ORF ISSUE BRIEF
JULY 2017
ISSUE NO. 190

Defining the protection of 'the public core of the internet' as a national interest

Dennis Broeders

ABSTRACT The norm to protect the public core of the internet, originally advocated by the Netherlands Scientific Council for Government Policy, can be operationalised in two ways. Both a *layered* approach and a *functional* approach to defining the public core of the internet provide productive ways to discuss safeguarding the functionality and integrity of the core logical and physical infrastructure of the internet from unwarranted state interventions. This brief discusses the tensions between the concept of 'the public core of the internet' and those of state sovereignty and national security. It describes two tiers of objection to the protection of the core internet infrastructure and suggests ways to mitigate them. It concludes that even though there are no easy answers to national security in the cyber age, in the long run, reducing ambiguity in cyberspace will benefit all states. Lifting the public core of the internet out of that ambiguity would be a good starting point.

INTRODUCTION

This brief engages with some of the arguments and discussions about the concept of 'the public core of the internet' and the proposed norm to protect it that were coined in the 2015 report, *The Public Core of the Internet: An International Agenda for Internet Governance* by the Netherlands Scientific Council for Government Policy (Wetenschappelijke Raad voor het Regeringsbeleid or WRR).[1] Since then, this author has debated the concept in various venues and conferences across the world, and can now offer answers to some of the questions and criticisms that have been raised. Section 2 will briefly set out the concept of 'the public core of the internet' as introduced in the WRR report and will highlight how the concept has been taken up in other initiatives and by other public and private actors. Section 3 outlines two modes of operationalising what the public core is or, more accurately, what should be covered by the concept. It describes a layered approach and a functional approach to defining the public core

of the internet. Section 4 deals with two of the main objections to the idea of the public core that this author has encountered in recent debates: the sovereignty objection, i.e., the public core of the internet is part and parcel of the Westphalian world and is not truly global in a legal sense and thus subject to national sovereignty; and the national security objection, i.e., why would states limit their sovereignty by agreeing to a norm of non-intervention when there is no certainty that others will adhere to that norm as well? This brief addresses these objections and offers suggestions to mitigate them. The brief closes with some conclusions in Section 5.

THE PROTECTION OF THE PUBLIC CORE OF THE INTERNET: A CALL FOR NORMS

In March 2015 the Netherlands Scientific Council for Government Policy (Wetenschappelijke Raad voor het Regeringsbeleid or WRR) published a report entitled, *The Public Core of the Internet: An International Agenda for Internet Governance*. This report called for the establishment of an international norm stipulating that the Internet's public core – its main protocols and infrastructure, which are a global public good – must be safeguarded against unwarranted intervention by states. This global public good does not comprise the whole of the internet or even enter into the content layer of the internet but is limited to the logical and physical infrastructural layers of the core internet. It is deliberately a 'lowest common denominator approach' that aims to keep the concept of the public core close to the minimum that is needed to protect the functionality of the internet. This minimalist approach should help secure as much international support for this norm of non-intervention as possible. Support would have to be grounded in a common understanding that safeguarding the integrity and functionality of the core internet is in the interest of all countries that have digitised their economy, government and society. Their common digital vulnerability and need for a functional internet to sustain growth and innovation should underpin their interest in collectively protecting the core of the internet and should transcend their many other political differences in internet-related issues. As every national digital economy, society and government ultimately rests on top of this public core, its functionality and integrity is indispensable for digital survival and growth. The protection of this global public good therefore aligns with the national interest and could be considered an 'extended national interest'.[2] The national interest thus aligns with the protection of the global public good.

Since the WRR report was published, the idea of the public core has gained more traction. In 2016 the Internet Society (ISOC) published a beta version of its Policy Framework for an open and trusted Internet in which it states that the technical community shares "a sense of collective stewardship towards the public core of the Internet and the open standards on which its technologies and networks are based".[3]

Also in 2016, the Global Commission on Internet Governance (or the Bildt Commission) published its final report called *One Internet*, which included a policy recommendation that resonates with the idea of the protection of the public core: "Consistent with the recognition that parts of the Internet constitute a global public good, the commission urges member states of the United Nations to agree not to use cyber weapons against core infrastructure of the Internet".[4] In 2017 the Dutch government made the protection of the public core of the internet a cornerstone of its International Cyber Strategy, as it declared: "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 our

dependence on the internet, it is necessary to exercise restraint when engaging in activities that can affect that public core".[5] The Dutch government has submitted a proposal for such a norm to the deliberations of the 2016-2017 UN Group of Governmental Experts (UN GGE) and aims to pursue the establishment of such a norm in other international fora as well. Most recently, in June 2017, the Global Commission on the Stability of Cyberspace, in some regards the successor of the Global Commission on Internet Governance, held its first full commission meeting in Tallinn and put the issue of protecting the public core of the internet at the top of its research agenda.[6]

FROM CONCEPT TO NORM

The 2015 report did not contain a blueprint of the public core of the internet. While it identified key parts of the logical and technical infrastructure as being part of the core, the report allowed for ambiguity in certain areas. After all, determining what is and what is not covered by the concept will influence the extent to which states and other parties see it as being aligned with their own (national) interests. The more the the concept of the public core is limited to the minimum requirements for the internet to function, the easier it is to get broad political support for a norm of non-intervention. Demarcating the edges of the concept and turning it into language fit for international diplomatic use required consultation with other parties, such as the technical community, civil society and state representatives from various corners of the globe.

In discussions with various stakeholders since publication of the report, two basic approaches emerged to determining what the public core 'is', or better, what is understood to be covered by the concept. The first approach to defining the public core is layered. There are three basic layers – namely, logical, physical and organisational – that have elements that may be considered part of the core:

(1) The logical infrastructure (e.g., TCP/IP, DNS, Routing protocols)

(2) The physical infrastructure (e.g., DNS servers, sea cables)

(3) The organisational infrastructure (e.g., Internet Exchanges, CERTs)

In this approach it is evident that key elements of the logical and physical infrastructure are part of the core of the internet, even when it is less evident where inclusion would stop. TCP/IP, DNS and routing are included even with the most limited definition of the concept. However, other protocols could be considered as well. The physical infrastructure is more complicated due to issues with sovereignty that will be discussed later. The organisational level is also complicated, even though there is some precedent for naming organisations that should be exempt from state interference in the cyber domain. The 2015 UN GGE consensus report emphasised that states should not attack the CERT of another country nor use their own CERT(s) to attack a country.[7] It is a most basic attempt by the participating states to differentiate organisations that are responsible for internet security – i.e., the security and functionality of the internet as a network – from organisations that are responsible for national security.[8] The former may be considered to be part of the public core.

The second approach to defining the public core is functional. Instead of listing what should or should not belong to the public core of the internet, it emphasises what the core of the internet does and stipulates that this should not be interfered with by states. This approach came up during a 2016 workshop that the Dutch Ministry of Foreign Affairs organised to prepare the country's position on the public core of the

internet for the 2016-2017 round of the UN GGE. In this meeting—which included representatives from the technical community and NGOs from various countries of the world—'protection of the public core' was defined as the protection of the general availability and integrity of the core forwarding and naming functions of the global internet.[9] Obviously, this approach does not fully eliminate the necessity to determine what the vital components of the core forwarding and naming functions are, but does facilitate a different conversation about setting a norm to protect that global functionality from unwarranted state intervention.

Lastly, it is worthwhile to note that diplomatic terminology does not always require razor-sharp definitions that are universally ascribed to in order to be useful and successful. Some concepts remain useful even as they are under-defined. For example, the UN GGE uses the term 'critical infrastructure' repeatedly in its 2015 consensus report even though it provides no definition. Moreover, the drafters were undoubtedly well aware of the wide variety among the participating states in what they understand to be critical infrastructure. The concept of the public core of the internet – the global critical infrastructure underlying most national critical infrastructures– could very well function in a similar manner. Getting the concept into diplomatic play may initially be more important than its precise demarcation. The interaction between diplomatic norms and real-life events may also shape the particulars over the course of years.

ALIGNING THE PROTECTION OF PUBLIC CORE OF THE INTERNET WITH SOVEREIGNTY AND NATIONAL SECURITY

The idea of the public core of the internet has been questioned mostly from the perspective of national security. Bringing the global internet 'in line' with the international system of sovereign states is an ongoing process in which national security actors tend to emphasise national sovereignty over (parts of) the internet and downplay its international character and functionality. Even though national security actors usually are not against a functioning internet in itself, there are also pressures and temptations to use the internet in an instrumental way to forward national security goals. As far as national security communities are concerned, the internet is both a source of threat as well as a possibility to build new capabilities for intelligence gathering and warfare. Their interventions on and in the internet can, however, damage the public core of the internet, creating (unforeseen) effects that will damage or compromise the availability and integrity of the core forwarding and naming functions. As such they are considered 'unwarranted interventions by states' that are declared off-limits by the proposed norm for the protection of the public core of the internet.

The rules of the road for state behaviour in cyber space are, however, far from fully crystallised. The fact that the 2016-2017 round of the UN GGE failed to produce a consensus report is a pertinent illustration. The formal point of departure is that international law applies online as it does offline[10] —although reportedly that principle was also a key disagreement in the most recent UN GGE[11]—but that does not cover all real-life situations in cyber space. This is in itself the basis of the norms process: one of its aims is to clarify larger (legal) principles and translate them into rules of the road and confidence-building measures (CBMs). Moreover, the development of cyber norms will be dynamic, they will evolve over time, and the content will differ in various forums. Finnemore and Hollis therefore argue that the norms process is in important ways the product when it comes to cyber norms.[12] This is also true for the protection

of public core that engages with various debates in cyber security and internet governance. Since the publication of the WRR report, the argument for establishing an international norm for the protection of the public core of the internet has been questioned on two related grounds: its tension with sovereignty and its tension with national security. Both objections will be addressed below.

The public core of the internet and the sovereignty objection

The sovereignty objection runs as follows. The widely held idea that the internet is a truly global phenomenon is false as the internet, in the end, consists of cables, server farms and other technical infrastructure that rest somewhere on or under the ground of a sovereign nation. It is territorial. The internet is therefore embedded in sovereign nations, covered by national legal systems; it is not a global public good.

The following is the counter-argument. The public core includes both core logical and core technical infrastructure of the global internet. In the logical layer – the protocols and standards that make naming and forwarding possible – the argument of territoriality does not apply. Protocols and standards are not territorial in any real sense and therefore it would be hard to apply the concept of sovereignty to them. However, at the level of the physical infrastructure, the argument of territoriality does hold for much of the core infrastructure. DNS servers are located within national borders and sea cables come ashore in sovereign nations. The question is whether that means that sovereignty should be applied without any limits on what governments can and cannot do with them.

As these core infrastructures facilitate the flow of global internet traffic, one could argue that intervening in them can have such adverse effects in other countries that it would create obligations for the first state to show restraint. If the United States, for instance, were to turn off all the DNS root servers within its sovereign territory, the repercussions for the global internet would be more than harmful. How this resulting transboundary harm should be characterised in terms of international law or international norms is less clear. It might constitute an international wrongful act if the results violate obligations under international law, such as perhaps the International Telecommunication Union (ITU) provisions on 'avoiding harmful interference' in other signatory states' communication networks and/or the general obligation to 'avoid technical harm to the telecommunication facilities of third countries'.[13] It might also be covered under the notion of the 'no harm principle' that comes from environmental law but may turn out to be applicable in the cyber domain as well,[14] or the notion of due diligence that is still very much under debate in the international law of cyber space.[15] All of these would create an obligation for the state to self-limit its sovereignty with regard to those physical elements of the public core of the internet that are within its territory.

A useful analogy to the organisation of such sovereign self-restraint might be with pooled resources such as rivers. Even though no one disputes that the river Rhine runs through the sovereign territories of Switzerland, Germany, France, Luxembourg and the Netherlands, the application of sovereignty to the water flowing through this river is more problematic. The downstream effects of, for example, dumping toxins into the water are so severe that they have become subject of international norms that aim to govern the joint stewardship of rivers, such as the 2004 Berlin Rules on Water Resources. These lay down rules and restrictions for states in both peace and wartime with regard to internationally shared water resources such as rivers that flow through multiple countries.

Even though the international frameworks are not legally binding,[16] the framework governing the joint stewardship of the Rhine is. Cooperation between the signatory states is laid down in the Convention for the Protection of the Rhine – and administered and overseen by the International Commission for the Protection of the Rhine – and is also covered by the European Water Framework Directive.[17] In other words, states have chosen to set themselves norms that limit their sovereignty in recognition of the fact that the river constitutes an international shared resource. This could be a viable model to mediate between the need to protect the public core of the internet, on the one hand, and the concept of sovereignty on the other.

The public core and the national security objection

The national security objection argues that cyberspace is both a source of threat to national security – for example, hostile actors using the internet and vulnerable critical infrastructures connected to the internet– and at the same time presents an opportunity to build military and intelligence capabilities. High-end military and intelligence capabilities in cyber space give some states a strategic advantage in relation to less advanced nations.[18] Currently, there are no norms prohibiting the build-up of cyber capabilities or the use of the logical and physical core internet infrastructure as a target or a carrier for an attack. It therefore makes perfect sense to build up capabilities in cyber space, and it makes no sense to subscribe a norm of non-intervention when there is no certainty that other states will adhere to such a norm. The state that does limit itself will create its own strategic disadvantage to those states that do not subscribe to the norm, or even those that subscribe to the norm but do not act accordingly. In other words: states that are first movers on such a norm will damage their national security.

The counter-argument is that national security can be threatened in more than one way and that these require different, even contrary, responses. In International Relations theory, the concept of the security dilemma is well known. A security dilemma exists when "many of the means by which a state tries to increase its security, decrease the security of others."[19] And how those others react to their decreased security can, in turn, decrease the security of the first state. In other words, building up offensive capabilities to protect yourself may spiral into an arms race that results in less individual and collective security. In that light it is important to note that cyber conflicts are often considered extremely escalatory conflicts.[20] The potential for a conflict to spin out of control is huge in the cyber domain and this may easily drag countries into a higher level of conflict than intended.

Cyber security lends itself well to the dynamics of the security dilemma. The number of states that are, on the record, building up military cyber capacity is growing steadily and it is safe to assume that not all states are open about their investments, capabilities and intentions. Moreover, many countries will have upgraded their technical cyber capacity considerably within a few years, giving a much larger group of states capacities that are currently reserved for only a few superpowers. What is considered cutting-edge today will be much more commonplace in five years' time. This will add to an already insecure landscape.[21] The blurring of lines between cyber intelligence operations and cyber offensive operations further exacerbates uncertainty and the possibilities to misread the other's intentions.[22] Some authors are therefore talking about the emergence of a cyber security dilemma.[23]

Give these dynamics, it is not surprising that the debate about norms for state behaviour in cyber space goes hand in hand with debate about confidence-building measures to decrease the possibilities for misreading state behaviour.[24]

There are no easy answers to national security in the cyber age, but it seems evident that the risks to national security associated with self-limitation when others may defect from such a norm have to be weighed against the risks of the cyber security dilemma and the escalation of cyber conflict. As Schmitt argues, "legal clarity breeds international stability."[25] Reducing ambiguity in cyberspace – even though it harbours temptations of short-term strategic advantages – is to the benefit of all states. Lifting the public core of the internet out of that ambiguity would be a good starting point.

CONCLUSION

The call to establish an international norm to protect the public core of the internet, as originally advocated by the Netherlands Scientific Council for Government Policy, has been taken up in various forms in different fora. Translating the concept into a viable international norm is an ongoing process that requires specifications of the concept and should also answer some of the objections that have been raised since the report's publication in 2015. This paper proposes two possible approaches to defining the public core of the internet: a layered approach and a functional approach. Both provide productive ways to discuss safeguarding the functionality and integrity of the core logical and physical infrastructure of the internet. However, it is also important to recognise that diplomatic terminology does not always require definitions that are universally ascribed to in order to be useful and successful. The unproblematic and productive use of 'critical infrastructures' in the context of the UN GGE is a case in point.

This paper further discusses two objections to the concept of the public core of the internet from the perspectives of (1) state sovereignty and (2) national security. The sovereignty objection, reasoning that core internet infrastructure is covered by territorial sovereignty and is therefore not global in a legal sense, can be overcome by focusing on potential transboundary harms that may result from interference with the public core and may create obligations for states. The paper discusses the model of the norms and laws for the joint stewardship of rivers such as the Rhine as a way to reconcile the simultaneous territorial and transboundary character of the core of the internet. The national security objection, meanwhile, reasoning that a state that subscribes to a norm that calls for self-restraint when others may not subscribe will damage its national security, has to be meditated by taking into account the parallel risk of an emerging cyber security dilemma. These different risks to national security have to weighed against each other and – given that cyber capabilities are likely to spread to a much larger group of states quite fast – the best route to international stability in the long run will go through increased legal clarity about responsible state behaviour. The route to that legal clarity will have to be paved by a dynamic, multi-forum norms process. ORF

ABOUT THE AUTHOR

Dennis Broeders is a senior Research Fellow at the Netherlands Scientific Council for Government Policy and professor of Technology and Society at Erasmus University Rotterdam, the Netherlands. He is the author of the 2015 report, *The Public Core of the Internet: An International Agenda for Internet Governance*.

ENDNOTES

1. Dennis Broeders, (2015) The Public Core of the Internet. An international Agenda for Internet Governance. (Amsterdam: Amsterdam University Press, 2015). https://english.wrr.nl/publications/reports/2015/10/01/the-public-core-of-the-internet See also Dennis Broeders, "The public core of the internet. Towards an international agenda for internet Governance", Global Policy – Digital Debates (2016): 24-30. http://www.orfonline.org/expert-speaks/the-public-core-of-internet/
2. Broeders, The Public Core of the Internet, 42-43.
3. Internet Society, A policy framework for an open and trusted Internet An approach for reinforcing trust in an open environment, (2016): 7. http://www.internetsociety.org/sites/default/files/bp-Trust-20170314-en.pdf
4. Global Commission on Internet Governance, One Internet, (Ontario and London: Centre for International Governance Innovation and Chatham House, 2016): 75, see also 58. https://www.ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report% 20-%20USB.pdf
5. Government of the Netherlands 'Building Digital Bridges'. International Cyber Strategy. Towards an integrated international cyber policy, (2017): 5. See: https://www.government.nl/documents/parliamentary-documents/2017/02/12/international-cyber-strategy
6. https://cyberstability.org/news/the-global-commission-on-the-stability-of-cyberspace-holds-first-full-commission-meeting-in-tallinn/
7. United Nations, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" July 22, 2015, UN Doc. A/70/174, see p. 8/17 (art. 13k). https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf
8. Broeders, The Public Core of the Internet, 96-99. This is in line with the policy recommendation to disentangle 'internet security' and 'national security'.
9. This international workshop on 'The Public Core of the Internet', was held in The Hague on 11 July 2016.
10. United Nations, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" July 22, 2015, UN Doc. A/70/174. https://ccdcoe.org/ sites/default/files/documents/UN-150722-GGEReport2015.pdf, see also: Michael Schmitt, ed., Tallinn Manual on the International Law Applicable to Cyber Warfare, (Cambridge: Cambridge University Press, 2013). https://www.peacepalacelibrary.nl/ ebooks/files/356296245.pdf
11. Arun Sukumar,"The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?", Lawfare Blog, 4 July 2017, https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well
12. Martha Finnemore and Duncan Hollis, "Constructing norms for global cybersecurity", American Journal of International Law 110(2016): 477. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2843913
13. Anthony Rutkowski,"Public international law of the international telecommunication instruments: cyber security treaty provisions since 1850", Info 13 (2011): 13-31.
14. Scott Shackelford, Scott Russell and Andreas Kuehn, "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors," Chicago Journal of International Law 17 (2016). Available at: http://chicagounbound.uchicago.edu/cjil/vol17/iss1/1
15. For a concise overview on this point see: Michael Schmitt, "Grey zones in the International Law of Cyberspace", The Yale Journal of International Law Online, (2017): 11-13. https://campuspress.yale.edu/yjil/files/2017/05/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1c52av8.pdf
16. See for an overview of the development of the international norms: Salman Salman, "The Helsinki Rules, The UN watercourses Convention and the Berlin Rules: Perspectives on International Water Law", Water Resources Development 23(2007): 625-640. http://www.internationalwaterlaw.org/bibliography/articles/general/Salman-BerlinRules.pdf
17. See: http://www.iksr.org/en/index.html
18. See for example: James Lewis, "Confidence-building and international agreement in cybersecurity", Disarmament Forum (2011): 57-58. http://www.unidir.org/files/publications/pdfs/confronting-cyberconflict-en-317.pdf
19. Robert Jervis, "Cooperation under the Security Dilemma", World Politics 30 (1978): 169.
20. Jason Healey's testimony before the United States House of Representatives Committee on Armed Services Hearing on "Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities" 1 March 2017, http://docs.house.gov/meetings/AS/AS00/20170301/105607/HHRG-115-AS00-Bio-HealeyJ-20170301-U1.pdf
21. Broeders, The Public Core of the Internet, 94.
22. Dennis Broeders, "The hybridization of cyber security governance: the emergence of Global Cyber Security Assemblages", Global Policy – Digital Debates (2017, forthcoming).
23. Myriam Dunn Cavelty, "Breaking the Cyber-security Dilemma: Aligning Security Needs and Removing Vulnerabilities", Science and Engineering Ethics, 20 (2014): 701-715. Ben Buchanon, The Cybersecurity Dilemma. Hacking, Trust, and Fear between Nations. (Oxford: Oxford University Press, 2017).
24. Lewis, "Confidence-building", 57-58.
25. Schmitt, "Grey zones", 21.

ORF OBSERVER RESEARCH FOUNDATION

Ideas • Forums • Leadership • Impact

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-43520020, 30220020. Fax : +91-11-43520003, 23210773.
E-mail: contactus@orfonline.org
Website: www.orfonline.org