WRR

SCIENTIFIC COUNCIL FOR GOVERNMENT POLICY

WRR-Policy Brief 2

The public core of the internet: an international agenda for internet governance

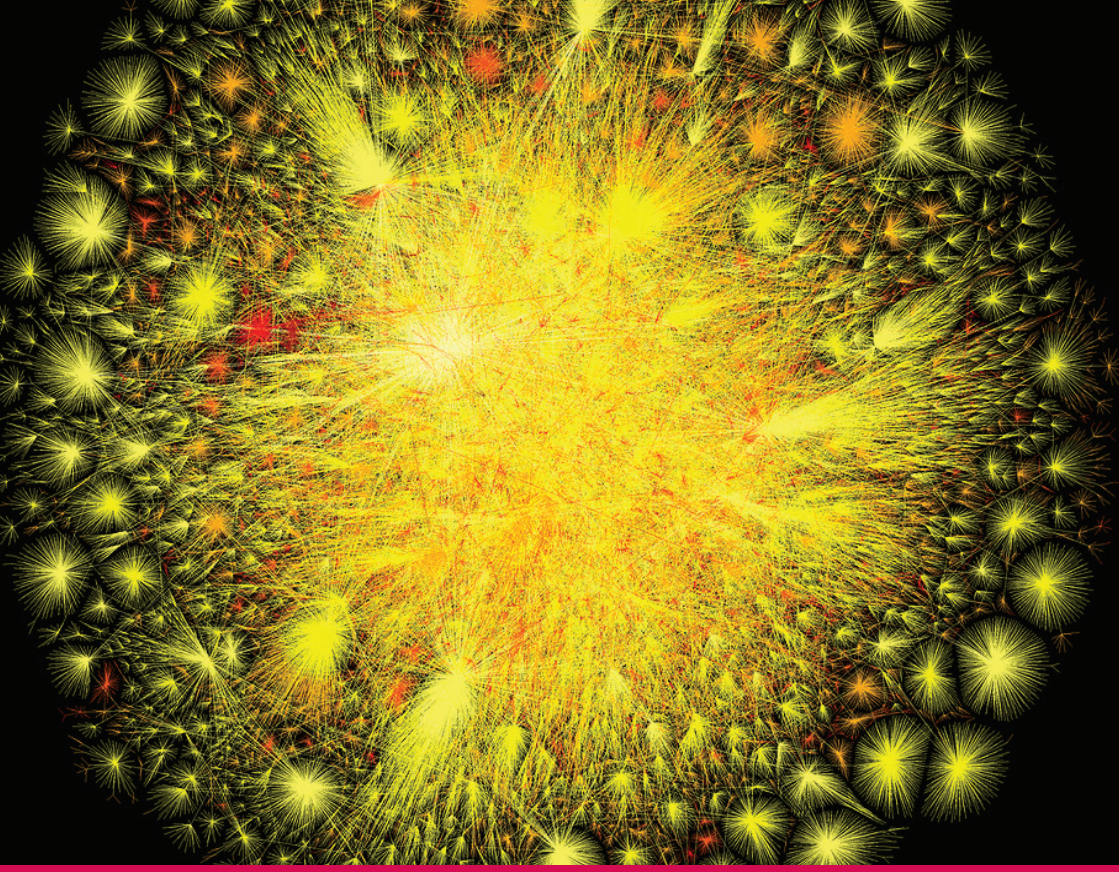
The growth and health of our digital economies and societies depend on the backbone protocols and infrastructure of the internet. This backbone is now in need of protection against unwarranted interference in order to sustain the growth and the integrity of the internet.

Dennis Broeders

Summary

The internet's backbone of key protocols and infrastructure can be considered a *global public good* that provides benefits to everyone in the world. Countering the growing state interference with this backbone requires a new international agenda for internet governance that departs from the notion of a global public good. Core ingredients of this strategy are:

- To establish and disseminate an international norm stipulating that the internet's public backbone – its main protocols and infrastructure– must be safeguarded against unwarranted intervention by governments.
- To advocate efforts to clearly differentiate at the national and international level between internet security (security of the internet infrastructure) and national security (security through the internet) and have separate parties address these different forms.
- To broaden the arena for cyber diplomacy to include new coalitions of states (including the so-called 'swing states') and private companies, including internet giants as well as internet intermediaries such as Internet Service Providers.



The Netherlands Scientific Council for Government Policy (WRR) is an independent advisory body which provides the Dutch government, both on request and on its own initiative, with long-term strategic policy advice on a range of topics. More information on the WRR can be found at www.wrr.nl.

The WRR's Policy Briefs provide reflections on current issues that have long term policy relevance.

April 2015, no. 2
Published by The Netherlands Scientific Council for Government Policy (WRR)
ISSN: 2352-1392

This policy brief is based on the Dutch report *De publieke kern van het internet* that the Scientific Council for Government policy presented to Bert Koenders, Dutch minister of Foreign Affairs, on 31 March of 2015. An international version of this report will be published shortly as: Broeders, D. (2015) *The public core of the internet. An international agenda for internet governance.* Amsterdam: Amsterdam University Press.

Please cite this publication as:
Broeders, D. (2015) *The public core of the internet: an international agenda for internet governance,* WRR-Policy Brief no. 2, April 2015. The Hague: WRR

1

INTERNET GOVERNANCE: BETWEEN THE TECHNICAL AND THE POLITICAL[1]

Everyday life without the internet has become unimaginable. It is rooted in our social lives, our purchasing behaviour, our work, our relationship with the government and, increasingly, with our everyday objects, from smart meters to the automobiles we drive and the moveable bridges that we cross *en route.* The internet is an invaluable source of economic growth and expands the social and cultural horizons of its users. Its openness is a motor behind many industries as well as an industry in itself, and provides opportunities for new interfaces between consumers and producers, citizens and governments and between people on a local, national and global scale. While it is hard to predict what direction the internet will take in the coming years and decades it is safe to say that interconnectedness and interdependence between the online and the offline worlds are likely to remain at the core. This makes the functioning and integrity of the internet as an infrastructure a vital necessity for the future. In turn, this underlines the importance of responsible governance in maintaining the functionality and integrity of the internet.

Internet governance and national interests

For a long time, internet governance was the exclusive domain of what is known in internet circles as the 'technical community'. That community laid the foundations for the social and economic interconnectedness of our physical and digital lives. Those foundations, with the Internet Protocol as the most prominent component, continue to function as the robust substructure of our digital existence. But the governance of that substructure has become controversial. The many economic and political interests, opportunities and vulnerabilities associated with the internet have led governments to take much more interest in the governance of the internet. Moreover, in terms of policymaking, the centre of gravity has shifted from what was primarily an economic approach (the internet economy, telecommunications and networks) to one that focuses more on national and other forms of security: the internet of cybercrime, vulnerable critical infrastructures, digital espionage and cyber-attacks. In addition, a growing number of countries seek to regulate their citizens' online behaviour, their reasons ranging from copyright protection and fighting cybercrime to censorship, surveillance and control of their own populations on and through the internet.

1. The author would like to thank Erik Schrijvers, Lisa Vermeer and Mark Bovens who were part of the project team that drafted the Dutch report on which this policy brief is based.

From governance of the internet to governance using the internet

Increasingly, governments view the backbone infrastructure and main protocols of the internet itself as a legitimate *means* to achieve their policy ends. Whereas internet governance used to mean governance *of* the internet, today it also means governance *using* the architecture of the internet[2]. In that second notion the internet becomes a policy instrument to achieve other (national) policy goals. Such interventions may have huge implications for the backbone of internet infrastructures and protocols and in turn, for the digital lives that we have built on top of it. Such interventions can undermine the integrity and the functionality of the internet. If the internet ceases to operate, many processes and routines, from the trivial – our Facebook status – to the essential – payment transactions – will grind to a halt. If the backbone protocols of the internet are corrupted, the internet becomes unreliable. Who would risk online banking in that case? If we cannot be sure that data will be sent and arrive at its intended destination, that will influence the kinds of economic and social processes that we do or do not entrust to the internet. Would we let the internet handle our private and work-related communications in that case? If we know that security gaps are deliberately being built into internet standards, protocols, and hardware and software to guarantee foreign intelligence and security services access, then our confidence in the internet will gradually crumble. If more and more countries withdraw behind digital borders, the internet will no longer operate as an international infrastructure as it has done so far. And in the worst-case scenario, the exploitation of vulnerabilities in the backbone protocols and infrastructures could lead to serious breakdowns in society and economy.

The internet's backbone as a global public good

This policy brief therefore argues that the backbone of the internet must be regarded as a global public good. As such, it should be protected against the interventions of states that are acting only in their own national interest, thereby damaging that global public good and eroding public confidence in the internet. In that respect, internet governance is at a crossroads: the internet has become so important that states are no longer willing or able to regard it with the same 'benign neglect' that long set the tone for most countries. At the same time, however, states do have national interests that go beyond the governance of the internet as a collective infrastructure. For the future of internet governance it is imperative to determine what part of the internet should be regarded as a global public good – and thus safeguarded from improper interference – and what part should be seen as the legitimate domain of national states, where they can claim a position and take up their role without harming the infrastructure of the internet itself.

2. See DeNardis (2012; 2013; 2014) for an elaboration on this distinction

2

TOWARDS A NEW INTERNATIONAL AGENDA FOR INTERNET GOVERNANCE

Growing state interference with this backbone infrastructure and protocols of the internet underlines the need for a new international agenda for internet governance that begins with the notion of a global public good.

A global public goods approach

The backbone of key protocols and infrastructure can be considered a *global public good*. Global public goods provide benefits to everyone in the world, benefits that can be gained or preserved only by taking specific action and by cooperating. The means and methods for providing a global public good may differ from one case to the next and can be undertaken by private or public parties, or combinations of the two.[3] This can be said to apply to the internet as a network and as an infrastructure. If key protocols like TCP/IP, DNS and routing protocols do not work properly, the internet's very operation will come under pressure. If these protocols are corrupted, everyone loses. The internet is 'broken' if we can no longer assume that the data that we send will arrive, that we can locate the sites we are searching for, and that those sites will be accessible. As a public good, the internet only works properly if its underlying values – universality, interoperability and accessibility[4] – are guaranteed and if it facilitates the main objectives of data security, i.e. confidentiality, integrity and availability.[5] It is vital that we – the users – can rely on the most fundamental internet protocols functioning properly. After all, these protocols underpin the digital fabric of our social and economic life. Our confidence in the integrity and continuity of all we have built on the backbone of the internet – our digital existence - thus very much depends on those underlying protocols.

The risks of national policies that tamper with backbone protocols and infrastructure…

The need for worldwide agreement about the importance of a properly functioning internet backbone seems obvious because it is these protocols that guarantee the reliability of the global internet. Recent international trends in policymaking and legislation governing the protection of copyright, defence and national security, intelligence and espionage, and various forms of censorship, however, show no signs of such agreement. If anything, they show the contrary. Some states see DNS, routing protocols, internet standards, the manipulation and building of backdoors into software and hardware and the stockpiling of vulnerabilities in software, hardware and protocols (so called 'zero days') as ideal instruments for national policies intent on monitoring, influencing and blocking the

3. Van Lieshout, Went and Kremer (2010)
4. See for example DeNardis (2013:4)
5. See for example Singer and Freedman (2014: 35)

conduct of people, groups and companies. The negative impact of such interventions in the backbone of the public internet falls to the collective, however, and impairs the internet' score values and operation. Illustrations of this trend include:[6]

- Various forms of internet censorship and surveillance[7] that use key internet protocols as well as enlisting the 'services' of internet intermediaries such as Internet Service Providers (ISPs) to block and trace content and users.[8]
- The transition of the so-called IANA-function, that includes the stewardship and maintenance of registries of unique Internet names and numbers. The debate on this transition may result in a more politicised management of the Domain Name System, which may have repercussions for finding and locating sites and users.[9]
- The online activities of military cyber commands, intelligence and security services, and sometimes even law enforcement agencies which undermine the proper functioning of the public core of the internet.[10] By corrupting internet standards and protocols, by building backdoors into commercial hardware and software and by stockpiling zero-day vulnerabilities these actors effectively damage the collective internet infrastructure and make it less secure. Moreover, they create a digital version of the 'security dilemma',[11] in which the use of cyberspace as an instrument for national security, in the sense of both cyber warfare and mass surveillance by intelligence services, undermines the overall level of cyber security on a global scale.[12]
- Legislation to protect copyright and intellectual property that permits the use of vital internet protocols to regulate and block content. 'Side-effects' of such legislation include the collateral blocking of content and users ('over blocking'), damage to the DNS and intermediary censorship through ISPs.[13]
- Some forms of internet nationalism and data nationalism – in which states seek to fence off a national or regional part of the internet – that require interventions in routing protocols. In extreme forms this may splinter the internet.[14]

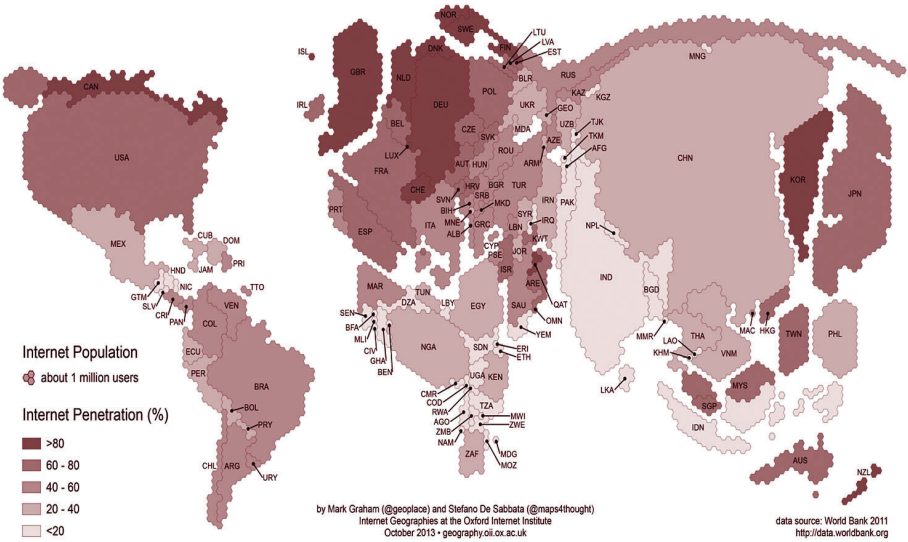
---

6. For a fuller discussion of these trends see Broeders (2015, especially chapters 3 and 4).
7. For the development of state censorship see: Deibert et al. (2008, 2010, 2011), DeNardis (2014, chp. 9).
8. See Zuckerman (2010) MacKinnon (2011); Benkler (2011); Van Eeten et al. (2014)
9. Mueller (2010); Zittrain (2014); Mueller and Kuerbis (2014)
10. Landau (2010, 2014); Rid (2103); Ablon et al.(2013); Greenwald (2014); Van Hoboken and Rubinstein (2014); Singer and Friedman (2014); Stockton and Golabek-Goldman (2014); Fidler (2014).
11. Jervis (1978)
12. Dunn Cavelty (2014)
13. Zittrain and Palfrey (2008); Mueller (2010); Lemly et al. (2011); Yu (2012, 2014); Masnick (2014)
14. See Maurer et al. (2014); Chander and Le (2015), although they see problems with almost all forms of data nationalism, not just those that require blocks in routing protocols.

…in a demographically and geopolitically changing internet

A number of powerful states have built up significant cyber capacity and are ahead of the rest in this trend. But many countries are now in the midst of digitising their state, economy and society and are building cyber capacity. Moreover, the internet is undergoing a demographic shift in which the centre of gravity is moving from the North and West to the East and South of the planet.[15] Figure 1 shows worldwide internet penetration and the regions where there is the most room for growth. The lighter the colour, the more potential for an increase in the number of internet users.

Figure 1 Internet users and internet penetration worldwide, 2011[16]



This shift has major consequences for the balance of power on the internet and how cyberspace is viewed culturally and politically. When the next billion (or billions) of users go online in the years ahead, these emerging states will develop their own national policies in relation to the online world and will have to ask themselves whether or not they will use the public backbone of the internet instrumentally in those efforts. Some of these countries

15. Deibert (2013b), see also Choucri (2012)
16. Source: Graham (2014)

have authoritarian regimes with a history of controlling and sometimes repressing their own population, and using modern technology to do so. There is no guarantee that these countries will spare the internet's public backbone as their societies continue to digitise. In addition, many countries will have upgraded their technical cyber capacity considerably in a few years, giving a much larger group of states the capacities that are currently reserved for only a few superpowers. What is cutting edge now will be common in five years' time. If in that same time the idea takes hold that national states are at liberty to decide whether or not to intervene in the internet's main protocols to secure their own interests, the impact on the internet as a public good is likely to be very damaging. For this reason there is no time to lose in securing the public backbone of the internet.

The internet's backbone should be an international neutral zone

Given these developments it should be an internationally shared priority to work towards establishing an international norm that identifies the main protocols of the internet as a neutral zone in which governments are prohibited from interfering for the sake of their national interests. This should be considered an extended national interest,[17] i.e. a specific area where national interests and global issues coincide for all states who have a vital interest in keeping the internet infrastructure operational and trustworthy. With the continuing spread of the internet and ongoing digitisation that is increasingly a universal concern.

- In order to protect the internet as a global public good there is a need to establish and disseminate an international standard stipulating that the internet's public backbone – its main protocols and infrastructure, which are a global public good – must be safeguarded against intervention by governments.

The starting point should be to place the drafting of such a standard on the international political agenda, something that will require making governments around the world aware of the collective and national importance of this neutral zone. Given the enormous differences between countries in terms of internet access, overall digitisation and technological capacity, this will require a serious diplomatic and political effort. This standard could be disseminated through relevant UN forums as well as though regional organisations such the Council of Europe, the OECD, the OSCE, ASEAN and the AU. This strategy would lay the foundations for what could eventually expand into a broader regime.

17. Knapen et al. (2011)

Securitisation and internet governance

Given the rising conflict between national security and internet security there is a need to separate and disentangle the various forms of security relating to the internet. The increased emphasis on national security has had a negative impact on the debate on cyber security. Some researchers maintain that cyber security and cyber warfare have become part of a 'securitised' discourse.[18] Many governments are seriously investing in capacity building in the realm of national and international cyber security in response to what is a relatively poorly defined threat. The term 'threat inflation' is often used to explain the rapidly expanding cyber security budgets and legislative powers, especially in the United States.[19] This could lead to a far-reaching militarisation of the cyber domain[20], the rise of a new cybermilitary-industrial complex[21] and even an arms race in cyberspace.[22] This in spite of the fact that initial attempts to study how the law of armed conflict applies to cyberconflicts, such as the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, show that so far, not a single cyber incident conforms to the legal definitions of 'war'.[23]

The need to disentangle internet security and national security

The emphasis on national security comes at the expense of a broader range of views on security and the internet. Defining and disentangling various views on security may in fact improve the security of the internet as an infrastructure.

- It is therefore vital to advocate internationally for a clear differentiation between internet security (security of the internet infrastructure) and national security (security through the internet) and to disentangle the parties responsible for each.

It is of paramount importance to delineate the various forms of security in relation to the internet. On one end of the spectrum there is the notion of internet security, i.e. ensuring that the network itself is secure and operational. On the other end, there is the notion of national security, with the focus on the state and the internet being regarded simultaneously as a source of threat *and* as a potential policy tool. Between the two ends of the spectrum is a view that focuses more on cybercrime and has law enforcement as the primary national, regional and international actors. Across the entire spectrum, private parties also play

18. Hansen and Nissenbaum (2009); Dunn Cavelty (2013); Singer and Friedman (2013)
19. Libicki (2012); Lin (2012); Rid (2013)
20. Libicki (2012); Dunn Cavelty (2012)
21. Brito and Watkins (2012); Deibert (2013b)
22. Nye (2011)
23. Schmitt (2013); AIV/CAVV (2011); see also Rid (2013)

various roles: as developers and suppliers of technology, as businesses that protect their own networks, and as consultants that implement 'security' on or by means of the internet, for clients ranging from Shell to the NSA.

Let CERTs be CERTs

Internet security relates to a technology-driven strategy, such as those of the Computer Emergency Response Teams (CERTs) that involves a public health-type approach to overall network security. The aim is to maintain the health of the internet as a network for the benefit of all users.[24] Trust, a shared understanding of network security and information-sharing have been key ingredients contributing to the gradual growth of international cooperation between the various CERTs. It is important not to confuse and/or mix this logic with that of national security, which places national interests above network interests. Importantly, a strict division is required between the actors responsible for national security, such as the military and the intelligence and security services, and parties such as the CERTs that safeguard the security of the internet itself. Confusing the two logics, or letting the second dominate, could seriously impair the mutual trust that the technical community has managed to build over the course of many years. These two forms of security must remain separate, even in periods when the security of the online and offline world is under threat. Nor should they be mixed under the pressure of budgetary restraints and a scarcity of qualified computer experts that is felt by various government agencies active in the broader field of cyber security.[25]

A route to establishing international norms in cyberspace

The process of debating the highest levels of national security – military cyber commands and intelligence and security services – is both the most crucial and the most complicated from the perspective of restraining government behaviour.[26] Considerations of state sovereignty make regulating these actors through international law or agreements a highly complex affair. There are, of course, various initiatives underway to arrive at international norms, but these are mainly set within the context of international security and are intended to prevent escalation between states. The Groups of Governmental Experts (GGEs) and other initiatives of this kind emphasise codes of conduct and Confidence-Building Measures that are meant to prevent states from misinterpreting each other's conduct online.[27] A clear division between different forms of security and the demarcation of the domains of the

24. See for example the Cyber Green Initiative: JPCERT/CC (2014)
25. Broeders (2014)
26. Deibert (2013a)
27. Kane (2014); Hurwitz (2014)

various actors involved could help these ongoing international deliberations about standards in cyberspace. A new norm declaring unwarranted intervention in the internet's public backbone out of bounds would also help to disentangle the various forms of security, some of which support the integrity of the public backbone – internet security – while others such as national security employ instruments that in fact damage it.

3 BROADENING THE DIPLOMATIC ARENA

The demographic shift in engagement with the internet and the rise of new big and mid-level powers in internet affairs challenges the still very dominant transatlantic take on internet governance. A recent report by the Council on Foreign Relations called on the US government to make this new reality the basis for its foreign cyber policy: 'The United States can no longer rely on its role as progenitor of the internet to claim the mantle of leadership'.[28] The Snowden revelations have caused that mantle to slip further by undercutting the US's moral leadership in internet matters. By extension, the 'Western' voice is seeing its dominance in the debates about internet governance challenged. It is therefore time to open, broaden and expand the arena for cyber diplomacy. There is a need to involve states that are still building their technical and political cyber capacities – for example the so called 'swing states'[29] – integrally in debates about internet governance. Secondly, there is a strong case to be made for targeting the big internet-based companies as explicit subjects of cyber diplomacy as well as a need to think through and regulate what the role and position of intermediary organisations on the internet – such as Internet Service Providers (ISPs) – is and should be.

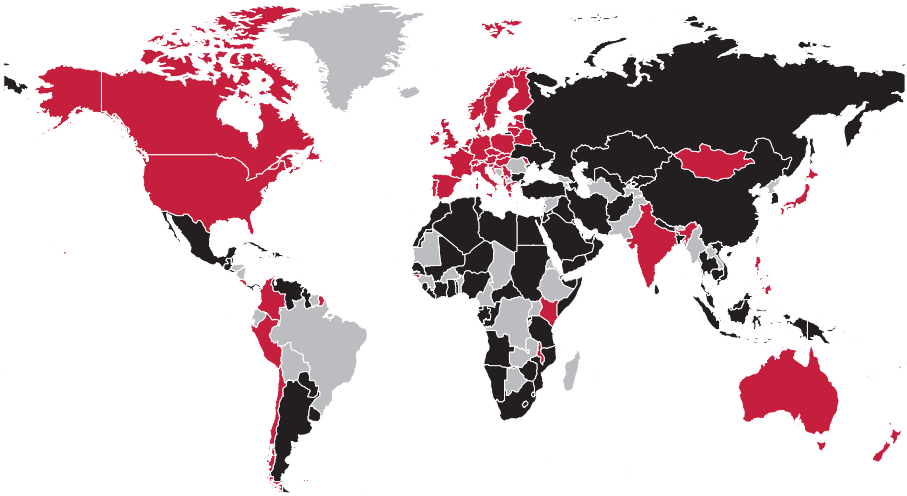
The need to build new coalitions…

The challenge for internet governance is how to build new, broad coalitions that are willing to support a standard that protects the internet's backbone. While the 'usual suspects' in the transatlantic axis, i.e. the EU and the OECD, are still important actors in internet governance, the bigger challenge lies elsewhere. The conversation between 'like-minded' allies will help to bring the desired standards and norms into focus, but the real impact in this arena will come from dialogue with states that are outside that circle.[30] That became clear during the 2012 World Conference on International Telecommunications in Dubai, when it came time to vote on the International Telecommunications Regulations (ITRs).

28. Council on Foreign Relations (2013: 67)
29. See Maurer and Morgus (2014)
30. Hurwitz (2014: 330)

The Western camp found itself in the minority when its members voted against new ITRs that would increase state influence over the internet and could open the door to its nationalisation, or balkanisation. Some 89 states, including China, Russia and many Arab nations, voted in favour while 55 others, including the member states of the EU, the US and most members of the OECD, did not sign. In figure 2 – based on ITU data - the opposing countries are coloured red and those in favour of the new ITRs are coloured black. The votes of the countries in grey were not formally registered due to outstanding membership fees.

Figure 2 Voting results on the ITRs, WCIT, Dubai 2012[31]



…by addressing the political middle ground

In diplomatic terms it is clear that there is much to be gained by engaging with the large group of countries that have not yet taken up a firm position on various issues of internet governance. These 'swing states' or 'fence sitters' are still developing their strategy, policies and capacity to engage with internet governance issues, especially at the international level. Diplomatic efforts focused on securing the public backbone of the internet will only succeed through effective engagement with these states, which could represent a political middle ground between the two extremes in the discussion. Maurer and Morgus[32] identified a top

31. Source: Techdirt.com
32. Maurer and Morgus (2014)

thirty of swing states worldwide by combining the voting results for the new international telecommunications treaty with a broad range of criteria, including membership of international organisations and degree of democratisation. They also looked at internet penetration, the presence of an active internet community, and the size of the digital economy. These swing states are neither the 'like-minded' states of the 'Western camp' nor the 'other-minded' states with repressive and dictatorial regimes. Nor are they very small states or states with few resources that are considered to have little influence. As such they are an important starting point for building new coalitions and broadening existing ones. It should also be noted that the digital superpowers of today – at least in terms of numbers of internet users – will not necessarily be the superpowers of tomorrow. The southward and eastward demographic shift that is unfolding in cyberspace underlines the importance of involving the swing states in the diplomatic effort to establish the norm that it is in the interest of *all* countries not to interfere with the internet's public backbone.

Private companies as part of the diplomatic dialogue

In the predominantly privately owned and run world of the internet, Apple, Google, Microsoft and other corporate giants are forces to be reckoned with. It is they who largely decide what our online lives look like and what new directions the information society will take. This also means that, more than in the past, these corporations should be approached from the perspective of diplomacy and the rule of law. This is a matter of power and counter-power, and – as in diplomatic relationships between states – the interests and agendas of such corporations will sometimes align and sometimes conflict with national and collective interests. For example, it is not clear why most Western countries maintain dialogues about human rights with authoritarian regimes but not with companies that are vital to the protection of privacy and freedom of communication around the world.[33]

Private power and government counter-power

Given that large internet companies are powerful and influential actors in internet governance they should be much more explicitly part of the diplomatic arena. Relevant issues include privacy and data protection, market dominance, the security of hardware and software, and data protection by means of encryption. Many governments are relatively weak parties in their dealings with these private-sector giants, for reasons of size and resources and also because of economic interests and dependencies in relation to these corporations. Regional organisations such as the EU sometimes take a stand. But even though the EU's political force is considerable, its gears grind slowly compared to the fast-paced internet economy. That much became clear in the infamous case that the European

33. AIV (2014)

Commission brought against Microsoft under EU competition law. While the fine was high and proportional (USD 860 million), the proceedings took so long that it was tantamount to 'solving the antitrust problem long after the competitors have died'.[34] Nevertheless, the authority to levy heavy sanctions – which is also part of the current negotiations with regard to the EU data protection regulation - gives the EU and its member states more muscle in their dialogue with these companies. The 'shadow of hierarchy' can be an important incentive for private parties to engage in serious dialogue with states.[35]

Government power and private counter-power

Recently, there has been informal pushback from internet companies against governments, and against the US in particular. Much of it has been driven by the Snowden revelations, which have seriously damaged the reputation of a number of leading American internet companies among internet users. Snowden's files put a number of the big internet-based companies on the spot as they were - intentionally or unintentionally - the sources of masses of data collected by the intelligence services. These companies are now responding by issuing transparency reports that disclose – as far as the law permits – what data or records governments request or demand, and by tightening up the encryption of their data transports.[36] Although much of this can be explained as an opportunistic drive to retain and/or regain customers, it is an interesting development in terms of power and counter-power. By raising the cost of mass surveillance through better encryption and maybe even forcing intelligence services to fine-tune their surveillance, their response can be seen as a first move towards counter-power. Microsoft is also fighting a legal battle against the US government's assertion that all data managed by a US company – even if it is held on servers in Ireland – can be commandeered by government.[37] In light of their market power and the crucial role they play in digitising the lives of entire populations, governments can no longer avoid diplomatic dealings with these information giants. These companies are more than potential investors that must be seduced and recruited and are more than violators of privacy that must be tackled: they are parties who merit serious diplomatic attention, with all the contradictions inherent to diplomacy.

34. Brown and Marsden (2013: 40)
35. Börzel and Risse (2010)
36. Van Hoboken and Rubinstein (2014)
37. See for example: http://www.theguardian.com/technology/2014/dec/14/privacy-is-not-dead-microsoft-lawyer-brad-smith-us-government.

Internet intermediaries: private parties or sheriff's deputies?

In the same vein, governments must be clearer about what they expect of the many intermediaries in cyberspace that facilitate digital life, starting with ISPs but also including search engines, cloud services, and so on. In a sense, these organisations are caught between a rock and a hard place. They are expected to deal with their customers ethically and responsibly, but also to comply with the requirements and demands of the authorities. In international terms, that may sometimes be seen to mean that Google should work with the US government but not with the Chinese. Although that makes sense from the perspective of human rights and the democratic rule of law, the absence of a clear understanding or even a structured discussion exploring what intermediaries may and may not do and what governments may and may not demand, is manifestly missing. When faced with a government request or subpoena (whether or not made in secret), intermediaries currently have three options: compliance, resistance and pre-emption. Pre-emption, where intermediaries take preventive action without being formally requested, is undesirable from a rule-of-law perspective. The deputation of private companies comes at the price of what has been termed intermediary censorship[38] and the fact that decision-making on what is and is not allowed slowly shifts towards private parties. Compliance and resistance are probably both necessary with a view to the division of power, although each on its own would be problematic. We have yet to see the start of a structured discussion on this topic, certainly at international level.

Extending the framework for business responsibilities

One way forward may be to build on the work of John Ruggie, the UN Secretary-General's Special Representative for Business and Human Rights. His work led to the publication in 2011 of the UN Guiding Principles on Business and Human Rights.[39] The Guiding Principles could be adapted to cover the duties and responsibilities of internet-based companies that play a major role – either de facto or because national law forces them to do so – in online and offline human rights situations in certain countries. In June 2014, the UN Human Rights Council adopted a resolution to establish an intergovernmental working group that is to elaborate a legally binding instrument on multinationals with respect to human rights.[40] The protection of the internet as a global public good, and the role that private companies may play in this regard, may follow a similar trajectory. The framework should make the role and responsibilities of internet-based companies clearer and ensure that they

38. Zuckerman (2010); MacKinnon (2011)
39. See: http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
40. See: http://business-humanrights.org/en/binding-treaty/un-human-rights-council-sessions

and governments hold each other accountable for their responsibilities and obligations – and for not overstepping them. A similar process could be launched regarding the mutual obligations of businesses and governments in protecting the public backbone of the internet.

4 NEW COALITIONS FOR THE PROTECTION OF THE INTERNET'S BACKBONE

This policy brief argues that the internet's backbone of key protocols and infrastructure should be considered a *global public good*. The protection of this public good requires a new international agenda for internet governance and the need to broaden the diplomatic arena and invest in new international coalition building. These new coalitions should work towards the establishment of an international norm that identifies the main protocols of the internet as a neutral zone in which governments are prohibited from interfering for the sake of their national interests.

References

Ablon, L., M. Libicki and A. Golay (2014) *Markets for cybercrime tools and stolen data. hackers' bazaar,* RAND National Security Research Division, Santa Monica: RAND.

AIV/CAVV (2011) *Cyber Warfare*, nr. 77, AIV/ nr. 22, CAVV, The Hague: Advisory Council on International Affairs.

AIV (2014) *The Internet. A Global Free Space With Limited State Control,* The Hague: Advisory Council on International Affairs

Benkler, Y. (2011) 'A free irresponsible press: Wikileaks and the battle over the soul of the networked fourth estate', *Harvard Civil Rights-Civil Liberties Law Review,* 46 (2): 311-396

Börzel, T. and T. Risse (2010) 'Governance without a state: Can it work?', *Regulation & Governance,* 4 (2): 113–134.

Brito, J. and T. Watkins (2011) 'Loving the cyber bomb? The dangers of threat inflation in cyber security policy', *Harvard National Security Journal*, 3 (1): 41-84.

Broeders, D. (2014) *Investigating the place and role of the armed forces in Dutch cyber security governance,* Breda: The Netherlands Defence Academy.

Broeders, D. (2015) *The public core of the internet. An international agenda for internet governance.* Amsterdam: Amsterdam University Press.

Brown, I. and C. Marsden (2013) *Regulating code: Good governance and better regulation in the information age,* Cambridge (Mass.): MIT Press.

Chander, A. and U. Le (2015) 'Breaking the Web: Data localization vs. the global internet', *Emory Law Journal.* Vol. 64: 677-730

Choucri, N. (2012) *Cyberpolitics in international relations,* Cambridge (Mass.): MIT Press.

Council on Foreign Relations (2013) *Defending an open, global, secure and resilient internet,* New York: Council on Foreign Relations.

Deibert, R. (2013a) *Bounding cyber power: Escalation and restraint in global cyberspace,* CIGI Internet Governance Papers nr. 6 (October 2013).

Deibert, R. (2013b) *Black code. Inside the battle for cyber space,* Toronto: Signal.

Deibert, R., J. Palfrey, R. Rohozinski en J. Zittrain (2008, eds.) *Access denied: The practice and policy of global internet filtering,* Cambridge (Mass.): MIT Press.

Deibert, R., J. Palfrey, R. Rohozinski en J. Zittrain (2010, eds.) *Access controlled: The shaping of power, rights, and rule in cyberspace,* Cambridge (Mass.): MIT Press.

Deibert, R., J. Palfrey, R. Rohozinski en J. Zittrain (2011, eds.) *Access contested. Security, identity, and resistance in Asian cyberspace,* Cambridge (Mass.): MIT Press.

DeNardis, L. (2012) 'Hidden levers of internet control. An infrastructure-based theory of internet governance', *Information, Communication and Society*, 15 (5): 720-738.

DeNardis, L. (2013) I*nternet points of control as global governance,* CIGI Internet Governance Papers nr. 2 (August 2013).

DeNardis, L. (2014) *The global war for internet governance,* New Haven: Yale University Press.

Dunn Cavelty, M. (2012) 'The militarisation of cyberspace: Why less may be better', pp. 141-153 in C. Czossceck, R. Ottis en K. Ziolkowski (eds.) *2012 4th International Conference on Cyber Conflict*, Tallinn: NATO CCDCOE Publications.

Dunn Cavelty, M. (2013) 'From Cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse', *International Studies Review,* 15 (1): 105-122.

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.

Eeten, M. van, M. Mueller and N. van Eijk (2014) *The internet and the state: A survey of key developments,* Den Haag: Raad voor Maatschappelijke Ontwikkeling.

Fidler, M. (2014) *Anarchy or regulation? Controlling the global trade in zero-day vulnerabilities,* Honors thesis in International Security Studies, Stanford University

Graham, M. (2014) 'Internet geographies: Data shadows and digital divisions of labour', pp. 99-116 in M. Graham en W. Dutton (eds.) *Society and the internet: How networks of information and communication are changing our lives,* Oxford: Oxford University Press.

Greenwald, G. (2014) *No place to hide. Edward Snowden, the NSA and the US Surveillance State, New York:* Metropolitan Books.

Hansen, L. and H. Nissenbaum (2009) 'Digital disaster, cyber security and the Copenhagen School', *International Studies Quarterly*, 53: 1155-1175.

Hoboken J. van, and I. Rubinstein (2014) 'Privacy and security in the cloud: Some realism about technical solutions to transnational surveillance in the post-Snowden era', *Maine Law Review,* 66 (2): 487-534.

Hurwitz, R. (2014) 'The play of states: Norms and security in cyberspace', *American Foreign Policy Interests,* 36 (5): 322-331.

Jervis, R. (1978) 'Cooperation under the security dilemma', *World Politics*, 30 (2): 167-214.

JPCERT/CC (2014) *The cyber green initiative: Improving health through measurement and mitigation*, JPCERT/CC Concept Paper, 10 August 2014.

Kane, A. (2014) 'The rocky road to consensus: The work of un groups of governmental experts in the field of ICTs and in the context of international security, 1998-2013', *American Foreign Policy Interests*, 36 (5): 314-321.

Knapen, B., G. Arts, Y. Kleistra, M. Klem and M. Rem (2011) *Attached to the World. On the anchoring and strategy of Dutch foreign policy.* Amsterdam: Amsterdam University Press

Landau, S. (2010) *Surveillance or security? The risks posed by new wiretapping technologies,* Cambridge (Mass.): MIT Press.

Landau, S. (2014) Making Sense of Snowden Part II: What's Significant in the NSA Surveillance Revelations , *IEEE Security and Privacy,* Vol. 12, No. 1, January/February 2014

Lemley, M., D.S. Levine and D.G. Post (2011) 'Don't break the internet', *Stanford Law Review Online,* 34, 19 december 2011.

Libicki, M. (2012) 'Cyberspace is not a warfighting domain', *I/S: A Journal of Law and Policy for the Information Society,* 8 (2): 321-336.

Lieshout, P. Van, R. Went and M. Kremer (2010) *Less Pretension, More Ambition. For development policy in times of globalization.* Amsterdam: Amsterdam University Press

Lin, H. (2012) 'Thoughts on threat assessment in cyberspace', *I/S: A Journal of Law and Policy for the Information Society,* 8 (2): 337-355.

Nye, J. Jr. (2011) 'Nuclear lessons for cyber security?', *Strategic Studies Quarterly,* 5 (4): 8-38.

MacKinnon, R. (2011) 'Corporate accountability in networked Asia', pp. 195-215 in R. Deibert, J. Palfrey, R. Rohozinski and J. Zittrain (eds.) *Access contested. Security, identity, and resistance in Asian cyberspace,* Cambridge (Mass.): MIT Press.

Masnick, M. (2014) 'The rebranding of SOPA: now called "Notice and staydown"', *Techdirt,* 14 March 2014, https://www.techdirt.com/articles/20140313/17470826574/rebranding-sopa-now-called-notice-staydown.shtml.

Maurer, T. and R. Morgus (2014) *Tipping the scale: An analysis of global swing states in the internet governance debate,* CIGI Internet Governance papers nr. 7 (May 2014).

Maurer, T., R. Morgus, I. Skierka en M. Hohmann (2014) *Technological sovereignty: Missing the point? An analysis of European proposals after June 5, 2013.* Report for Transatlantic Dialogues on security and freedom in the digital age.

Mueller, M. (2010) *Networks and states. The global politics of internet governance,* Cambridge (Mass.): MIT Press.

Mueller, M. and B. Kuerbis (2014) 'Towards global internet governance: How to end U.S. control of ICANN without sacrificing stability, freedom or accountability', *TPRC Conference* Paper, available at SSRN: http://ssrn.com/abstract=2408226.

Rid, T. (2013) *Cyber war will not take place,* Londen: Hurst and Company.

Schmitt, M. (2013, ed.) *Talinn Manual on the international law applicable to Cyber Warfare,* Cambridge: Cambridge University Press.

Singer, P. and A. Friedman (2014) *Cyber security and cyberwar. What everyone needs to know,* Oxford: Oxford University Press.

Stockton, P. en M. Golabek-Goldman (2013) 'Curbing the market for cyber weapons', *Yale Law and Policy Review,* 32 (1): 101-128.

Yu, P. (2012) The Alphabet Soup of Transborder Intellectual Property Enforcement. *Drake Law Review Discourse,* June 2012, pp. 16-33

Yu, P.K. (2014) 'Digital copyright enforcement measures and their human rights threats', in C. Geiger (ed.) *Research Handbook on Human Rights and Intellectual Property,* Edward Elgar.

Zittrain, J. (2014) 'No, Barack Obama isn't handing control of the internet over to China. The misguided freakout over ICANN, *New Republic,* 14 March 2014.

Zittrain, J. and Palfrey (2008) 'Internet filtering: The politics and mechanisms of control', pp. 29-56 in R. Deibert, J. Palfrey, R. Rohozinski and J. Zittrain (eds.) *Access Denied: The Practice and Policy of Global Internet Filtering,* Cambridge (Mass.): MIT Press.

Zuckerman, E. (2010) 'Intermediary censorship', blz. 71-85 in R. Deibert, J. Palfrey, R. Rohozinski and J. Zittrain (eds.) *Access controlled: The shaping of power, rights, and rule in cyberspace,* Cambridge (Mass.): MIT Press