet's public core encapsulates the Internet routing, naming and numbering systems (the Domain Name System), security and identity cryptography mechanisms, and communications cables."

The use of the term has not been universally supported. China, for example, expressed doubts that the term should be in the Chair's report, stating: "Given the limited amount of time we have, attention should also be drawn to avoid introducing concepts that have not gained global consensus yet ("public core" for instance) into the report."[28]

In March 2020, a non-paper quoted the specific language proposal by the Netherlands: "State and non-state actors should 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**,** [would be] guidance for implementation of UN GGE 2015 recommendation 13(f) and therefore bringing this also under the scope of UN GGE 2015 recommendation 13(g)."[29]

---

https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/letter-to-chair-of-oewg-kingdom-of-the-netherlands.pdf

[20] "Initial 'Pre-Draft' of the Report of the OEWG On Developments in the Field of Information and Telecommunications in the Context of International Security and Non-Paper Listing Specific Language Proposals Under Agenda Item 'Rules, Norms and Principles' From Written Submissions Received Before 2 March 2020," Comments from Germany, Open-Ended Working Group, U.N. General Assembly, April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/20200401-oewg-german-written-contribution-to-pre-draft-report-1.pdf

[21] Ambassador Nadine Olivieri Lozano, "Letter to the Chair of the UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security," Open-Ended Working Group, U.N. General Assembly, 9 April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/20200409-switzerland-remarks-oewg-pre-draft.pdf

[22] "Joint Comments from the EU and its Member States on the Initial 'Pre-Draft' Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunication in the Context of International Security," Open-Ended Working Group, U.N. General Assembly, May 2020, https://front.un-arm.org/wp-content/uploads/2020/05/eu-contribution-alignments-oewg.pdf

[23] Civil Society Perspectives on the "Initial Pre-Draft of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security," Open-Ended Working Group, U.N. General Assembly, April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/cs-coordination-perspectives-on-oewg-pre-draft.pdf

[24] "Global Partners Digital response to the pre-draft," Global Partners Digital, March 2020, https://front.un-arm.org/wp-content/uploads/2020/04/oewg-pre-draft-gpd-response-final.pdf

[25] "Microsoft's contribution to draft OEWG report on cybersecurity," Microsoft Inc., April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/microsoft-response-to-draft-oewg-report.pdf and

[26] Internet Society's response to the initial pre-draft report of the OEWG: https://front.un-arm.org/wp-content/uploads/2020/04/internet-society-response-pre-draft-report-of-oewg-04-14-20-en.pdf

[27] "Protecting People In Cyberspace: The Vital Role Of The United Nations In 2020," Microsoft Inc., April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/protecting-people-in-cyberspace-december-2019.pdf

[28] "China's Contribution to the Initial Pre-Draft of OEWG Report," Open-Ended Working Group, U.N. General Assembly, April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf

[29] "Non-Paper Listing Specific Language Proposals Under Agenda Item "Rules, Norms and Principles" From Written Submissions Received Before 2 March 2020," OEWG, March 2020, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-OEWG-ICT-non-paper.pdf

In December 2020, during the informal "Multi-stakeholder Cyber Dialogue to support the ongoing discussion at the UN Open-Ended Working Group (OEWG) on developments in the field of information and communication technology (ICT) in the context of international security," representatives from the GCSC and ISOC further explored the feasibility of using the term "public core."[30]

On 19 January 2021, the OEWG published the *Zero Draft Report*, in which the term "public core" was not mentioned.[31] The same occurred in the *First Draft Report*, published on 1 March 2021.[32]

From 8 to 12 March 2021, the OEWG held its third substantive session, during which the Netherlands delegation suggested the following corrected language about the public core in the *Zero Draft Report:*

"In line with the text on the protection of the public core that was included in the pre-draft, taking into account the convergence on the exact wording, we propose the following. We would like to propose to change the formulation in the last sentence of paragraph 21 on 'integrity, functioning and availability' to the [necessity of protecting] "the technical infrastructure essential to the general availability or integrity of the internet". This holds for para 50 as well. Additionally, we would like to mention the importance of the "protection of the technical infrastructure essential to the general availability or integrity of the internet" under the conclusion/recommendation section of *rules, norms and principles* as well."[33]

Other countries supported the Netherlands position, both orally and in written contributions during the session, with the United Kingdom noting: "We extend our thanks to the Netherlands for working with us and others to refine their proposal on the 'public core' and welcome the inclusion of the compromise text."[34]

On two occasions, there were separate hour-and-a-half long informal virtual OEWG multistakeholder exchanges, during which member states heard opinions by other stakeholders on the content of the First Draft report. Some of these opinions mention the "public core," namely the GCSC comment and statement, which express regret that the term was not included in the consensus report.[35,36,37]

---

[30] "Lets' Talk Cyber: Rules, Norms and Principles," Livecasts, December 2020, (starts at 1:59:00), https://letstalkcyber.livecasts.eu/rules-norms-and-principles

[31] "Draft Substantive Report [Zero Draft]," Open-Ended Working Group, U.N. General Assembly, 19 January 2021, https://front.un-arm.org/wp-content/uploads/2021/01/OEWG-Zero-Draft-19-01-2021.pdf

[32] "Substantive Report [First Draft], 1 March 2020, Open-Ended Working Group, U.N. General Assembly," https://front.un-arm.org/wp-content/uploads/2021/03/210301-First-Draft.pdf

[33] "The Netherlands – Written Proposals to OEWG Zero Draft," Open-Ended Working Group, U.N. General Assembly, February 2021, https://front.un-arm.org/wp-content/uploads/2021/02/Netherlands-OEWG-written-comments-to-zero-draft.pdf

[34] "United Kingdom Comments on the Zero Draft Report," Open-Ended Working Group, U.N. General Assembly, February 2020, https://front.un-arm.org/wp-content/uploads/2021/02/UK-submission-to-OEWG-ICTs-zero-draft-002.pdf

[35] "Contributions by Inter-governmental Organizations (IGOs) and Non-Governmental Organizations (NGOs)", Open-Ended Working Group, U.N. General Assembly, 2020, https://www.un.org/disarmament/open-ended-working-group/

[36] "Comments From the GCSC on the First Draft of the Substantive Report of the U.N. Open-Ended Working Group," Global Commission on the Stability of Cyberspace, 3 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/GCSC-Submission-to-OEWG-First-Draft-Report-March-2021.pdf

[37] "Statement from the GCSC on the Final Draft of the Substantive Report of the U.N. Open-Ended Working Group," Global Commission on the Stability of Cyberspace, 12 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/GCSC-Statement-OEWG-Multistakeholder-Consultation-Final-Draft-Report-March-2021.pdf

In the end, the Final OEWG Report included the following language on that subject, in two points 18 and 26 of the report: [38]

"18. States concluded that there are potentially devastating security, economic, social and humanitarian consequences of malicious ICT activities on critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public. While it is each State's prerogative to determine which infrastructures it designates as critical, such infrastructure may include medical facilities, financial services, energy, water, transportation and sanitation. Malicious ICT activities against CI and CII that undermine trust and confidence in political and electoral processes, public institutions, or that impact the general availability or integrity of the Internet, are also a real and growing concern. Such infrastructure may be owned, managed or operated by the private sector, may be shared or networked with another State or operated across different States. As a result, inter-State or public-private cooperation may be necessary to protect its integrity, functioning and availability."

"26. While agreeing 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, States further concluded that the COVID-19 pandemic has accentuated the importance of protecting healthcare infrastructure including medical services and facilities through the implementation of norms addressing critical infrastructure, such as those affirmed by consensus through UN General Assembly resolution 70/237."

Conclusion

There are some, who see the term "public core" being used not only in the context of the GGE and OEWG, but beyond. For example, one of the GCSC members wrote this about the GCSC public core norm: "This norm has a lot of potential for further elaboration and could be the starting point for drafting a new type of international agreement, fixing rights and responsibilities not only for states but also for non-state actors."[39]

The introduction of a new term such as "public core" in a U.N. document, which "has not gained global consensus"[40], and which has not been defined by the U.N., could open the floor for multiple interpretations and competing definitions as well as providing opportunities for the U.N. and other IGOs to use the term "public core" as a reference in their own work. This, in turn, can expand the competence or scope of the work of these IGOs to include items currently within other multistakeholder entities' missions and remits.

The ICANN org, through its GE team, will continue to provide information to the ICANN community when such statements or proposals touch on the technical governance of the Internet or ICANN's mission.

---

[38] "Final Substantive Report," Open-Ended Working Group, U.N. General Assembly, 10 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[39] Kleinwächter, Wolfgang, "Advancing Cyberstability: Protect the Public Internet Core and Improve Cyber Hygiene," CircleID, November 2019, https://www.circleid.com/posts/20191124_cyberstability_protecting_public_internet_core_and_cyber_hygiene/

[40] "China's Contribution to the Initial Pre-Draft of OEWG Report," Open-Ended Working Group, U.N. General Assembly, April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf

Appendix I
International Cyber Strategy

In 2017, the Dutch government stated that in releasing the *International Cyber Strategy*, it is "fulfilling the pledge it made in its response to advisory reports by the Advisory Council on International Affairs (AIV) ('The Internet: A Global Free Space with Limited State Control') and by the Scientific Council for Government Policy (WRR) ('The Public Core of the Internet')."[41]

In this document, among others, we note the following statements:

- In point 2.4.: "The economic and social advantages associated with the internet require the 'public core' of the internet to function in a reliable, predictable, stable, and safe way. This core possesses elements of an international public good that transcends individual sovereign and private interests. The Netherlands recognises that, given the nature of cyberspace and our dependence on it, it is necessary to exercise restraint when engaging in activities that can affect that public core. To the greatest possible extent, the responsibility for maintaining and cultivating this public core should fall to the technology community, with the state playing a supporting role."[42]

- In point 4.2.: "Given the global public interests associated with the internet, the government is also working to ensure the recognition of the core of the internet as an international public good. The Netherlands recognises that, given the nature and dependence of cyberspace, it is necessary to exercise restraint when engaging in activities that can affect that public core. The Netherlands is working on developing and promoting the acceptance of international norms and rules of conduct, and to that end it has submitted a proposal to the United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security."[43]

[41] Ministry of Foreign Affairs, Netherlands, "Building Digital Bridges, International Cyber Strategy Towards an integrated international cyber policy," Letter to the Parliament, 2017 https://www.government.nl/documents/parliamentary-documents/2017/02/12/international-cyber-strategy

[42] Ministry of Foreign Affairs, Netherlands, "Building Digital Bridges, International Cyber Strategy Towards an integrated international cyber policy," Letter to the Parliament, 2017, point 2.4, principle 4.

[43] Ministry of Foreign Affairs, Netherlands, "Building Digital Bridges, International Cyber Strategy Towards an integrated international cyber policy," Letter to the Parliament, 2017, point 4.2.

Appendix II
Advisory Council on International Affairs (AIV) Report

In its 2014 report, “The Internet: A Global Free Space with Limited State Control,” the Advisory Council on International Affairs (AIV) acknowledged that “the addressing and domain name system, which are of huge commercial importance, must also be regarded as part of internet governance.”[44]

[44] “The Internet: A Global Free Space with Limited State Control,” Advisory Council on International Affairs, November 2014, p. 48, https://www.advisorycouncilinternationalaffairs.nl/documents/publications/2014/12/01/the-internet

Appendix III
Public Core Definition

The following constituent parts (packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, physical transmission media) are further detailed in the GCSC May 2018 Bratislava definition of the public core of Internet: [45]

"**Packet routing and forwarding** include, but are not limited to: the equipment, facilities, information, protocols, and systems which facilitate the transmission of packetized 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 which transport that bandwidth to users. It includes systems needed to assure routing authenticity and defend the network from abusive behavior. 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, standardization, and maintenance processes.
Naming and numbering systems include, but are not limited to: systems and information used in the operation of the Internet's Domain Name System, 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 internationalized 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 standardization processes and outcomes for protocol development and maintenance.
The cryptographic mechanisms of security and identity include, but are not limited to: the cryptographic keys which are used to authenticate users and devices and secure Internet transactions, and the equipment, facilities, information, protocols, and systems which enable the production, communication, use, and deprecation of those keys. This includes PGP keyservers, 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 standardization 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.
Physical transmission media include, but are not limited to: physical cable systems and installations for wired communications serving the public, whether fiber or copper. This includes terrestrial and undersea cables and the landing stations, data centers, and other physical facilities which support them. It includes the support systems for transmission, signal regeneration, branching, multiplexing, and signal-to-noise discrimination. It is understood to include cable systems that serve regions or populations, but not those that serve the customers of individual companies. Some experts believe that far more categories of Internet and ICT-enabled infrastructure are deserving of protection, so this definition may be broadened in the future."

[45] "Definition of the Public Core, to Which the Norm Applies," Global Commission on Stability in Cyberspace, May 2018.