Aligning the international protection of 'the public core of the internet' with state sovereignty and national security

Article · November 2017

DOI: 10.1080/23738871.2017.1403640

CITATIONS
2

READS
225

1 author:

Dennis Broeders
Leiden University
47 PUBLICATIONS **741** CITATIONS

SEE PROFILE

Journal of Cyber Policy

ISSN: 2373-8871 (Print) 2373-8898 (Online) Journal homepage: http://www.tandfonline.com/loi/rcyb20

Aligning the international protection of 'the public core of the internet' with state sovereignty and national security

Dennis Broeders

To cite this article: Dennis Broeders (2017) Aligning the international protection of 'the public core of the internet' with state sovereignty and national security, Journal of Cyber Policy, 2:3, 366-376, DOI: 10.1080/23738871.2017.1403640

To link to this article: https://doi.org/10.1080/23738871.2017.1403640

JOURNAL OF CYBER POLICY, 2017
VOL. 2, NO. 3, 366–376
https://doi.org/10.1080/23738871.2017.1403640

Routledge
Taylor & Francis Group

Aligning the international protection of 'the public core of the internet' with state sovereignty and national security

Dennis Broeders

Netherlands Scientific Council for Government Policy and Department of Public Administration and Sociology, Erasmus University, Rotterdam, Netherlands

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. The article further 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.

ARTICLE HISTORY
Received 17 July 2017
Revised 25 September 2017
Accepted 7 October 2017

KEYWORDS
Cyber security; internet governance; the public core of the internet; sovereignty; national security

1. Introduction

This article 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 was laid down in the 2015 report *The Public Core of the Internet: An International Agenda for Internet Governance* by the Netherlands Scientific Council for Government Policy (Broeders 2015). Since then, I have 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. This article draws on the original report, but can be read separately as the main concepts are explained briefly below. The article limits itself to the role of the state in relation to the protection of the public core of the internet. Obviously other actors – such as private companies and other non-state actors – can play a vital role in inflicting damage on or protecting the public core of the internet but they are not the focus of this article.

Section 2 will briefly set out the concept of the public core of the internet as introduced in the 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.

CONTACT Dennis Broeders broeders@wrr.nl

Section 4 deals with two of the main objections to the idea of the public core that I have encountered in recent debates. The first is the sovereignty objection, i.e. the public core of the internet is part and parcel of the Westphalian world, is not truly global in a legal sense and is therefore subject to national sovereignty. The second is 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? Both objections will be addressed and suggestions made to mitigate them. Lastly, Section 5 will draw some conclusions.

2. The protection of the public core of the internet: a call for norms

In March 2015, the Netherlands Scientific Council for Government Policy 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 as close as possible 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. In this sense, the public core debate relates to the internet fragmentation debate. The wide array of forms of internet fragmentation that Drake, Cerf, and Kleinwächter (2016) outline in their overview for the World Economic Forum lists many forms of internet fragmentation that do not interfere with the public core of the internet. Some deeper forms of fragmentation however – such as interference with the root zone or data localisation that require changes in routing protocols – may damage the functioning of the public core. As every national digital economy, society and government ultimately rests on top of the 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' (Broeders 2015, 42–43). The national interest thus aligns with the protection of the global public good.

Since publication, the idea of the public core has gained 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' (ISOC 2016, 8). Also in 2016, the Global Commission on Internet Governance (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' (Global Commission on Internet Governance 2016, 75, see also 58). In 2017 the Dutch government made the protection of the public core of the internet a cornerstone of its International Cyber Strategy:

> 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. (Government of the Netherlands 2017, 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.[1]

3. 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 it limits itself 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 requires 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 with regard to determining what the public core 'is', or better, what is understood to be covered by the concept. Neither of these approaches cast the concept in iron as the technological development of the internet is neither finished nor predictable: it is always possible that new protocols and infrastructures emerge that should be considered part of the public core. The concept requires some degree of flexibility. The first approach to defining the public core is *layered*. There are three basic layers – logical, physical and organisational – that have elements that may be considered part of the core:

(1) The logical infrastructure (TCP/IP, DNS, routing protocols …)
(2) The physical infrastructure (DNS servers, sea cables …)
(3) The organisational infrastructure (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 within 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 (UN 2015, 8, art. 13.k). It is a most basic attempt by the participating states to separate 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 (Broeders 2015, 96–98). 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 Dutch 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.[2] Obviously, this approach does not fully eliminate the need to determine what the vital components of the core forwarding and naming functions are, as it implicitly points towards core naming and numbering protocols (IP and DNS) and routing protocols, such as BGP, and perhaps also the tier one submarine cable infrastructure. This language does, however, facilitate a different conversation about setting a norm to protect that global functionality from unwarranted state intervention.

Lastly, it is worth noting that diplomatic terminology does not always require razor-sharp definitions that are universally ascribed to in order to be useful and successful. Some concepts prove to be useful even if 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.

4. 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 are usually 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. This is the difference between what DeNardis (2012, 726) calls the 'governance *of* the internet infrastructure' in which the interests of the internet as an infrastructure prevail, and 'governance *using* the internet infrastructure', in which national policy goals dominate and the internet infrastructure is considered instrumental towards achieving them. To national security communities, the internet is both a source of threat as well as an opportunity to build new capabilities for intelligence-gathering and warfare. To some extent states already shape the internet into a version that aligns with their political views and interests – the Chinese internet differs from the UK internet – indicating a fragmentation of the world wide web that is mostly located at the content level but is operated through the lower technical levels. However important these modifications are in terms of the political and public sphere on the internet, this 'Westphalianising' of the internet (Demchak and Dombrowksi 2011) does not necessarily damage the public core. Other state 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 cyberspace 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 (Schmitt 2013; UN 2015) – although reportedly that principle was also a key disagreement in the most recent UN GGE (Sukumar 2017) – but that does not cover all real-life situations in cyberspace. 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. Moreover, state interventions in the infrastructure and logical layers of the core internet – sanctioned by declaring cyber the 'fifth domain of warfare' – are in constant development and our guide to understanding the means and methods that states employ in this domain are primarily documents leaked by whistle-blowers and what is revealed through the digital forensics of private cybersecurity companies, academics and NGOs. State programmes, methods and capabilities for operating in cyberspace tend to develop fast and in secrecy. This burdens the norms process with a fast-moving target.

The development of cyber norms will be dynamic and evolve over time, and the exact scope and content will differ in various fora. Finnemore and Hollis (2016, 477), therefore, argue that the norms process *is* in important ways the product when it comes to cyber norms. This also goes for the protection of the public core which engages with several debates in cybersecurity and internet governance. Since publication of the 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.

4.1. 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 rests 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 and as such, is not a global public good.

The counterargument runs as follows. 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. The *distribution* of critical internet resources – IP addresses and domain names, also known as the IANA function – has some elements of being subject to sovereignty as they are formally distributed by ICANN under Californian law, but the operation of the core protocols such as TCP/IP and DNS is not subject to sovereignty. 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. For example, if the United States were for political reasons to force Verisign, the company that operates the root zone, to block an entire top-level domain such as .ir for Iran, the repercussions could be global.[3] Another fictional example would be the Dutch government shutting down the Amsterdam Internet Exchange (AMS-IX) which would have repercussions far beyond Dutch borders. The same would go for the blocking of submarine internet cables that connect the continents – especially since they come ashore in a fairly limited number of countries and locations. The fact that internet topography does not align with national borders implies that hard cuts in core infrastructure – located in a sovereign nation – will usually be felt transnationally.

How the resulting transboundary harms 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 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' (Rutkowski 2011, 18–19). 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 (Shackelford, Russell, and Kuehn 2016), or the notion of due diligence that is still very much under debate in the international law of cyberspace (Schmitt 2017, 11–13). 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 shared 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 to 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 (Salman 2007), 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.[4] 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.

4.2. The public core and the national security objection

The *national security objection* runs as follows. Cyberspace is a source of threat to national security – hostile actors using the internet, vulnerable critical infrastructures, etc. – and at the same time presents an opportunity to build military and intelligence capabilities. High-end military and intelligence capabilities in cyberspace give some states a strategic advantage in relation to less-advanced nations (see for example Lewis 2011, 57–58). 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. Therefore, it makes perfect sense to build up capabilities in cyber space and it makes no sense to subscribe to 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 the first movers on such a norm will damage their national security.

The counterargument is that national security can be threatened in more ways than one 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' (Jervis 1978, 169). 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.[5] 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.

Cybersecurity lends itself well to the dynamics of the security dilemma. The number of states that are on record as 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 from now, 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 (Broeders 2015, 94). The blurring of lines between cyber intelligence operations and cyber offensive operations, further, exacerbates uncertainty and the possibilities for misreading the other's intentions (Broeders 2017). Some authors are, therefore, talking about the emergence of a cybersecurity dilemma (Dunn Cavelty 2014; Buchanon (2017). Given these dynamics, it is not surprising that the debate about norms for state behaviour in cyber space goes hand in hand with the debate about confidence-building measures to decrease the possibilities for misreading state behaviour (Lewis 2011, 57–58).

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 cybersecurity dilemma and the escalation of cyber conflict. As Schmitt argues, 'Legal clarity breeds international stability' (Schmitt 2017, 21). 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.

5. Summary and 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 various 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 publication in 2015. This article 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 article 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 article 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, reasoning that a state that subscribes to a norm that calls for self-restraint when others may not subscribe will damage its national security, should be meditated by taking into account the parallel risk of an emerging cyber security dilemma. These different risks to national security have to be 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.

Obviously, states debating norms in international fora cover only one inroad into the issue of international stability in cyberspace and the protection of the public core. Van Eeten and Mueller (2013) in the context of the academic literature on internet governance noted a preoccupation with official organisations such as ICANN, the Internet Governance Forum (IGF) and the World Summit on the Information Society (WSIS) at the expense of many other structures and venues – such as net neutrality, content filtering, the economics of cybersecurity – where much of the actual governance takes place. Similarly, when it comes to the protection of the public core of the internet the actions and preferences of the corporate world – for example in advocating the use of internet infrastructure for copyright enforcement – and the actions of non-governmental actors – sometimes serving as proxies for states – will also help determine what is possible and impossible. Also, other fora than those sanctioned by the UN system may prove important to test the waters and build much-needed coalitions that are broader than like-minded countries. From a national diplomatic perspective, there is no reason – other than resources – for any state to limit its efforts to enhance stability and security in cyberspace to the usual intergovernmental fora (Broeders 2015, 89–105).

Realistically, states do not just develop norms around a negotiation table. Often norms simply 'emerge' through state behaviour in real life. Especially large and powerful states sometimes send a message of 'do as I say, not as I do' when their diplomatic statements and behaviour are at odds with each other. This underlines both the limitation and the necessity of a norms process. It is limited because norms do not legally bind states. It is necessary because legal norms are not a viable option at this moment and the norms process does create a normative benchmark where previously there was none to challenge state behaviour when it violates a norm. It is inevitably a process of small steps and setbacks. The most recent setback has been the failure of the last round of the UN GGE to deliver a consensus report, leading some commentators to speak of 'the end of an era'.[6] The cyber norms process is broader than the UN GGE, however. The Tallinn Manual Process that focused on the question of how existing international law applies to cyberspace is not a state-run process and is not legally binding. However, if only by being the most solid piece of internationally collaborative thinking that is available on the issue, it does serve as an important benchmark for state and military lawyers and as such shapes the debate. The norms process may develop further at the level of regional international organisations and through the work of independent, hybrid commissions such as the Global Commission on the Stability of Cyberspace that has taken the issue of the protection of the public core of the internet on board, before it resurfaces at the global political level of the UN.

Notes

1. https://cyberstability.org/news/the-global-commission-on-the-stability-of-cyberspace-holds-first-full-commission-meeting-in-tallinn/. The commission at that time also issued a call for proposals on its first research programme on the public core of the interment, calling for reproach proposals on: (1) Defining the Public core of the Internet, (2) Identifying Internet-Accessible Critical Information Infrastructures, (3) Overview of Cyber Diplomatic Initiatives, (4) Overview of Cyber Norms in Theory and Practice and (5) Protecting the Core.
2. This international workshop on 'The Public Core of the Internet', was held in The Hague on 11 July 2016.

3. This would require deep interference with the DNS Root Zone generation and signing process that takes place at Verisign as operator of the root zone. The efficacy of the measure would depend on the pervasiveness of DNSSEC: without pervasive DNSSEC validation, DNS operators might continue to serve stale data. With DNSSEC, stale data would be invalidated at signature expiration time. Regardless, the action would cause the need for various DNS operators across the world to take conscious action to route around such interference.
4. See: http://www.iksr.org/en/index.html
5. 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
6. http://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/

Acknowledgements

The author wishes to thank the two anonymous reviewers and the editorial team for constructive and insightful comments. He also wants to thank Olaf Kolkman (ISOC) for much appreciated help with the argument and language on some of the finer technical details. Any remaining errors are his own.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributor

Dennis Broeders is professor of Technology and Society at the Department of Public Administration and Sociology of the Erasmus University Rotterdam and a senior research fellow at the Netherlands Scientific Council for Government Policy (WRR), an advisory body to the Dutch government within the Prime Minister's department. His research broadly focuses on the interaction between technology, society and policy, with specific areas of interest in cyber security and internet governance, surveillance and Big Data. He is the author of *The public core of the internet. An international agenda for internet governance* (2015, Amsterdam University Press).

References

Broeders, D. 2015. *The Public Core of the Internet: An International Agenda for Internet Governance*. Amsterdam: Amsterdam University Press.

Broeders, D. 2017. "The Hybridization of Cyber Security Governance: The Emergence of Global Cyber Security Assemblages." *Global Policy – Digital Debates* 2017: 38–44.

Buchanon, B. 2017. *The Cybersecurity Dilemma. Hacking, Trust, and Fear Between Nations*. Oxford: Oxford University Press.

Demchak, C., and P. Dombrowksi. 2011. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* 2011 (Spring): 32–61.

DeNardis, L. 2012. "Hidden Levers of Internet Control: An Infrastructure-based Theory of Internet Governance." *Information, Communication and Society* 15 (5): 720–738.

Drake, W., V. Cerf, and W. Kleinwächter. 2016. Internet Fragmentation: An Overview. Future of the Internet Initiative White Paper, January 2016." *World Economic Forum*. http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

Dunn Cavelty, M. 2014. "Breaking the Cyber-security Dilemma: Aligning Security Needs and Removing Vulnerabilities." *Science and Engineering Ethics* 20 (3): 701–715.

Eeten, M. van, and M. Mueller. 2013. "Where Is the Governance in Internet Governance?" *New Media & Society* 15 (5): 720–736.

Finnemore, M., and D. Hollis. 2016. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110 (3): 425–479, see p. 477. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2843913.

Global Commission on Internet Governance. 2016. *One Internet*. Centre for International Governance Innovation and Chatham House. https://www.ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf.

Government of the Netherlands. 2017. "Building Digital Bridges". International Cyber Strategy: towards an integrated international cyber policy. https://www.government.nl/documents/parliamentary-documents/2017/02/12/international-cyber-strategy.

Internet Society. 2016. *A Policy Framework for an Open and Trusted Internet an Approach for Reinforcing Trust in an Open Environment*. http://www.internetsociety.org/sites/default/files/bp-Trust-20170314-en.pdf.

Jervis, R. 1978. "Cooperation Under the Security Dilemma." *World Politics* 30 (2): 167–214.

Lewis, J. 2011. "Confidence-building and International Agreement in Cybersecurity." *Disarmament Forum* 2011 (4): 57–58. http://www.unidir.org/files/publications/pdfs/confronting-cyberconflict-en-317.pdf.

Rutkowski, A. 2011. "Public International Law of The International Telecommunication Instruments: Cyber Security Treaty Provisions Since 1850." *Info* 13 (1): 13–31.

Salman, S. 2007. "The Helsinki Rules, The UN Watercourses Convention and the Berlin Rules: Perspectives on International Water Law." *International Journal of Water Resources Development* 23 (4): 625–640. http://www.internationalwaterlaw.org/bibliography/articles/general/Salman-BerlinRules.pdf.

Schmitt, M., ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press. https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.

Schmitt, M. 2017. "Grey Zones in the International Law of Cyberspace." *The Yale Journal of International Law Online*, 11–13. https://campuspress.yale.edu/yjil/files/2017/05/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1c52av8.pdf.

Shackelford, S., S. Russell, and A. Kuehn. 2016. "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors." *Chicago Journal of International Law* 17 (1): Article 1. http://chicagounbound.uchicago.edu/cjil/vol17/iss1/1.

Sukumar, A. 2017. "The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?" *Lawfare Blog*, July 4 2017. https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

United Nations. 2015. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." July 22. UN Doc. A/70/174. https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf.