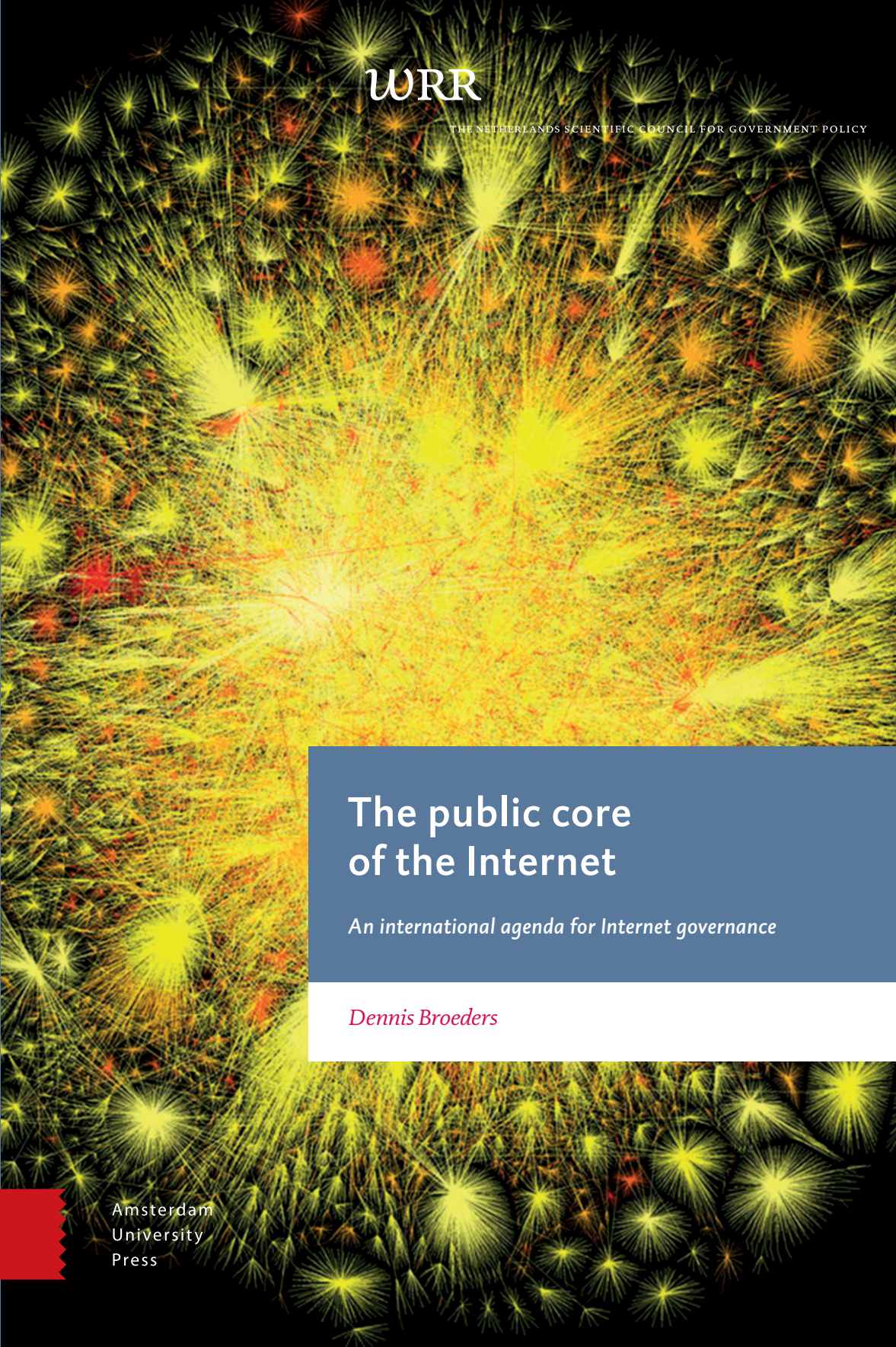

WRR
THE NETHERLANDS SCIENTIFIC COUNCIL FOR GOVERNMENT POLICY
The public core of the Internet
An international agenda for Internet governance
Dennis Broeders
Amsterdam University Press

The public core of the Internet

This book is based on a report that was published by The Netherlands Scientific Council for Government Policy (WRR). According to the Act of Establishment, it is the Council's task to supply, for the benefit of government policy, scientifically sound information on developments which may affect society in the long term, and to draw timely attention to likely anomalies and obstacles, to define major policy problems and to indicate policy alternatives.

The council draws up its own programme of work, after consultation with the Prime Minister, who consults the cabinet on the proposed programme.

The Netherlands Scientific Council for Government Policy
Buitenhof 34
Postbus 20004
2500 EA The Hague
Telephone 070-356 46 00
E-mail info@wrr.nl
Website www.wrr.nl

WRR

THE NETHERLANDS SCIENTIFIC COUNCIL FOR GOVERNMENT POLICY

The public core of the Internet

AN INTERNATIONAL AGENDA FOR INTERNET GOVERNANCE

Dennis Broeders

Amsterdam University Press, Amsterdam 2015

Cover: OPTE 'The Internet 2010' © 2014 LyonLabs, LLC and Barret Lyon/ Creative Commons

Layout: Textcetera, The Hague

ISBN	978 94 6298 195 9
e-ISBN	978 90 4853 176 9 (pdf)
NUR	805

CONTENTS

PREFACE

This book is a translation and adaptation of the Dutch report *De publieke kern van het Internet (The public core of the Internet)* that the Netherlands Scientific Council for Government Policy presented to Bert Koenders, the Dutch Minster for Foreign Affairs, on the 31st of March 2015. It advised the Dutch government to make cyberspace and Internet governance a serious priority for its foreign policy. The successful organisation of the Global Conference on Cyber Space in April 2015 (GCCS2015) in The Hague provided the Dutch government with an excellent stepping stone to promote its goals of a safe and open Internet through the global arena of cyber diplomacy. Dutch cyber diplomacy will be intensified in the wake of this conference, building – amongst others- on the insights and recommendations put forward in this report.

The core messages in the original report and in this book are not limited to the Netherlands however, but have a global appeal. Its main argument is that the Internet's infrastructure and core protocols should be regarded as a global public good that is in need of protection against unwarranted interventions by states and other parties. Its main policy recommendation is that states should work towards establishing an international standard that identifies the Internet's core protocols as a neutral zone in which governments, pursuing their national interests, are prohibited from interfering. This is a goal that is of crucial importance for all states whose societies and economies depend on the integrity and functionality of the Internet. Increasingly, that is the vast majority of states.

The original report was drawn up by a project team headed by Dennis Broeders, senior research fellow at the Council and professor of Technology and Society at Erasmus University Rotterdam. The other members of the group were Erik Schrijvers and Lisa Vermeer, both research fellows at the Council. Member of the Council Mark Bovens was also involved in the project.

While writing this report, the project group consulted numerous experts in the fields of Internet governance and cybersecurity. Their comments were extremely valuable and the Council would like to thank the interviewees for their time and effort. The Council would also like to thank Jan van den Berg, Nico van Eijk, Marieke de Goede, Erik Huizer and Corien Prins, who commented on earlier versions of the Dutch report.

Prof. André Knottnerus
Chairman Netherlands Scientific Council for Government Policy

SUMMARY

The Internet's core 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 public core requires a new international agenda for Internet governance that departs from the notion of a global public good.

INTERNET GOVERNANCE BETWEEN THE TECHNICAL AND THE POLITICAL

Everyday life without the Internet has become unimaginable. It is inextricably interwoven with our social lives, our purchasing behaviour, our work, our relationship with the government and, increasingly, with our everyday objects, from smart meters to the cars we drive and the moveable bridges we cross en route. 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 their 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 a much greater 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 an approach that focuses more on national and other forms of security: the Internet of cybercrime, vulnerable critical infrastructure, digital espionage and cyberattacks. In addition, a growing number of countries are seeking to regulate their citizens' online behaviour, for reasons ranging from copyright protection and fighting cybercrime to censorship, surveillance and control of their own populations on and through the Internet.

Attempts by national states to 'fence off' their own national area of cyberspace, and their increased role in its governance, may have repercussions for the Internet's backbone infrastructure. The Internet was developed to operate internationally, without regard for the user's status or nationality – an underlying principle that benefits all users. It is mainly the Internet's public core, consisting of infrastructure, protocols and standards, that routes data so that it reaches all four corners of the globe. If these protocols and standards fail or become corrupted, the performance and integrity of the entire Internet is put at risk. The Internet is 'broken' if we can no longer assume that the data we send will arrive, that we can locate the sites we are searching for, and that those sites will be accessible. Recently, however, a growing number of states have tampered with the Internet's core infrastructure in order to further their own national interests.

In this regard, 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. It is imperative for the future of Internet governance to determine which part of the Internet should regarded as a global public good – and thus safeguarded from improper interference – and which part should be seen as the legitimate domain of national states, where they can stake a claim and take up their role without harming the infrastructure of the Internet itself.

THE INTERNET'S CORE AS A GLOBAL PUBLIC GOOD

This study 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. 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. This can be said to apply to the Internet both as a network and as an infrastructure.

These benefits derive largely from the Internet's core protocols, including the TCP/IP Protocol Suite, numerous standards, the Domain Name System (DNS), and routing protocols. As a global public good, the Internet only works properly if its underlying values – universality, interoperability and accessibility – are guaranteed and if it facilitates the main objectives of data security, i.e. confidentiality, integrity and availability. It is vital that we – the users – can rely on the most fundamental Internet protocols functioning properly: those 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 public core of the Internet – our digital existence – thus very much depends on those underlying protocols. Although national states will inevitably want to 'create an Internet in their own image', we must find ways to continue guaranteeing the overall integrity and functionality of the public core of the Internet.

FROM GOVERNANCE *OF* THE INTERNET TO GOVERNANCE *USING* THE INTERNET

To highlight the problem we can differentiate between two forms of Internet governance. The first is governance *of* the Internet's infrastructure, i.e. the governance of the core infrastructure and protocols of the Internet. It is this public core that drives the Internet's development. The collective infrastructure takes precedence in this form of governance. The second form is governance *using* the Internet's infrastructure. In this case, the Internet becomes a tool in the battle to control

online content and behaviour. The issues vary from protecting copyright and intellectual property to government censorship and surveillance of citizens. Increasingly, governments view the 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 – with the technical management and performance of its infrastructure being the top priority – the trend today is increasingly towards governance *using* the Internet. Such interventions can undermine the integrity and functionality of the Internet and, in turn, undermine the digital lives that we have built on top of it.

THREATS TO GOVERNANCE OF THE INTERNET INFRASTRUCTURE

Governance of the Internet's public core – i.e. governance of the Internet – is entrusted to a number of organisations that are collectively known as the 'technical community'. Although that governance is mostly in good hands, pressure is building on it from several quarters. Political and economic interests – sometimes combined with new technologies – are challenging the collective character of the network.

- Economic interests – for example copyright protection and revenue models for data transport – are putting pressure on policymakers to abolish or, conversely, offer legislative protection to net neutrality, previously the Internet's default setting.
- The transition of the 'IANA function', which includes the stewardship and maintenance of registries of unique Internet names and numbers. There is mounting pressure to remove oversight of IANA from the US's sphere of influence, for reasons of international political legitimacy. The debate on this transition may result in more politicised management of the Domain Name System, which in turn may have repercussions for the ability to find and locate sites and users. Most countries would benefit from IANA functions that are as 'agnostic' as possible, especially when it comes to the administrative tasks
- Another challenge is the rise of the national security mindset in cyberspace. The technical approach of the CERTs (with a focus on 'keeping the network healthy') and their international alliances is at odds with the approach of national security actors, such as intelligence agencies and military cyber commands. It is important to prevent these approaches becoming confused and/or mixed, because national security conflicts with the collective interest of the network's overall security.

THREATS RESULTING FROM GOVERNANCE *USING* THE INTERNET INFRASTRUCTURE

The need for worldwide consensus on the importance of a properly functioning public core of the Internet seems obvious because it is these protocols that guarantee the reliability of the global Internet. However, recent international trends in policymaking and legislation governing the protection of copyright, defence and

national security, intelligence and espionage, and various forms of censorship, show no signs of such a consensus. 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-day vulnerabilities') as ideal instruments for national policies focused on monitoring, influencing and blocking the conduct of people, groups and companies. The negative impact of such interventions is borne by the collective, however, and impairs the Internet's core values and operation. Illustrations of this trend include:

- Various forms of Internet censorship and surveillance 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.
- The online activities of military cyber commands, intelligence and security services which undermine the proper functioning of the public core of the Internet. 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.
- 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 ('overblocking'), damage to the DNS and intermediary censorship through ISPs.
- Some forms of Internet nationalism and data nationalism – in which states seek to fence off a national or regional part of the Internet – which require interventions in routing protocols. In extreme forms this could lead to splintering of the Internet.

TOWARDS AN INTERNATIONAL AGENDA FOR INTERNET GOVERNANCE

The international political landscape of Internet governance is also changing rapidly. The next billion (or billions) of users will go online in emerging economies that may have a different cultural and political outlook on cyberspace from the still dominant 'Western' view. In addition, 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 cutting edge today will be much more commonplace in five years' time. If in that same timeframe 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 core of the Internet.

THE INTERNET'S PUBLIC CORE SHOULD BE AN INTERNATIONAL NEUTRAL ZONE

Given these developments, it should be an internationally shared priority to work towards establishing an international standard 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, i.e. a specific area where national interests and global issues coincide for all states that 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 core – 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 entail 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 as 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.

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 different views on security may in fact improve the security of the Internet as an infrastructure.

- It is therefore vital to advocate at international level that a clear differentiation be made 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. At one end of the spectrum there is the notion of Internet security, i.e. ensuring that the network itself is secure and operational. At 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. It is important to separate the technology-driven strategy of the CERTs, which involves a public health-type approach to overall network security, from the logic of national security, which places national interests above those of the network.

THE NEED TO BUILD NEW COALITIONS IN CYBERSPACE

Given the international demographic and political shifts in cyberspace, it is 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 fully in the debates about Internet governance. Secondly, there is a strong case to be made for targeting the large, 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. Lastly, states need to make more productive use of the expertise of NGOs and other private stakeholders, especially in thinking through the effects of national and foreign policies on the technical operation of the Internet as a whole.

1 INTERNET GOVERNANCE AT A CROSSROADS

> Today's Internet is a fortuitous accident. It came into being through a combination of an initial lack of commercial interests, government benign neglect, military requirements for survivability and resilience, and computer engineers building open systems that worked simply and easily. Battles over its future are going on right now: in legislatures around the world, in international organizations like the ITU, and in Internet organizations like the IGF.
> Bruce Schneier (2013: 13)

1.1 INTRODUCTION

Everyday life without the Internet has become unimaginable. Everything – the economy, our social lives, our infrastructure and public life in general – ties into and branches out from it. And it will become even more important in the decades ahead as the 'Internet of Things', cloud computing and mobile data technology gather momentum and new applications come along that we cannot envisage yet. All this means that our social, public and economic lives will depend increasingly on an infrastructure that spans the globe and is, in essence, non-territorial. That infrastructure – the software and protocols underpinning the Internet – was built by private parties and an international technical community; except for substantial investments in the Internet's early development, governments have mainly been involved indirectly.

Most people are unacquainted with and uninterested in the deep layers that determine how the network operates, just as they are unfamiliar with the workings of their car engine. They don't really care how their car works, as long as it does. They leave the rest to the experts. For a long time, the same was true of the Internet. It began life as ARPANET, a small network of American universities and the US Department of Defense, and was known only among the true pioneers, who maintained, modified and expanded the network themselves. As the Internet grew, and especially after the 1991 launch of the World Wide Web (WWW), which made it possible to access information simply by 'surfing' between websites, it became increasingly important to our everyday lives. At the same time, the Internet's 'engine' and physical infrastructure faded more and more from the view of everyday users.

States now take a keen interest in the Internet. Whereas fifteen years ago, newspapers tended to report on the Internet's economic potential – with the 'dot.com bubble' in around 2000 as a glitch in the rise of the WWW – today's Internet features in virtually every aspect of public and political life. Politicians recognise that it has become one of the pillars of the economy and intrinsic to people's social and professional lives. They also recognise that cybercrime is on the increase; they observe that all our critical infrastructures are in fact linked to the Internet; they

realise that Google, Apple and Facebook know more about their citizens than they do, and exploit that information; and they see how the military and intelligence communities are becoming increasingly active and intrusive online. With the Internet taking centre stage and at the root of so many opportunities and threats, a growing number of authorities have become interested in its deeper layers and how they are governed.

As a global infrastructure, however, the Internet is at odds with a world in which states do their utmost to secure their national interests online. While it is certainly not the case that national policy has no impact on the Internet – or rather, on the parties that shape, maintain and use the Internet – the international nature of the Web often makes it very difficult for states to secure their national interests. There is also little international cooperation – let alone international political consensus – on the issue of the Internet's governance. That does not mean that the Internet is ungoverned, of course. On the contrary, over the past thirty years it has been managed, developed and expanded by a network – which arose more or less from the bottom up – of private parties, NGOs, academics and also authorities, in what is known as a multistakeholder system (see e.g. Goldsmith and Wu 2008; Mueller 2010; Deibert 2013; DeNardis 2014). However, states are now demanding a bigger role for themselves, putting enormous pressure on the bottom-up nature of this system. There is no consensus among states, nor among the other stakeholders, on the choices that need to be made concerning the future of Internet governance, even though some of those choices may have huge implications for the way the Internet itself operates.

This book aims to outline an international policy agenda for Internet governance that makes some of those necessary choices. It proceeds from the need to strike the right balance between guaranteeing and protecting the Internet infrastructure as a global public good on the one hand, and integrating the Internet as a normal part of international and diplomatic relations on the other.

1.2 INTERNET GOVERNANCE AT A CROSSROADS

The fact that states are claiming a greater role for themselves in Internet governance is no surprise, given that the Internet has become a vital component of their economies and societies. The *laissez-faire* attitude long taken by most countries is now considered by many to be imprudent and inappropriate. That does not mean that every state has a clear notion of what the Internet is and how it can best be regulated. In fact, opinions are very much divided on matters such as freedom of speech, fighting cybercrime and the protection of intellectual property rights. Such matters are part and parcel of both national policymaking traditions and international diplomatic relations between states. The fact that some of these issues are online manifestations of old problems does not necessarily alter them,

but it does mean taking a very different approach at times, and seeking a very different form of international cooperation. This book aims to contribute to an international governance agenda that focuses on the Internet's deep technological layers and software protocols. It does not address directly such vital issues as online freedom of speech or the mass surveillance of personal data as separate issues, but instead considers them when state policies *use* the deeper layers of the Internet and in doing so pose a threat to its integrity and its operational functionality. The reliability of the Internet – both technically and in terms of 'trust' – depends on how its 'public core' operates. If the Internet fails, is unreliable, then it is unreliable for every Internet user around the world. And although some states will inevitably want to 'create the Internet in their own image', there is a need to find ways to continue guaranteeing the general operability of its core.

1.2.1 A GLOBAL INFRASTRUCTURE AND NATIONAL INTERESTS

Some authors believe that Internet governance has reached a crossroads in which two worlds are set to clash: the global and non-territorial world of the Internet versus the world of national states, with territorial sovereignty as the organising principle of international relations. Sovereignty and the Internet appear to be irreconcilable concepts. The Internet itself is not restricted by national borders and the Transmission Control Protocol/Internet Protocol (TCP/IP) has been set up to ensure that packets of information basically always arrive at the right destination. Or, as John Gilmore put it: 'The net interprets censorship as damage and routes around it' (quoted in Maher 2013). At the same time, however, states are increasingly trying to control the global Internet, subject it to national policies and/or regulate it internationally. Some do so to control their own people, some to defend their economic interests, and some to enforce their sovereignty by military means. It is clear that states are increasingly inclined to draw borders in cyberspace and introduce the concept of territorial sovereignty to the Internet. Just as the Wild West was gradually absorbed and tamed by the USA, so some commentators maintain that states will do the same to the 'anarchist Internet'. Others refer to the rise of a 'Westphalian model' on the Internet. This is a reference to the Peace of Westphalia, signed in 1648, in which the concept of sovereign states became the legitimate organising principle for international relations. Here, it is used to indicate that states wish to claim sovereignty on the global Internet. Demchak and Dombrowksi (2011; 2013: 33) warn that a cyber-Westphalian doctrine cannot emerge without ending in conflict: 'The process of establishing cyber borders and thus states' sovereignty will be non-linear, dangerous and lengthy'. It is a process that fits in with a broader trend towards renationalisation, where a belief in the advantages of economic and cultural globalisation – which long set the standard and which produced many benefits – is set off against national interests. For example, acting under the banner of economic security, states are considering the relationship between international investment, transnational take-overs and geopolitical trends on the one hand, while simultaneously protecting their own

industries and critical infrastructures. How can countries that are deeply integrated into the global economy navigate a course between naivety and paranoia (NCTV 2014)? Even with respect to the global Internet, states must weigh their national interests against the international net. The three quotes that follow illustrate how much the role of states and opinions about that role have changed in recent years.

'We reject: kings, presidents and voting. We believe in: rough consensus and running code'

In 1992, this is how David Clark, a professor at MIT and an Internet pioneer, described how the 'Internet community' tackled what is now known as 'Internet governance' (quoted in Goldsmith and Wu 2008: 24). It rejected democratic decision-making on how the network should develop, nor did it accept top-down political authority. Rough consensus between the engineers and other stakeholders, who regarded the Internet mainly as a technological challenge, was sufficient. In their eyes, it was essentially a non-political network that through technological breakthroughs and a growing mass of users gradually turned into a global 'network of networks'. Although the Internet certainly had government to thank for its early development – in particular the government of the United States – most countries for a long time regarded it as scarcely needing governance, or even considered it uncontrollable to a certain extent.

'Good luck! That's sort of like trying to nail Jell-O to the wall'

Six years later, US President Bill Clinton was still convinced that the Internet was ungovernable. His statement came in 1998 after attempts by China to control and spy on the Internet, and more specifically on Chinese Internet users (quoted in Goldsmith and Wu 2008: 90). Widely regarded as one of the first censorship and surveillance projects targeting the Internet and Internet users, it introduced the expression 'Great Firewall of China' to the modern language. We are now several generations of Internet surveillance further and the technology used to detect and monitor users has become ever more refined (Deibert et al. 2008; 2010; 2011). Or, as Tim Wu (2010: 309) puts it: 'The Jello was, somehow, nailed to the wall'. The Internet is no longer the sanctuary it used to be for anonymous users. Businesses and government authorities monitor the behaviour of Internet users closely. Businesses do so because data about users' online behaviour can be turned into profit in various ways; the authorities do so because they believe that such data hold the key to increased security and tighter control of the population. Of course, different countries have different ideas about what security entails. Dutch, Iranian, American, and Russian concepts of security and freedom contrast starkly, both on the Internet and in the 'real' world. Unlike his predecessor Clinton, US President Barack Obama has long abandoned the notion that the Internet is uncontrollable. The revelations about the global surveillance practices of the

National Security Agency (NSA) have intensified the debate about the future of the Internet (Greenwald 2014). For a well-funded organisation like the NSA, at any rate, the opportunities appear to be unlimited.

'The Internet is a CIA project'
So claimed Russia's President Vladimir Putin in April 2014 during a media forum in St Petersburg,[1] one of many signs that the concept of the Internet as a global, apolitical network is waning. Or, put better, that politicians do not accept it as such. Politicians are making an ever-stronger case for the need to control the Internet. Yet another development, which many see as worrisome, is the militarisation of the Internet, with a growing list of countries regarding it as the fifth domain of warfare (after land, sea, air and space) and rapidly building up military cyber capacity and cyber intelligence services (see e.g. Singer and Friedman 2014; Guitton 2013; Deibert 2013; Dunn Cavelty 2013). That brings the Internet into the realm of high politics, i.e. the domain of national and international security. And once it has landed there, states are unlikely to go back to viewing it with benign neglect.

1.2.2 THE INTERNET AS A GLOBAL PUBLIC GOOD?

Although the Internet operates in a world ruled by states, it has an enormous global significance. At its most basic, it was developed to operate internationally, regardless of the user's status or nationality – an underlying principle that is beneficial to all users. The Internet has derived its strength from its growth and from its impressive ability to accommodate billions of users and new applications in the first decades of its existence. Or, as Vint Cerf (2013: 7) – one of the 'fathers of the Internet' – put it, 'The resources of the Internet, while finite, are not bounded except by our ability to construct more resource to grow the shared virtual space the Internet and its applications create'.

Thanks to its international design and global significance, parts of the Internet bear the markings of a global public good. Global public goods provide benefits to everyone in the world, benefits that can be gained or preserved only by taking targeted action and by cooperating. The 'public' part of a public resource lies in the fact that it affects all, or in the need for it to be available to all. That says nothing, however, about how that resource must be *provided*. The means and methods for the provision of 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 (Lieshout, Went and Kremer 2010). The same can be said to apply to the Internet as a network and infrastructure. In that context, the public part refers not to the content of the WWW or to the Internet as a public sphere, but to the operation of the Internet as a *system* that makes all the applications and content possible. Laura DeNardis (2014: 17) has pointed out the vital importance of the operation of that network: 'no less

than economic security, modern social life, culture, political discourse, and national security are at stake in keeping the Internet globally operational and secure'.

Pure global public goods have two essential traits: they are non-excludable and non-rivalrous. In other words, no one can be excluded from using the good, and one person's use is never at the expense of another person's. Strictly speaking, that does not hold true of the Internet. Both the authorities and businesses can exclude people from using it. Internet access and use is also not free, which in itself makes it excludable. Indeed, some governments – for example Egypt in 2011 – have even switched off the Internet during periods of unrest and crisis by shutting down the networks for a few days. However, both traits do apply to the way in which the technical community has set up the Internet and nurtured its development. To quote DeNardis again (2013: 4): 'With the exception of repressive political contexts of censorship, the Internet's core values are universality, interoperability and accessibility'. These core values focus on including, not excluding. The technical and logical core of the Internet, i.e. the basic protocols that determine how the network and data traffic are operated, is thus founded on values that support non-excludability. The history of the Internet's growth shows that its stakeholders have gone to great lengths to make it non-rivalrous by expanding its capacity again and again. Given sufficient technical progress – i.e. an increase in bandwidth and computing power – the set-up of the Internet is such that there is enough for everyone. In this book, the Internet's core is therefore regarded as an impure global public good,[2] in the same way that infrastructure is, for example (Went 2010).

1.2.3 GLOBAL VERSUS NATIONAL: A KEY PROBLEM OF INTERNET GOVERNANCE

National states are demanding more space and a greater role on the Internet, and specifically in matters of Internet governance. This trend may have implications for the core technical and logical infrastructure of the Internet as a global public good. States have had little input into the design and set-up of the structure that has governed the Internet since the 1980s and fostered its spectacular growth. Now that they are weighing in with a broad spectrum of national interests, some of them contradictory, and with their differing interpretations of freedom and security, the challenge is to give their national and international interests a greater say in this governance structure without damaging the public core – the very basis for the Internet's growth. Many researchers believe that the battle for the future of the Internet is being waged right now. Ronald Deibert's 2013 book is entitled *Black code. Inside the battle for cyberspace*; the first chapter heading of Milton Mueller's book *Networks and states* (2010) is 'A battle for the soul of the Internet'; and Laura DeNardis' latest book (2014) is entitled *The global war for Internet governance*. The question of how we can balance national interests against the governance of the Internet as a global public good is one that requires a mainly international response. The contributions of individual countries to this question are

shaped by their own foreign and national policies, which radiate out to affect other nations as well as the international domain. Those effects can naturally be either positive or negative.

1.3 SETTING THE SCENE: THREE TRENDS IN CYBERSPACE

As the international agenda regarding the Internet and the battle for its governance evolves, three trends are playing themselves out in the background that are particularly critical for the international arena. They are the demographic shift among worldwide Internet users, the securitisation and militarisation of the Internet, and the 'datafication' of society. Obviously, other trends that have a major impact on the development of the Internet could also be identified, specifically technological ones such as mobile data access and cloud computing. We will address those trends whenever they are important for our analysis. The trends that we focus on here are distinctive because they are a major influence on the international political arena.

1.3.1 DEMOGRAPHIC SHIFT

The Internet is rapidly conquering the world. In 2012, a little less than two and a half billion people were online. The Internet penetration rate is greatest in the West, where it ranges from 63.2 percent in Europe to 78.6 percent in the United States.[3] Indeed, many parts of the Western world are reaching saturation point. Today, growth there can largely be attributed to the rise in the number of Internet-enabled devices that each of us owns. The penetration rates in Africa (15.6%) and Asia (27.5%) are much lower, but the absolute number of users in Asia for example is many times higher. Asia has more than a billion Internet users, with China alone accounting for half that number. According to statistics collected in 2011, English was still slightly ahead of Chinese as the dominant language online, but the growth rates indicate that it has probably lost its lead by now. Between 2000 and 2011, the number of English-speaking Internet users increased by 301 percent, while the number of Chinese-speaking users grew by 1478 percent and the number of Arabic-speakers by 2501 percent (Choucri 2012: 61). Deibert (2013) believes that 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. Figure 1 shows worldwide Internet penetration and the regions where there is room for growth. The lighter the colour, the more potential for increasing the number of Internet users.

This shift has major consequences for the balance of power on the Internet and how cyberspace is viewed culturally. The next billion people to go online will live in relatively poor countries, have different cultural and political traditions from users in the West, and have governments that have different ideas about online security and freedom.

Figure 1.1 Internet users and Internet penetration worldwide, 2013

Source: Graham, De Sabatta and Zook (2015)

All these things will have repercussions for European and 'Western' foreign policy regarding the Internet. A recent report by the Council on Foreign Relations (2013: 67) calls 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'. The 'Western' voice may no longer dominate the Internet debate. In terms of Internet governance, the world may be divided into two camps: a camp that wants to reinforce the current bottom-up, multistakeholder model, and a camp that, conversely, wants more top-down influence for national states. In between these two extremes is a large group of countries known as 'swing states' or 'fence-sitters', which have not defined their position or come down clearly on one side or the other (see e.g. Maurer and Morgus 2014; Clemente 2013). As other notions of what the Internet is and should be gain political traction, they will shape the political playing field on matters of the Internet's design and future in the international domain.

1.3.2 SECURITISATION OF THE INTERNET

The security mindset is rife on the Internet. Cybercrime has clearly increased, and the rising number of companies that are now venturing online – connecting even their most basic processes to the Internet – has made the economy all the more vulnerable. Governments also see growing threats; in addition to cybercrime and the theft of trade secrets and confidential corporate data, they are becoming increasingly worried about the vulnerability of critical infrastructures and about economic and political espionage by other states. In its *Cyber Security Assessment Netherlands 2013*, published shortly before the start of the Snowden revelations, the Netherlands Cyber Security Centre had already explicitly named China, Russia, Iran and Syria in that context, but can now add its allies the USA and the UK to its list of cyber spies. Although threats to cybersecurity are increasing, it is difficult to say to what extent – because much of the relevant data are missing or biased[4] – and which are the realistic scenarios for the future. That makes it hard to see whether the rising budgets and growing attention on the part of policymakers are in proportion to the actual danger involved and/or focused on the right threat. The term 'threat inflation' is often used to explain the rapidly expanding cybersecurity budgets and legislated powers, certainly in the United States (Libicki 2012; Lin 2012; Rid 2013).

The Internet has also been elevated to the highest echelons of security policy in recent years. Cybersecurity and cyber warfare are rapidly growing areas of policymaking that have access to mounting budgets and an increasing scope of powers (Bauman et al. 2014; Guitton 2013; Severs 2013). The Internet's growing status as a domain of warfare also influences the way states view it. Many countries now consider the Internet to be the fifth domain of warfare, after land, sea, air and space. The language of war and national security affects the way the authorities regard the Internet. Some in government circles say that such language is critical as threat

piles upon threat; others, including some military strategists, question the usefulness of this framing. But terminology such as 'cybergeddon' (World Economic Forum 2014) and 'digital Pearl Harbor' (Clarke and Knake 2010) only fuels what the Copenhagen School of International Relations calls 'securitisation'. This particular school of thought argues that security threats are not objective facts but are rather the product of political discourse. Issues are thus politicised, placing them on the political agenda; in extreme cases, they are even 'securitised' (Lawson 2013: 88). When that happens, the issue is no longer 'debated as a political question, but dealt with at an accelerated pace and in ways that may violate normal legal and social rules' (Buzan et al. 1998: 23, quoted in Hansen and Nissenbaum 2009: 1158). Securitisation carries the risk that vital safeguards under the rule of law, democratic control and transparency of governance will be weakened in favour of rapid decision-making and national security. A good example is the US and other governments' political, military and legislative response to 9/11.[5]

Some researchers believe that cybersecurity and cyber warfare have also become part of a securitised discourse (Hansen and Nissenbaum 2009; Dunn Cavelty 2013; Singer and Friedman 2013). The fact that governments are taking serious action on national and international cybersecurity in response to what is a relatively poorly defined threat and despite much disagreement on a number of critical questions – such as 'what is a cyber attack?' and 'what is cyber warfare?' – may have huge consequences. It could lead to the far-reaching militarisation of the cyber domain (Libicki 2012; Dunn Cavelty 2012) and the rise of a new cybermilitary-industrial complex (Brito and Watkins 2011; Deibert 2013). It could also lead to an arms race in cyberspace (Nye 2011). And – as has often been the case in the past – the very response to danger may even give rise to other, new dangers. The advent of security as a key issue on the Internet – as opposed to the economic perspective that states adhered to in the Internet's early days – has profound consequences for the way in which states position themselves with respect to Internet governance and the priorities that they set.

1.3.3 THE DATA REVOLUTION

The third crucial trend for the future of Internet governance is datafication. There are three factors that play a role in datafication: the volume of data, the nature of the data and their analysis, and how and where the data are used (Van Dijck 2014; Mayer-Schönberger and Cukier 2013). The gigantic increase in the volume of data collected on human behaviour – whether or not it was provided voluntarily – and corporate and government recording and storage of data and metadata have changed the Internet and the way we perceive it. Data have become the lifeblood of Internet businesses and 'data is the new oil' has become a new catch phrase. Companies such as Facebook, Twitter and Google collect data on users in exchange for applications that are provided 'free of charge'. The advent of mobile Internet technology means that the data they collect is not confined to user

behaviour online but also connects to our daily geographical movements. They then use the data to match advertisers and customers as closely as possible. In the current era of Big Data, 'more is better' has also come to apply to the way we look at the world. With more data being collected, the nature of the data collections and their analysis have also changed. Many see the ability to combine as much data as possible and to use statistical analysis to distil correlations and conclusions – sometimes unexpected ones – as a source of new applications and markets in the Internet economy (Degli Esposito 2014). The authorities have also cottoned on to the vast number of ways that Big Data can be analysed and used, for example in health care, in municipal government, and – last but not least – in the area of security. The gathering momentum of Big Data has enormous implications for such issues as privacy and data protection, for the way research is conducted (more data-mining, less hypothesis-driven), and for the international balance of power on and in relation to the Internet.

Increasingly, datafication is 'everywhere'. A typical example is the rise of the Internet of Things (IoT). One of the major forces in this area, Cisco Systems, has gone a step further and now speaks of the 'Internet of Everything'. The IoT refers to the way in which countless devices are connected and 'communicate' with one another online. They obviously include mobile phones, but also things such as refrigerators and cars ('on-board computers'), industrial machinery and logistical processes. Advances such as these shift questions of data management and security from the computer and telephone to other devices and purposes. Doing so also blurs the line between online and offline activities – a trend to which various researchers drew attention in a 2014 advisory report presented to the European Commission and bearing the apt title *The Onlife Manifesto*.[6]

With data now being so critical to the way businesses view customers and governments view citizens – their own and those of other countries – data storage, management and analysis have also gained importance in the international domain. Privacy and personal data protection are sacrosanct concepts in EU legislation, relatively speaking, but the new reality of datafication is putting pressure on the rights and safeguards that have been enshrined in policy and legislation. EU rules on personal data protection enacted in 1995 had a radiating effect on the rest of the world (a 'Brussels effect' – Bradford 2012). The EU has been negotiating new rules since 2012, and the question is whether the new Regulation will have the same sort of impact. Some aspects, for example the size of fines for data misuse, may have major consequences. With the EU potentially setting the standard for the rest of the world, and with vast amounts of ever more valuable data being collected, there are major interests at stake in this new EU legislation.

Some businesses now know much more about the citizens of a particular country than their own governments do, even though it used to be governments that were in control of the biggest data collections (Taylor and Broeders 2015). This has naturally not escaped the latter's notice. One of the most shocking revelations about the NSA was the extent to which its surveillance activities focused on data collected by the private sector, and the degree to which US companies 'assisted' the NSA in that regard (Greenwald 2014). In 2013, the historian Timothy Garton-Ash wrote in the 'opinion' section of *The Guardian* that the conclusion was clear: 'were Big Brother to come back in the 21st century, he would return as a public-private partnership' (see also Lyon 2014). The NSA revelations showed how much data certain companies – most of them American – actually collect and to what extent governments can access those data. Bruce Schneier (2013) claims that we live in what is in fact the feudal age of the Internet, with power resting in the hands of large Internet companies and governments. The users, who seemed so unfettered and powerful in the early days, have come to depend on these feudal lords for their security, privacy and other online rights, without having much influence over them. To a certain extent, large Internet companies and governments are condemned to work together, with the balance of power sometimes tipping towards one and then towards the other. But Big Data management and the potential for far-reaching surveillance – commercial, government or combined – also has implications for the international balance of power and inter-state relations.

1.4 AIM AND STRUCTURE OF THE BOOK

This book focuses on the future of international Internet governance and the contribution that national states can make, either on their own or as part of regional and international organisations and other international coalitions. It aims to contribute to an international agenda for Internet governance that strikes a balance between guaranteeing and protecting the core protocols and infrastructure of the Internet as a global public good on the one hand, and normalising the Internet as a component of international relations on the other. Given the significance of the global net, Internet-related issues should be an integral part of any modern foreign policy.

Chapter 2 looks more closely at Internet governance by drawing an analytical distinction between 'governance *of* the Internet's architecture' and 'governance *using* the Internet's architecture'. As a global public good, the Internet is mainly categorised under the former heading, but it can be put at risk when states develop national policies that *use* the internet's architecture in a technically ill-advised manner. Chapter 2 argues that securing the Internet as a global public good can be considered an extended national interest for all states that depend on the Internet for their economic growth and socioeconomic vitality.

Chapters 3 and 4 build on the analytical distinction between 'governance *of* the Internet' and 'governance *using* the Internet'. Chapter 3 investigates governance *of* the Internet and discusses how the Internet's public core is managed. That public core is founded on values such as universality, interoperability, accessibility, integrity, availability and confidentiality, which all go to guarantee the functionality of 'the Internet' as a global system for its users. The task of living up to those values and fulfilling those functions has been entrusted to various institutions, protocols and standards. The 'Team Internet' that manages these protocols and functions is highly efficient and effective in many ways, but falls short in others. Shortcomings can be attributed both to design flaws and frictions between what is best for the Internet technically and the network administrators' revenue models (for example the problem of upgrading from IP4 to IP6) and to political and economic interests and legitimacy issues. Other problems have found their way onto the international agenda because the growing economic and political significance of the Internet has attracted new parties and stakeholders that meddle in the technical operation and governance of the public core. In each case, conflicts about the governance of the public Internet are more likely to be caused by shifts in international political and/or economic relations than by dissatisfaction about the technical operation of the Internet.

Chapter 4 addresses four controversies – most of them national in origin – concerning interventions in the Internet's core protocols and principles. The first involves a series of recent draft acts and an international treaty to protect copyright and intellectual property rights online. The second is about one of the most difficult problems from an international human rights perspective: censorship and restrictions on freedom of speech. Both controversies illustrate the pivotal role that Internet Service Providers (ISPs) are assigned and/or pressured into in regulating the behaviour of consumers, users and corporations. The third controversy is the growing online presence of the intelligence agencies and military cyber commands and the implications this has not only for privacy but also for the integrity of the Internet's technical operations. The fourth and final controversy concerns attempts by states to nationalise parts of the Internet and what this means for its operation and functionality of the Internet as a whole. Each of these controversies involves actual or potential infringements of the principles of universality, interoperability and accessibility caused by actions, policy and legislation that place national and/or economic interests above the interests of the Internet's public core.

Chapter 5 presents conclusions and recommendations. The conclusion of this book is that it is technically possible to damage the integrity and reliability of the Internet's public core, making its operation as a whole unreliable. It would therefore benefit Internet governance to organise public and private power and counterpower in a way that enhances the integrity of the Internet and freedom online.

Based on three principles of negarchy – division, mixture and restraint – a number of recommendations are made to shape a new international agenda for Internet governance. The first item on that agenda should be to secure the Internet's public core against improper state interference driven by national interests. A norm of non-intervention should be adopted for the Internet's core architecture. The second aim is to reframe international cyberpolitics so that Internet governance and national or international security are demarcated, for example by making a clearer distinction between different forms of security and the parties involved. The third aim of the agenda concerns cyber diplomacy and involves broadening the diplomatic arena and investing in new international coalition-building.

NOTES

1 See: http://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-Internet-cia.

2 Because it is technically possible to exclude people from the Internet, economists refer to it as a 'club good', i.e. a good whose benefits accrue only to members. My decision to refer to it as an impure global public good is based on the technical and protocol-related set-up of the Internet as described above, with universality, interoperability and accessibility as its core values.

3 Unless otherwise stated, all figures in this section have been taken from Internet World Stats: www.Internetworldstats.com.

4 Good data is in short supply because many threats play themselves out in the private commercial domain. Because they fear damaging their reputations, companies are not keen for their vulnerability to become public knowledge. Cybersecurity companies (the MacAfees of the world), on the other hand, find it useful for companies to regard threats as major incidents. And information provided by intelligence services adds to the sense of threat: it cannot be verified and may also be biased (see also Broeders 2014).

5 See, for example, the Human Rights Watch (2012) report *In the name of security,* which analyses 130 countries that introduced or amended counterterrorism legislation in the wake of 9/11. Many of these 'post-September 11 laws, when viewed as a whole, represent a broad and dangerous expansion of government powers to investigate, arrest, detain, and prosecute individuals at the expense of due process, judicial oversight, and public transparency' (p. 4).

6 See: http://link.springer.com/book/10.1007%2F978-3-319-04093-6.

2 FREEDOM, SECURITY AND INTERNET GOVERNANCE

> Internet governance structures were originally based on familiarity, trust, and expertise and on 'rough consensus and running code'. Things have changed.
> Laura DeNardis (2014: 18)

2.1 INTRODUCTION: STATES AND INTERNET GOVERNANCE

The future of cyberspace depends on the extent to which governments show themselves capable of pursuing their national interests on the Internet without damaging its public core. It also depends on the continued efforts of a large number of private, commercial, technical and civil-society parties that have made the Internet what it is today. In practical terms, they are the Internet's mainstay and the engine that has driven its turbulent growth over the past thirty years. The fact that states are now claiming a bigger role for themselves will not change that entirely or any time soon. Milton Mueller (2010: 8) uses the notion of 'networked governance' to describe this multi-actor system; technically speaking, the Internet is a network of networks involving a large number of networked actors who must resolve issues of 'rights, authority and distributional conflict' in cyberspace. Collaboration is by no means a given, however: 'what is a loose network today may become a more institutionalized – and possibly hierarchical – form of interaction tomorrow' (Mueller 2010: 8).

The time has come to give serious thought to this latter idea. For various reasons of their own, states are putting pressure on the institutions currently active in Internet governance. Some do so because they want more leeway to control the use of cyberspace in their own territory and to 'nationalise' the net. One example is the debate about whether the US Department of Commerce should continue to oversee the work of the Internet Corporation for Assigned Names and Numbers (ICANN), which issues and administers IP addresses and domain names (known as the 'IANA functions', for Internet Assigned Names Authority), or whether oversight should be transferred to another party, such as the United Nations, for example its International Telecommunication Union (ITU). A key factor in this debate is opposition to the influence that a single state, the US, is exerting on ICANN. State pressure may also be motivated by a perceived need to tighten up cybersecurity. Lewis (2013: 3), for example, states that 'the greatest challenge to the legitimacy of the existing multi-stakeholder structure is its failure to make the Internet more secure'. Other states claim that the structures that have evolved over the past thirty years have not kept up with the changing landscape of international politics, both in cyberspace and beyond.

The current emphasis on national security does raise serious questions about the way state influence is growing in cyberspace, however. Ronald Deibert (2013a: 9-10) puts it this way:

> There is an instinctive tendency in security-related discussions to default to the tradition of realism, with its accompanying state-centrism, top-down hierarchical controls and erection of defensive perimeters to outside threats. In the creation of cyber commands, in spiralling arms races among governments, in 'kill switches' on national Internets and in the rising influence of the world's most secretive agencies into positions of authority over cyberspace, we see this tradition at play.

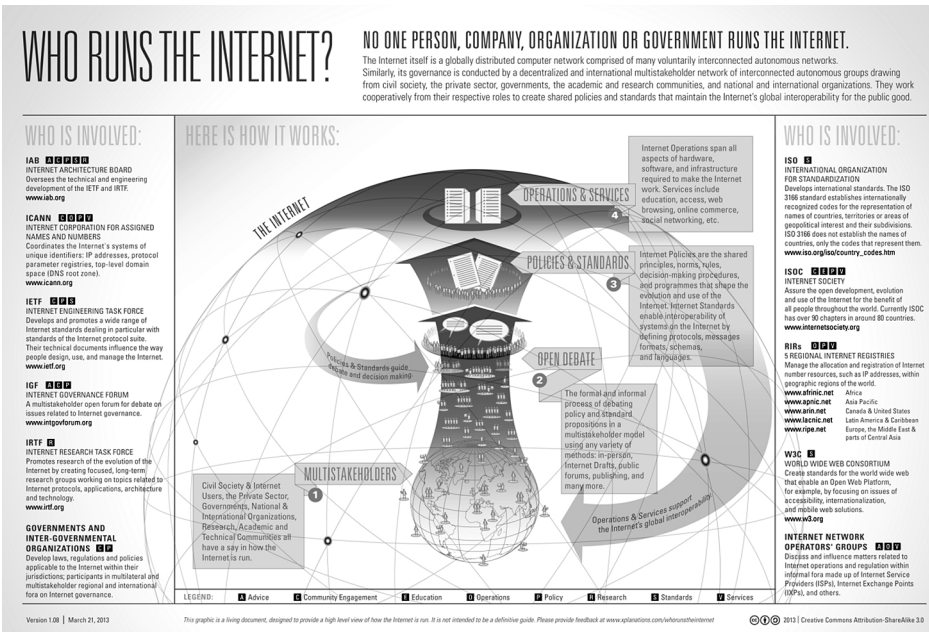
Others share his concern, but also feel that it is no more than logical for states to claim their place in Internet governance. The transition to a system in which governments gradually replace the informal communities that currently dominate Internet governance, or at least have a say in matters, is both desirable and unavoidable, according to Lewis (2013: 6): 'The definition of borders in cyberspace is no more a balkanisation than the existence of borders in the physical world; only those who still believe in the one-world global commons could interpret this as such.' The borderless nature of cyberspace (and its governance) is a victim of the Internet's own success. This book argues that states will have to be facilitated in their desire to represent their national interests in Internet governance while ensuring that the Internet's core infrastructure continues to operate as it should.

This chapter elaborates on this idea by placing it in an analytical framework. Section 2.2 begins by explaining the notion of Internet governance. The literature tends to concentrate on the broad spectrum of organisations involved, but that can obscure *what* precisely needs to be governed, and why. We emphasise governance of the various technical and socio-technical layers of the Internet, and only then consider the organisations involved. Section 2.3 delves deeper into this subject by drawing a distinction between 'governance *of* the Internet's architecture' and 'governance *using* the Internet's architecture'. It is mainly the first form of governance that applies to the Internet as a global public good, but that public good can also be put at risk when states initiate national policy that intervenes fundamentally in the Internet's architecture (i.e. governance *using* the Internet's architecture). Section 2.4 describes the model of 'distributed security', as a potential basis for a foreign policy on cyberspace. This model is based on the notion of freedom as a fundamental value and involves three principles that are intended to safeguard that freedom – mixture, division and restraint – in the process of policymaking, and more specifically policymaking aimed at international security. Finally, section 2.5 argues that securing the Internet as a global public good is essentially an extended national interest.

2.2 SETTING THE SCENE: INTERNET GOVERNANCE

The Internet is governed by a coalition of formal and more informal organisations that control certain components of access to the net, the distribution of scarce resources (such as IP addresses), and data transmission. Much of that control is embedded in a variety of different protocols and standards that function as the 'rules of the road' for Internet traffic. The system as a whole is referred to as 'Internet governance', which Milton Mueller (2010: 9) describes as 'the simplest, most direct and inclusive label for the ongoing set of disputes and deliberations over how the Internet is coordinated, managed, and shaped to reflect policies'. Because a wide variety of different parties contribute to Internet governance, some of them officially and others in an informal capacity, we refer to the system as a 'multistakeholder model'. Figure 2.1 describes some of the many actors, organisations and forums involved in Internet governance and shows how difficult it can be to see the wood for the trees. It is often not clear which decisions are taken where and what role, influence and position the various stakeholders actually have in Internet governance.

Figure 2.1 Stakeholders in the Internet ecosystem



Source: ICANN

Some commentators have also noted that 'Internet governance' and the relevant organisations involved in it describe only partially the forces that are actually driving the Internet's development. Van Eeten and Mueller (2013) believe that the academic literature's preoccupation with official organisations such as ICANN, the Internet Governance Forum (IGF) and the World Summit on the Information Society (WSIS) ignores other structures, issues and domains that have as much, if not more influence on how the Internet is actually governed, for example the economy of cybersecurity, net neutrality, content filtering and regulation, copyright protection, peer-to-peer file transfer, and the Interconnection Agreements between ISPs. In their view (2013: 730), it is in these arenas where much of the Internet's actual governance takes place.

Internet governance thus seems to fit the description of multi-centred or polycentred governance, where there may not be a clear-cut hierarchy between the actors (see Marks and Hooghe 2004: 21). In political terms, hierarchy scarcely plays a role on the Internet. There is no state, business or organisation that governs the 'the Internet' as a whole. The protocols and standards – to which many of the actors involved have contributed – lay down the technical laws and rules according to which the Internet itself operates. That is why some researchers refer to 'infrastructure-based forms of Internet governance' (DeNardis 2012; 2009) or a 'regulatory shaping of "code" – the technologies that underpin the Internet – to achieve more efficient outcomes' (Brown and Marsden 2013: ix).

This book approaches Internet governance not by looking at the many organisations that concern themselves with cyberspace, but by considering, at least initially, the technical operation of the Internet, especially those parts that can be regarded as a global public good. What we mean by 'Internet governance' becomes clearer if we analyse the Internet's architecture as a layered structure. Table 2.1 summarises four different academic views of the Internet. While the four views agree on the essentials, they also differ on some points or emphasise other aspects.

Table 2.1 The Internet as a layered structure, four times over

Brown en Marsden (2013: 8)	**Libicki** (2009: 12)	**Choucri** (2012: 8)	**Deibert** (2012: 5)
Content			
Applications			
Presentation			
Session			
Transport (TCP)		Actors	Level of ideas
Network (IP)	Semantic layer	Information content	Regulatory level
Data Link	Syntactic layer	Logical building blocks	Code level
Physical	Physical layer	Physical foundation	Physical infrastructure

The layers in each column can all be reduced to three. The lowest layer encompasses the physical and technical infrastructure, which makes data transfer possible and is part of the global public good. The top layer is the socioeconomic layer, where money is generated and people interact. This is the everyday face of the Web. It is where the political battle over the Internet and what is and is not permissible in its 'public' area is fiercest. It is not a global public good, however. Finally, there is the middle layer, which consists of protocols, standards, codes and organisations that keep the net's hardware and deeper layer of software running, and that states see as important for regulating cyberspace, both nationally and internationally. Some parts of this layer may be regarded as part of the global public good, whereas others may not, or to a lesser extent. The precise boundaries are difficult to determine; everything is subject to change and opinions differ on this score. This is the layer where engineers, businesses, international organisations and governments battle over what should be defined as a global public good. If so defined, it merits our special protection.

2.3 TWO FORMS OF INTERNET GOVERNANCE

To clarify the key elements of Internet governance, we follow Laura DeNardis (2012; 2013; 2014). She makes a vital and very useful distinction between 'governance *of* the Internet's infrastructure' and 'governance *using* the Internet's infrastructure' (DeNardis 2012: 726). Governance *of* the Internet's infrastructure concerns the deeper layers of the Internet and how they are organised and developed. In other words, this is about governing the system under the bonnet, the engine that drives the Internet's development. It covers a number of the critical infrastructures and protocols that we can regard as a global public good. In the case of governance *using* the Internet's infrastructure, the Internet is deployed as a tool in the battle to control content on the net. The issues vary from protecting copyright and intellectual property to government censorship and surveillance of citizens. While such control plays a significant role in Internet governance, international politics and the protection of human rights, it does not affect the Internet as a global public good – at least not normally. Occasionally, however, it does – specifically when states intervene extensively in the Internet's infrastructure for reasons of security or other national interests.

2.3.1 GOVERNANCE OF THE INTERNET'S INFRASTRUCTURE

The governance *of* the Internet's infrastructure is concerned with the deeper layers of the Internet, the essential technical and logical infrastructure. At its most basic, the answer to the question 'When is someone on the Internet?' is 'When that person is using the Internet Protocol (IP)'. The IP is one of the crucial standards that allow us to regard the Internet as a global public good. DeNardis (2013) lists three areas of Internet governance that play an important role in the most basic layer. They are (1) control over 'Critical Internet Resources', and especially control over

domain names, top-level domain names and IP addresses; (2) the defining of Internet standards and protocols (for example the TCP/IP protocol); and (3) the Interconnection agreements, which regulate and set prices for the traffic between the various networks that make up the Internet. While these three areas of governance also cover things that are not part of the Internet as a global public good, they are useful as initial categories. There are also many standards and protocols that are important to the Internet or the WWW but do not contribute to it as a global public good. One of these is the infamous BitTorrent Protocol, a protocol for peer-to-peer file sharing, which in the public's mind has become synonymous with piracy. While convenient, it does not affect the Internet's core infrastructure. The IP, on the other hand, lays down the standard that permits all participating computers to share and exchange any type of data, contributing to the universal and non-rivalrous nature of the net. The Hypertext Transfer Protocol (HTTP) regulates how 'clients', for example a search engine, communicate with 'servers', i.e. the computers that host a website or other content. That makes it one of the core protocols.[1]

As a global public good, the Internet operates properly when certain core values or principles underpinning its functioning as a system are guaranteed. We can also ascribe certain values to the security of the data circulating on the Internet or, put better, the data that users circulate on the Internet. These values are summarised in Table 2.2. Whether we trust or distrust the Internet depends on their presence or absence.

Table 2.2 Values related to the operation of the Internet and data security

Internet core values	Internet design principles	Key aims of data security
Universality Interoperability Accessibility	Openness Interoperability Redundancy End-to-end	Confidentiality Integrity Availability
DeNardis (2013: 4)	Ziewitz and Brown (2014)	Singer and Friedman (2014: 35)

DeNardis (2013: 4) identifies three core values: universality, interoperability and accessibility. They ensure that – all things being equal – the Internet operates in the same way in The Hague as it does in New York or Bangalore. They took precedence while the net was being developed and support the idea of it as a global public good. Ziewitz and Brown (2014) list four design principles covering approximately the same territory: openness, interoperability, redundancy and 'end-to-end' (the principle that application-specific functions ought to reside in the end hosts of a network rather than in intermediary nodes. The network itself is neutral or 'dumb'). The third set of values is based on the idea of data security and has three key aims:[2] confidentiality, integrity and availability (Singer and Friedman 2014: 35). Confidentiality means being able to assume that our information and data will remain private. Integrity means that the system and the data it contains cannot be

altered without proper authorisation. Without integrity, in other words, we can no longer trust the system. In cyberspace, integrity is closely linked to routing, for example. Technically speaking, the Internet is designed so that packets of data are always sent and routed, regardless of their content. If the Internet's integrity is put at risk and we no longer know whether data will arrive or may be altered en route, we may lose confidence in the Internet and in the social and economic activities that we now perform in cyberspace and entrust to the Internet infrastructure. Availability is the most obvious of the three, and also touches directly on reliability and confidence.

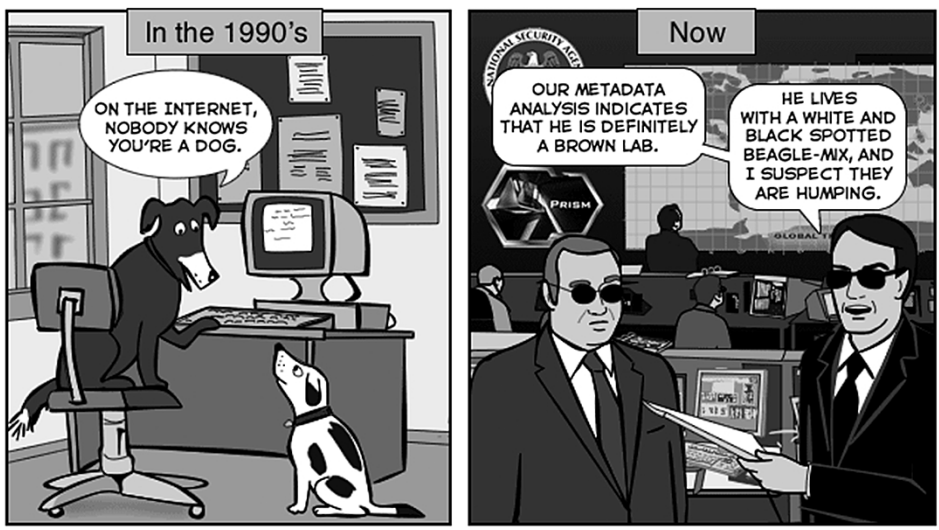
The three sets of values and aims are basically complementary. The core values of the Internet and its architecture are supported by the key aims of data security. Together they safeguard the integrity with which the Internet operates as a public infrastructure and, in doing so, act as signposts for governing its infrastructure as a global public good. Users trust the Internet because that infrastructure operates properly, and that implies that the relevant governance structures also operate properly. We define users broadly to include everyone from individuals to small and very large public and private users. The problem is that these values are not the specific responsibility of any one party or organisation. Basically, all the organisations involved in the governance of the Internet are responsible. That is naturally a difficult basis from which to operate, especially now that other parties with narrower political and economic interests are demanding a bigger role – whether or not we view such demands as legitimate within the context of Internet governance. That is why we have to acknowledge the importance of these values by adopting the more procedural perspective of 'distributed security', which we will discuss in section 2.4.

2.3.2 GOVERNANCE *USING* THE INTERNET'S INFRASTRUCTURE

The second form of governance attempts to regulate the conduct of individuals, groups and businesses ('the governed') by using the Internet, or technical aspects of it, as an instrument. Governance of this kind often involves matters of national policy – restricting freedom of expression, protecting intellectual property rights and copyright, improving security and fighting crime – using the Internet's infrastructure as a regulatory tool. It is difficult to regulate the public space of the Internet because it is essentially a global system. At the same time, however, that global public space also contains an identifiably national space, for example owing to language (e.g. Dutch-language websites), domain names (e.g. .nl), and links to people, organisations and businesses active (in this example) in the Netherlands. What complicates regulatory matters even more is that this space is both international and national. Few people would now claim that this public space and the people and organisations that populate it cannot be regulated. As described in Chapter 1, China (and many other countries) have managed to nail Bill Clinton's Jell-O firmly to the wall. In recent years, businesses and governments have effectively broken

down the user anonymity which so typified the early days of cyberspace. Today, only those who use encryption and TOR (The Onion Router) or PGP (Pretty Good Privacy) software are difficult to trace and identify online. In a world of Big Data, cloud computing, the Internet of Things and mobile Internet, we have become increasingly transparent and traceable. The dog in Peter Steiner's famous 1993 cartoon for *The New Yorker* ('On the Internet, nobody knows you're a dog') is no longer quite as anonymous as he once was.

Figure 2.2 Anonymity in cyberspace, then and now



Source: The joy of tech

At the same time, much of the Internet – the 'deep Web' – remains uncharted territory for most users and beyond the reach of regulators. The deep Web is also populated by all sorts of black markets – including the infamous Silk Road, a platform for selling everything from an online DDoS attack to an offline hit man, which has now been shut down (Ablon et al. 2014). Governments have enormous difficulty tackling cybercrime and cyberattacks, which often come from other countries and/or the deep Web.

Spurred on by a broad spectrum of national interests, states are attempting to intervene in the conduct of citizens, consumers and Internet users. Some do so by interfering with or tapping into the Internet's technical infrastructure, or through the intermediaries that facilitate Internet access to end users (Internet Service Providers or ISPs) and help them navigate the Web (e.g. search engines). Law enforcement and intelligence agencies request or commandeer data on Google and Facebook users in connection with criminal investigations. These companies in turn publish transparency reports[3] revealing which authorities make such requests and

how often they do so. Usually, they are prohibited from stating precisely *what* intelligence agencies have requested; in any case, it has now become obvious that agencies do not always bother asking for permission. Governments often target intermediaries in their attempts to control user behaviour, for example to prevent illegal downloads or abusive behaviour and slander. Many states use Internet intermediaries to spy on and censor activities of their nationals which are considered legal in many parts of the world and which are sometimes even protected under human rights law. ISPs, for example, are vital distribution points on the Internet, making them the ideal channel for government efforts to block child pornography, censor political opinion, and everything in between. In the realm of international relations, this form of Internet governance touches on the vital issues of Internet freedom and the protection of human rights in cyberspace.

Governance using the Internet's architecture can have direct consequences for the way the Internet operates as a system, for example when government policy imposes demands on or interferes with the Internet's core protocols and mechanisms. In that case, national policy intended to regulate the conduct of actors *on* the Internet also affects the core *of* the Internet – the global public good. A pertinent example from the US involves two pieces of legislation, SOPA and PIPA, designed to combat online piracy and protect copyright.[4] Had these bills become law, they would have intervened in the deep layer of the Domain Name System (DNS), which 'converts' the Web addresses that we all use (e.g. www.wrr.nl) into addresses (80.95.169.156) that the IP recognises. These laws would have allowed the US government to render infringing sites inaccessible, but they would have also put the stability of the entire DNS system at risk. Or, as DeNardis (2014: 8) put it: 'The SOPA/PIPA legislation would have required modifications to Internet governance technologies, changes with direct implications for security and freedom'. National policy of this kind corrodes the Internet's core values of universality and integrity (see also DeNardis 2013). This book looks specifically at governance that uses the Internet's architecture and also affects its operation as a global public good.

2.4 FREEDOM AS THE ANCHOR: DISTRIBUTED SECURITY

As an international network, the Internet is best served when there is enough freedom (to innovate and allow communication to flow freely) and enough security (to prevent damage and maintain confidence in its operation). Less clear is how policymakers can model and support freedom and security, especially at the international level. For example, the Netherlands has prioritised the freedom and security of (and on) the Internet in various policy documents (Ministerie van Veiligheid and Justitie 2011; 2013a; 2013b; Ministerie van Buitenlandse Zaken 2011; 2013; Ministerie van Defensie 2012; 2013), but these values, while fundamental, are also abstract and offer little guidance for everyday policymaking. Every country has its

own interpretation of freedom and security, including freedom and security on the Internet. The same is true, albeit to a lesser extent, of the core values, design principles and key aims of the Internet as described in section 2.3.1. Although they are more concrete than the concepts of freedom and security – and hugely significant when it comes to public confidence in the Internet – they can only offer guidance if they have the active support of the various parties involved in the Internet's governance structures. Once again, interests and interpretations can vary considerably. This book aims to support these values at both the abstract and more operational levels by developing a procedural perspective, based on a system of 'checks and balances', intended to protect the Internet's public core.

While acknowledging the inspiring nature of these fundamental core values, we shift the focus to a more *procedural* interpretation of security aimed at improving security whilst at the same time doing everything possible to safeguard freedom. In this regard we draw on Ronald Deibert's ideas about *distributed security* (2012; 2013a; 2013b; 2014). His model focuses on improving security while simultaneously imposing a system of checks and balances on and between the actors charged with state security. The liberal state is founded on the concept of freedom. Security should restrict that freedom as little as possible.[5]

> Distributed security emphasizes checks and balances on power, oversight on authority, and protections for rights and freedoms. It is part of a tradition emphasizing the negation of violence and power that is at the heart of liberal-republican theories of security going back to ancient Greece (Deibert 2012: 16).

Deibert argues that distributed security is especially important at a time when states are increasingly framing the Internet in terms of national security. Their natural tendency towards secrecy, the expanding influence and competences of government agencies responsible for national security and the often limited legal and democratic oversight on those competences must be contained within a model that checks that power and organises and embeds counterpower at the national and international level. Fundamental rights and freedoms will be better protected that way, and liberal states will be forced to develop a consistent national ideology of security and freedom that they can then propagate abroad. The structures designed to check and control political power on the Internet must be based on three principles (Deibert 2013a: 11-12):

- *mixture:* the intentional combination of multiple actors with governance roles and responsibilities in a shared space;
- *division:* a design principle that no one of these actors is able to control the space in question without the cooperation and consent of others;
- *restraint:* reinforcement of restraint on power, including checks and balances on governments, law enforcement and intelligence agencies.

These archetypal principles of the constitutional state draw on the age-old tradition of the separation of powers and power-sharing as developed in the Roman Empire and by the founding fathers of the United States. In a national context, they are easy to identify. The traditional ideal is the separation of powers or power-sharing between the executive, legislative and judicial branches of government, although it is seldom perfect even at the national level. Forms of oversight, accountability and shared responsibility for policy domains are further examples of *division, mixture* and *restraint*. The national context differs substantially from the international arena, however. International politics do not take place in a closed political system with a formal division of power, nor is it a democratic constitutional system with a defined citizenry, elected representatives, a government and a judiciary. That does not mean that it is bereft of laws; there are treaties, there is international law, and there are international and regional courts and tribunals whose rulings are binding. The point, however, is that there is no authority that consistently and systematically monitors compliance with these laws – although ad hoc coalitions, some deriving their political support and legitimacy from the United Nations, may enforce or oversee some rules and resolutions. International relations are based on the territorial integrity of sovereign national states. The Internet, a horizontal and global phenomenon, challenges this notion.

Interestingly enough, the current system of Internet governance already encompasses a number of elements consistent with the model of distributed security and its underlying principles of division, mixture and restraint. Specifically, these principles to some extent underpin the more technical aspects of Internet governance. Mueller et al. (2013) describe the technical community as cooperating non-hierarchically and voluntarily to solve Internet problems of the most serious kind, including cybersecurity threats (e.g. botnets and malware) or even issues affecting routing and other central processes. In that sense, the technical community is what Haas (1992) has described as an 'epistemic community': 'a network of professionals with recognized expertise and competence in a particular domain and an authoritative claim to policy-relevant knowledge within that domain or issue-area'. This is why Deibert believes in boosting these peer-to-peer communities and offering them firmer guarantees under a system of distributed security. However, that runs contrary to current tendencies: 'The general trend is towards more state involvement, hybrid forms of networked-hierarchical practices, growing secrecy, and politicization of technical standards' (Deibert 2014: 50).

Distributed security also connects the national level to the international; after all, 'a country cannot lament the loss of rights and freedoms internationally when those very rights and freedoms are being eroded at home' (Deibert 2012: 17). The most obvious example is the US's loss of moral leadership in the realm of Internet governance following revelations about the NSA's surveillance programmes (Greenwald 2014). The Snowden and Manning leaks have been detri-

mental to the US and they have also cast a shadow on the 'Western camp' in Internet governance matters, causing its members to question whether they actually share the same views on freedom and security. Besides the surveillance and espionage issue itself, this nervousness has therefore also impaired the Western international efforts and position at a crucial time, when many countries are choosing sides in matters of Internet governance. But the link between the national and international levels can also come in a very different guise. The preoccupation with cybersecurity is a modern-day, digital version of an old problem in international politics, known as the security dilemma. According to Jervis (1978: 169), a security dilemma exists when 'many of the means by which a state tries to increase its security decrease the security of others'. And how those others react to their decreased security can, in turn, decrease the security of the first state. Ultimately, a digital arms race may decrease the security of all, not to mention of the Internet itself. In Deibert's view, the principle of restraint is most at risk and should therefore receive the most attention in foreign policy.

2.5 CONCLUSION: INTERNET GOVERNANCE AND EXTENDED NATIONAL INTERESTS

Many countries in the world, at various stages of economic development, share a vital interest in a free, open and secure Internet. A number of the features that have led to the Internet's success and growth must furthermore be safeguarded and protected where necessary. As discussed earlier, some of the Internet's core components can be regarded as a global public good and warrant international protection. As a public resource, an open Internet is so beneficial to countries with an open economy and international outlook that it should be considered an 'extended national interest'. This term was coined by the Dutch Scientific Council for Government Policy (WRR) in 2010 to describe those areas where national interests align with strategic global issues that can be defined as global public goods. This provides a good starting point for a national diplomatic agenda on Internet governance. Governments need to explore (a) how global public goods relate to their national interests and those of their citizens; (b) where the most substantial interfaces between global public goods and national interests are located; and (c) how and how much governments would be willing and prepared to contribute to safeguarding such global public goods (Knapen et al. 2011: 47).

In the realm of Internet governance, a useful first step would be to draw an analytical distinction between 'governance *of* the Internet' and 'governance *using* the Internet'. Governance *of* the Internet is intended to safeguard those parts of the Internet that are part of the global public good, regulating its deep technological and logical layers and preventing states seeking to secure their national interests in cyberspace from impacting on the Internet's fundamental protocols and infrastructures in the process. The deep layers that embody the collective nature of the

Internet have become all the more vulnerable with the encroaching securitisation of cyberspace and states' demands to play a greater role in Internet governance. National policy can cause disruptions that eat away at the universality, interoperability and accessibility of the Internet as a whole (DeNardis 2014) or endanger the confidentiality, integrity and availability of the Internet as an information system (Singer and Friedman 2014). Such disruptions will undermine the Internet as a global public good and the digital substructure of much of our economy and society today. The values and principles reviewed above must be combined with a procedural outlook that can help us determine the future of Internet governance. Our suggestion is to apply the model of distributed security to Internet governance. This model improves security while imposing a system of checks and balances on and between the actors charged with state security. To safeguard freedom – the concept underpinning the liberal tradition on which distributed security is based – we must apply the principles of mixture, division and restraint as much as possible in designing a system and practice of Internet governance. These principles can ensure that power is shared, restrained, transparent, and made subject to oversight.

NOTES

1 The core protocols are sometimes grouped together under the label TCP/IP. In that case, they also include the Simple Mail Transfer Protocol (SMTP), the File Transfer Protocol (FTP) and the Hypertext Transfer Protocol (HTTP) (DeNardis 2014: 67).

2 Also referred to as the CIA triad: Confidentiality, Integrity and Availability.

3 See for example: http://www.google.com/transparencyreport/ and https://www.facebook.com/about/government_requests.

4 SOPA stands for the Stop Online Piracy Act and PIPA for the Protect Intellectual Property Act. Both have been withdrawn, probably for good.

5 Or, as Bauman et al. (2014: 139) put it: 'The liberal example is one of security through liberty, not security at the expense of liberty'.

3 GOVERNANCE OF THE PUBLIC INTERNET

> Internet governance functions have been around for far longer than the term Internet governance.
> Laura DeNardis (2009: 13)

3.1 THE INTERNET AS A GLOBAL PUBLIC GOOD

The Internet's public core embodies a number of abstract values. Universality, interoperability, accessibility, integrity, availability and confidentiality are the core values that guarantee 'the Internet' as a global system. In essence, they are about functionalities. Although rather ethereal in nature, the impact of this core is very practical in some respects. That is because the task of upholding these values and functions has been entrusted to institutions, protocols and standards that support and guarantee the core public infrastructure of the Internet. This chapter is about those institutions, protocols and standards, and about new issues that have arisen within that context in the wake of technological, economic and political change.

As the above quote by DeNardis (2009: 13) makes clear, Internet governance predates the term itself by many years. In the short history of cyberspace, however, that governance has changed and professionalised considerably. The paper notebook in which Internet pioneer Jon Postel kept a list of who had been assigned which IP address was replaced long ago by ICANN, a professional organisation that now administers the almost four billion IP addresses issued since those early days. ICANN, which acts as the Internet Assigned Numbers Authority (IANA), has become controversial and a fierce debate is raging as to whether this particular *organisation* is the best candidate to perform this critical Internet governance *function*. In other words, while a particular solution may have made sense in the past, it is not necessarily the best choice in the present or future. As long as the values underpinning the Internet are safeguarded, the question of *who* performs a given function is less important than that it is actually performed. The Internet's growth has created governance problems that go far beyond the need to replace Jon Postel's notebook. Some of these are technical and related to the growth of the network itself (for example the need to update the Internet Protocol from version 4 to version 6). Other problems have found their way onto the agenda because the Internet's growing economic and political significance has attracted new parties and stakeholders, some of which meddle in the technical operation and management of its public core. Engineers now find that other parties – parties with economic and political or geopolitical interests – are taking an interest in the operation of the net, leading to mounting tension in some areas.

Basing ourselves on the terminology used in Chapter 2, we speak of the governance *of* the Internet's infrastructure when referring to the core of the Internet as a public good. Although it is not always clear what that core encompasses, there is no question that certain protocols and functions belong to the global public good of the Internet. Those protocols and functions are managed by a number of organisations. This 'Team Internet' – which consists of both the organisations and the protocols themselves – is highly efficient and effective in many ways, but falls short in others. Its shortcomings may be related to design flaws and technical incapacity, but also to political and economic pressures, stakeholder interests and questions of legitimacy. Section 3.2 begins by describing Team Internet. It explains what belongs to the public core of the Internet and which organisations manage and operate it. It also briefly reviews the achievements of Team Internet in terms of network growth, numbers of users, and social and economic wealth that has been built on the Internet's backbone. Section 3.3 reviews four major controversies *about* the governance of the public Internet. Such conflicts are more likely to have been caused by shifts in international political and/or economic relations than by dissatisfaction about the technical operation of the Internet.

3.2 TEAM INTERNET: STEWARDS OF THE INTERNET'S CORE

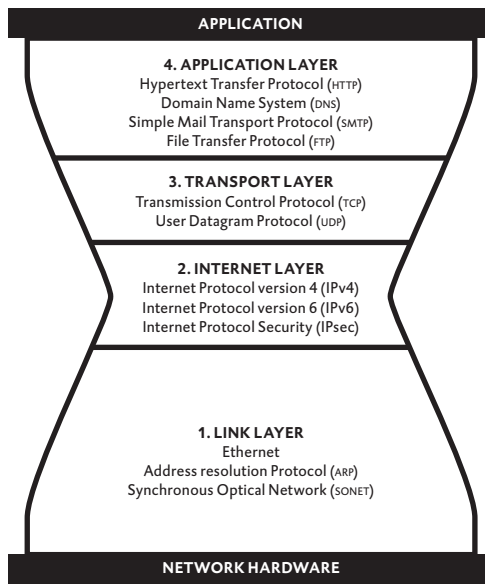
We can look at the governance of the Internet as a global public good in various ways. If we view it in terms of people and organisations, then its governance lies with those who develop, administer and operate the public core of the Internet. If we view it in terms of technology, then the protocols and standards – and in some cases the technical infrastructure – are important to governance. These functions and roles obviously overlap on some points. The point is that 'Team Internet' is made up of many different people and organisations – most of them active in the private sector and/or civil society, a minority in government – and of technical standards and protocols. Those protocols may well be technical or logical in nature, but that does not make them immune to interests, politics and power (DeNardis 2009; 2014; Mueller 2009; 2012; Brown and Marsden 2013). For every protocol that has been promoted to the status of a standard, there were alternatives that did not succeed for one reason or another. Software and protocols have a huge regulatory impact. 'Code is law', as Lessig (1999; 2006) put it. Politics and other manifestations of power do matter, and may be embedded right into the code and protocols themselves.[1]

The developers tend to be loosely organised groups of people and organisations that produce and discuss the software protocols and standards and finally 'elevate' them to standards. The quotation marks around this word indicate that it is ultimately worldwide acceptance that turns a protocol into a genuine standard. The key developers are the Internet Engineering Task Force (IETF), the Internet Society (ISOC), the World Wide Web Consortium (W3C) and similar organisa-

tions in which renowned, independent 'netheads' such as Vint Cerf and Tim Berners-Lee originally led the pack (Brown and Marsden 2013: 12). They come up with ideas for protocols and standards that regulate data transfer, interoperability, interconnection and routing between networks, and the format of the data transmitted across the Internet. IETF, for example, came up with the Internet Protocol, HTTP and HTML, which were later adopted by its partner W3C. These and a few other organisations constitute what is known in Internet terminology as the 'technical community'. They are relatively open in structure. For example, anyone can basically attend IETF meetings. They also clearly operate more in the private sector than in the public, and they have a huge impact on the protocols and standards that constitute the Internet's core.

The work of these developers provides the logical building blocks of the Internet itself, i.e. the protocols and standards that keep the Internet running and route data so that it reaches all corners of the world. The most important protocols are known collectively as the TCP/IP Protocol Suite. The Transmission Control Protocol (TCP) and the Internet Protocol (IP) are at the very heart of this suite. Without them, the net will not operate. The protocols in the TCP/IP Protocol Suite are divided into four layers: the link layer, the Internet layer, the transport layer and the application layer. Figure 3.1 lists the core protocols in each layer.

Figure 3.1 The TCP/IP Protocol Suite



Source: Adapted from DeNardis 2009: 8

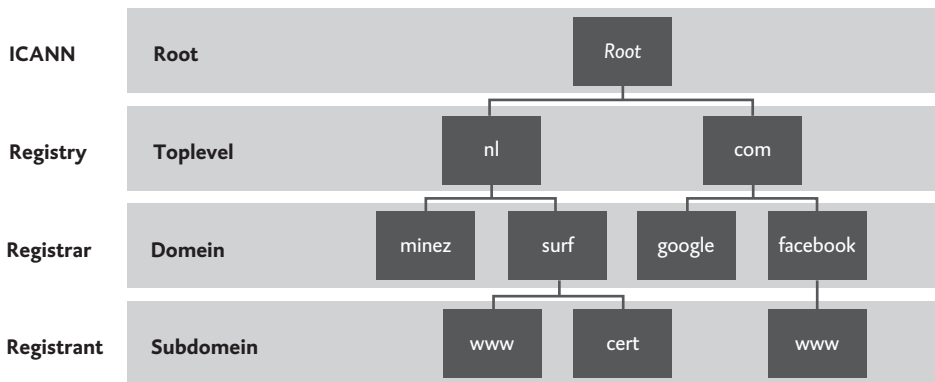
Each layer in the model plays a crucial role in communication over the Internet. The application layer contains digital data in a form that 'ordinary' people can comprehend, such as text and numbers. The two layers below this – transport and Internet – regulate the way information is converted into bits and bytes and divided into packets that are transmitted over the Internet's networks. The link layer ensures that data can move across the entire net, regardless of the hardware connection (i.e. wireless or cable). As its name implies, the Internet Protocol or IP is the most crucial protocol for the operation of the Internet. The layered model is sometimes depicted as an hourglass, with IP as the narrowest part. The protocols in the other layers function as alternatives for each other (transport is possible via TCP *and* UDP) but the Internet layer only operates via IP, at least at the present time (DeNardis 2009: 9). All these protocols are vital to the Internet's operation in their own way, but a few of them stand out within the context of this study because they (a) embody certain values that underpin the Internet as a global public good and/or (b) have been targeted by private parties and, specifically, by states as channels for controlling the Internet or for exercising control *using* the Internet. The main targets are TCP/IP and DNS because they generate the Internet's most critical resources, i.e. the Internet addresses that facilitate communication and the domain names for Websites. These 'Critical Internet Resources' (CIRs) are 'virtual, Internet specific, globally unique resources rather than physical architecture or virtual resources not specific to the Internet' (DeNardis 2014: 36).

Before TCP/IP was elevated to a standard, devices manufactured by IBM, for example, could not communicate with those manufactured by Apple. TCP/IP lays down the standard for data transport and requires every device that sends and/or receives information over the Internet to have a device or session-specific IP address (a unique number). Without this address, data cannot be sent or received. During transmission, TCP/IP breaks the data down into small packets and adds a header containing the source and destination IP addresses and the correct packet sequence. The packets take different routes through the networks that together constitute 'the Internet' and are only reassembled in the correct order when they have arrived at their final destination. The network (the routers, the Internet Service Providers) does not review the packet content but is only concerned with identifying the most efficient route, depending on the degree of network congestion. This is known as the end-to-end principle, which, in its most extreme form, considers the network to be 'dumb'. The principle states that data content and data processing ought to reside in the end hosts of a network, i.e. the computers of the sender and receiver. The network itself is neutral, or 'dumb', and merely relays the data. Or, as the technical community explained in *The Architectural Principles of the Internet*: 'the goal is interconnectivity, the tool is the Internet Protocol, and the intelligence is end to end rather than hidden in the network' (cited in Ziewitz and Brown 2014).

Critical Internet Resources

IP addresses are critical Internet resources because they make it possible for two unique users to communicate. Since IP addresses are unintelligible to ordinary users and difficult to memorise, the pioneers of the Internet introduced domain names. A domain name, for example www.wrr.nl, represents the user's IP address, which remains invisible. This means that domain names must also be unique and can only be issued once to a single person or organisation. Certain domain names are obviously extremely valuable. The Coca Cola Company is very keen to own www.cocacola.com, www.cocacola.nl and other such domain names because they are logical places that people interested in Coca Cola will seek out. The task of issuing domain names is entrusted to a hierarchical structure made up largely of private organisations. At the top of the pile is ICANN, a 'non-profit public benefit corporation' incorporated under the laws of California. ICANN manages the root zone (the 'dot' in a Web address) and issues the top-level domain names, the broadest category to which websites are assigned (the letters to the right of the dot). These can be either generic top-level domains (TLD) such as .com or .org, or a country-code TLD such as .nl. The TLDs are entered into registries. The US company Verisign, for example, administers the generic TLD '.com' registry, while the Dutch company SIDN does the same for the country-code TLD '.nl'. The next level down are the 'registrars', businesses and organisations authorised to sell names to customers within a specific domain. The hierarchy is shown in Figure 3.2.

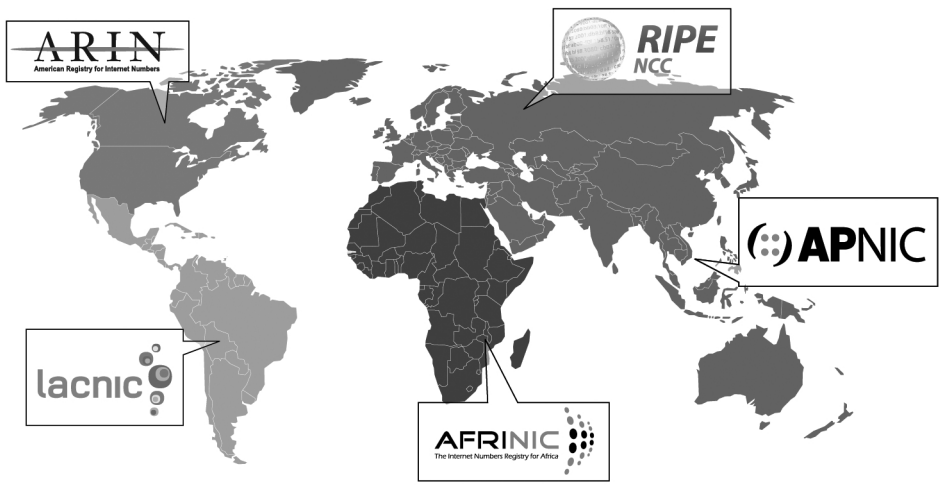
Figure 3.2 The hierarchy of Internet domains and domain names



Mueller (2002: 2-6) stresses that the importance and value of domain names and IP addresses – which lie at the core of the Internet's operation – may be conceptualised in two different ways. If they are handled poorly, the Internet could 'break', but at the same time they have been turned into marketable commodities that can even be worth a lot of money. In other words, they are critical to the Internet's operation as a global public good, but they also have an economic and political value. This means that economic and political interests figure in the debate. These

critical Internet resources are created by issuing new domain names and IP addresses. Their administration consists of registering IP addresses and domain names, updating the registry and making it accessible to the public. ICANN is the top organisation in both respects (issuing and administration). It is the only organisation authorised to create new top-level domain names (for example .apple, .shop and .xxx) and to manage the root of the Domain Name System (DNS). ICANN – under a contractual relationship with the US Department of Commerce – is responsible for issuing IP addresses (one of the IANA functions), which they allocate in large blocks to five regional organisations (Regional Internet Registries, RIRs); see Figure 3.3. The RIRs in turn allocate smaller blocks of IP addresses to local registries; they in turn distribute these blocks to Internet Service Providers and, finally, to end users. Some regions are running out of IP addresses. To address this problem, Team Internet decided in 1995 to develop and launch a new version of the Internet Protocol (IP version 6 or IPv6), which has an almost infinite number of addresses. The transition to IPv6 has been slow, however; it involves making changes deep in the Internet's core infrastructure and all around the world.

Figure 3.3 RIR allocation of IP addresses



Source: ARIN

Domain names must be unique so that the packets of data sent over the Internet reach the correct destination. They must also be linked to an IP address. That process is managed by the DNS. DeNardis (2014: 41) describes it this way: 'The DNS is a look-up system that handles billions upon billions of queries per day locating requested Internet resources. It is an enormous database management system (DBMS) distributed internationally across numerous servers with the purpose of providing the locations of resources such as a website, email address, or file'.

An international network of 'root' servers – a disproportionate number of them located in the US and Europe – ensures that the data packets arrive at the appropriate destination. The operation of the Internet thus depends on a DNS that is consistent and accurate.

Operators: Internet exchanges, CERTs and ISPs

In addition to the core infrastructure of protocols, standards and organisations, there are many other components that play a vital role in facilitating Internet traffic as we know it. Without Internet exchanges such as AMS-IX in the Netherlands and the undersea cables that link the continents, worldwide communication would be impossible. Routing agreements between the various networks that collectively make up the Internet govern how data move across the world. And the various public, private and mixed Computer Emergency Response Teams (CERTs) work to keep the local, regional and international Internet healthy by battling Distributed Denial of Service (DDoS) attacks, viruses and malware. Internet Service Providers or ISPs are usually the most direct link between users and the Internet. They give users access to the Internet and often provide other services, for example domain name registration, e-mail services or website hosting. As a vital link in the Internet's socioeconomic domain, ISPs are also often the go-to organisations to facilitate and execute interventions in the online world for political (law enforcement, censorship, security) and economic (copyright) reasons.

3.2.1 THE OVERWHELMING SUCCESS OF TEAM INTERNET

Team Internet has a fantastic track record when it comes to the Internet's growth. As mentioned earlier, we can scarcely imagine our social, cultural and economic lives now without the Internet. It is a fundamental and ever-expanding part of our economy and society, with 'our' digital society now being as tightly interwoven with the rest of the world as the Internet itself. Everyday life will only grow more closely intertwined with the Internet in the years ahead, especially as cloud computing and the 'Internet of Things' gather momentum. Storing data in the cloud severs their bond with a specific territory and location, while the Internet of Things will link our homes, our cars, our appliances and even our bodies to the Internet. Cyberspace has expanded in a multitude of different directions by making use of infrastructures, both existing (telephone, cable) and new (optical fibre and wireless networks). Governments have often played a vital role in that process, but in all other ways the Internet has developed without much government intervention into a network capable of accommodating virtually every new user, application and innovation. According to Zittrain (2008), it is precisely the open nature of the Internet – its open standards and protocols, which lower the threshold for anyone with promising new ideas – that have allowed it and everything that depends on it to thrive. Statistics on the number of users and websites and the online economy speak volumes about the success of a network that had such humble beginnings.

The Internet as a whole is often described as a 'best effort network'. This means that the interaction between the various component networks and providers combined with the basic protocols render the best service possible by making efficient use of the available bandwidth, but without guaranteeing a specific level of quality in advance. 'The Internet' does its best, but there are no guarantees. It is primarily the increase in bandwidth that has fuelled the growth of the Internet, especially as the number of bits and bytes being transmitted across the net has increased exponentially in recent years as its use has expanded. Text on the Internet has now been eclipsed entirely by photographs, music, videos and streaming, causing the pressure on the net to increase exponentially. By way of illustration: Netflix and YouTube – currently the two most popular streaming sites – are responsible for almost half the peak Internet traffic in the US (Anders 2014). Some have referred to the recent precipitous rise in available data as the 'data revolution' (Kitchin 2014). In 2012, IBM estimated that 90 percent of the data available worldwide had been created in the preceding two years. Numerous reports and analyses concur that the volume of data generated worldwide has increased exponentially and will continue to do so (Kitchin 2014: 69-72). Much of it is generated on or by the Internet, and/or is transmitted across the network. Team Internet's greatest achievement is that so far, cyberspace has been able to accommodate this tremendous growth without either imploding or exploding. However, the Internet's success has also made it more interesting for economic and political stakeholders. This means that the engineers are now finding that other parties – parties with economic and political interests – are taking a major interest in the Internet and its operation.

3.3 PROBLEMS IN THE GOVERNANCE OF THE INTERNET AS A GLOBAL PUBLIC GOOD

The governance of the Internet has run into problems over time. For example, its exponential growth led to the IPv4 exhaustion problem. Moreover, technological advances such as Deep Packet Inspection (DPI) create new opportunities to monitor data traffic, and conflicting political and economic interests lead to debates about how IP addresses and domain names should be issued and administered. Opinions about cybersecurity are also changing. In all these instances, the technical approach of Team Internet is often at loggerheads with the political and economic interests of other parties. Even the introduction of IPv6 – on the face of it, purely a technical update – has become bogged down in economic interests and political impasses. These debates can be viewed in different ways, but can also be framed as a conflict between the collective significance of the Internet as a global public good versus more narrowly defined national, political or economic interests. We briefly discuss four of these debates below. Our object is to distinguish the collective infrastructure of the global public good – which must not become the plaything of national political interests – from those aspects of the debate which, whether we like it or not, have an inherently political component. The debates are

(1) the collective problem of updating the Internet Protocol to version 6; (2) the discussion concerning stewardship of the IANA functions and the controversial role and position of ICANN; (3) the debate about Deep Packet Inspection and net neutrality; and (4) the discourse about changing attitudes towards cybersecurity and how it should be tackled.

3.3.1 A COLLECTIVE ACTION PROBLEM: THE (NON-)ADOPTION OF IPV6

The Internet's growth is based on a stock of available IP addresses that can hook up new users and applications to cyberspace. Of course, that means that there has to be a plentiful supply of such addresses. The current protocol, IPv4, is running out of steam, even though its inventors were visionary enough to create roughly four billion unique IP addresses at a time when there were only a few thousand users. ICANN, as the Internet Assigned Names Authority or IANA, allocated the last four blocks of IPv4 addresses in 2011. Two regions, RIPE-NCC (Europe) and APNIC (Asia), have already exhausted their entire allotment of IPv4 addresses (OECD 2014a: 14) and are facing an acute shortage. The transition to the latest protocol, IPv6, has been slow, however. The new protocol would immediately solve the exhaustion problem because it provides for the creation of 340 undecillion unique IP addresses (3.4×10^{38}). Although the technical community had warned about IPv4 exhaustion as far back as 1990 and the new IPv6 standard was already available in the decade that followed (DeNardis 2009), the adoption of IPv6 has been lamentably slow. Belgium (29%) and the US (10.2%) are in the lead; a handful of countries have an adoption rate of between 3 percent and 10 percent, and the rest lag far behind, with 0 percent adoption being common in some parts of the world.[2] The biggest problem is that IPv6 does not have 'backward compatibility' with IPv4. In other words, until everything and everyone has transitioned to IPv6, we all need to maintain two IP addresses to guarantee the reception of data. That makes IPv6 adoption a collective action problem. Those who are unable to obtain IPv4 addresses because the stock in their region has been exhausted will benefit from IPv6 adoption, but to communicate globally, they have to depend on other users adopting the new protocol as well – including users who can still obtain IPv4 addresses. The transition is also expensive and requires an investment on the part of ISPs without giving them a 'first-mover advantage', since issuing IPv6 addresses does not give their existing customers any noticeable extras.

DeNardis (2014: 81) explains this less than ideal situation as the outcome of the technical community's culture and strong sense of solidarity: 'Although retrospectively this seems like a design problem, at the time IPv6 was selected, the assumption was that Internet users would want to upgrade for the network's overall good'. But today's billions of Internet users no longer feel that solidarity. Others point out that the IPv4 format simply did not have the space to accommodate a compatible extension.[3] Today, along with the upgrade to IPv6 – which as stated is proceeding extremely sluggishly, although some believe that is changing

(Czyz et al. 2013) – an international market has emerged for IPv4 addresses that have been allocated but not yet used (Mueller and Kuerbis 2013). The non-transition to IPv6, the trade in IPv4 addresses and the persistent use of technical tricks (middleware) allowing multiple users to 'share' a single IP address are affecting the stability of the Internet and leading to fragmentation. Governments are also growing nervous about the non-transition to IPv6 because it could seriously damage the Internet economy, but they can do nothing to speed up or force the changeover (OECD 2014a: 7). All they can really do is plead and offer incentives, as the OECD did in its Seoul Declaration for the Future of the Internet Economy: 'Encourage the adoption of the new version of the Internet Protocol (IPv6), in particular through its timely adoption by governments as well as large private sector users of IPv4 addresses, in view of the ongoing IPv4 depletion.'

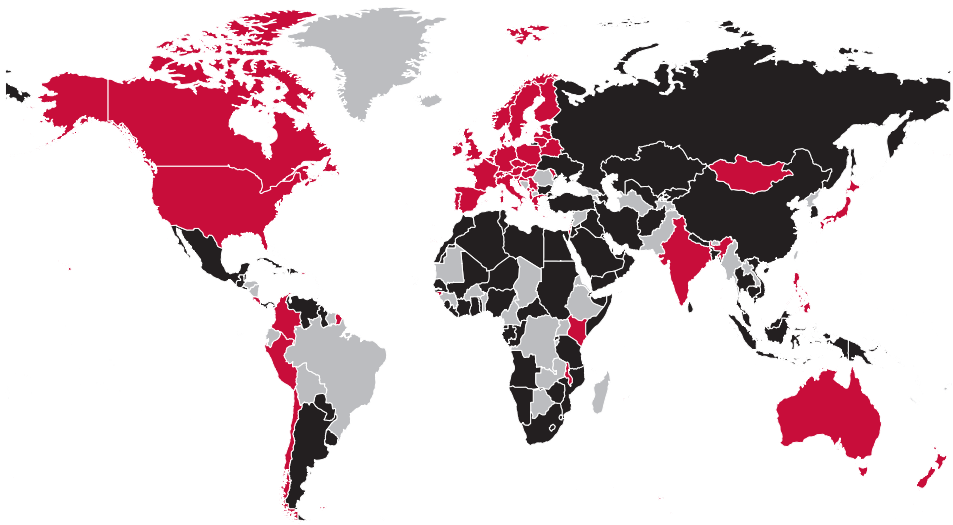
3.3.2 ISSUING AND ADMINISTERING IP ADDRESSES AND DOMAIN NAMES

IP addresses and domain names are issued and administered by the Internet Corporation for Assigned Names and Numbers (ICANN), a US non-profit public benefit corporation. ICANN was assigned these tasks – known as IANA functions – by the US government, which had funded the management of the Domain Name System (DNS) until then. Its decision has long been disputed because the contractual relationship between ICANN and the US Department of Commerce allows the government of the United States to influence the allocation of IP addresses and domain names, the Critical Internet Resources. Edward Snowden's recent revelations have damaged the US government's credibility as the guardian of a free Internet and added fuel to this debate. It has led to even more vigorous calls to alter a system in which ICANN and the US government play such a vital role. In March 2014, the US government itself opened the door to change by announcing its intention to end its relationship with ICANN in its present form. This was not the first time that the United States had made such an announcement, however. In the previous instance, it ended up simply renewing its contract with ICANN and nothing changed. Opinions are sharply divided about the US's announcement. Some commentators claim that President Obama is putting the Internet up for grabs and placing US national security at risk; others believe that other forms of oversight of the IANA functions could be equally effective (Zittrain 2014).

The discussion goes back much further than that, however. Many countries look askance at the US's privileged position in the management of what can be regarded as a global public good. Roughly speaking, there are two camps that wish to reform ICANN, or rather, oversight of the IANA functions pertaining to the allocation and administration of domain names and IP addresses. The first camp consists of the multilateralists, known in the Internet community as the proponents of 'multistakeholderism'. They believe that the best way to guarantee the future of the Internet is to place the management of its critical resources in the hands of a broad coalition of individuals, organisations, civil society, businesses and authorities.

The other camp consists of the nationalists, who want to alter the governance of the Internet to give states more control and authority over their 'own national Internet'. The first camp is mainly made up of people and organisations that populate the 'Internet community'. Many states also support the idea of multistakeholderism, though few of them would surrender their own (growing) influence entirely. Indeed, states are loath to let others have a say in what goes into official declarations and conventions on Internet governance, and NGOs consequently have only indirect and limited input into such matters (Cogburn 2010; Dutton and Peltu 2010). The second camp is headed by authoritarian states aiming to exercise the same control over their populations online as they do offline.

Figure 3.4 **Signatories and non-signatories to the International Telecommunications Regulations, 2012**



Source: Techdirt.com

The two camps fought over control of the Internet's 'names and numbers' through many different rounds without making any headway. That changed in 2012 during the World Conference on International Telecommunications (WCIT) in Dubai, when UN member states gathered to negotiate a new telecommunications treaty (the International Telecommunications Regulations, or ITRs) under the auspices of the UN's International Telecommunication Union (ITU). The new agreement, which many analysts believe opens the door to the balkanisation of the Internet, made it patently clear that the world is sharply divided on the subject of Internet governance: 89 states, including China, Russia and many Arab states, signed the new treaty, while 55 states, including the US, the EU member states, most other OECD members and countries such as Mongolia, India and Peru, refused to sign

and openly resisted the agreement. Figure 3.4, which is based on the ITU's own data, reveals how the world is divided on this point. The countries in red are those that refused to sign the new ITRs, and the countries in black are those that did sign. The votes of the countries shown in grey were not officially recorded for various reasons, for example failure to pay membership dues.

From a diplomatic perspective, it should be noted that the future of this debate does not lie with the countries at the opposite ends of the spectrum – they are unlikely to waver in their positions – but with the states in the middle. These 'swing states' or 'fence-sitters' are often well aware of the importance of internet governance issues and are emerging players at the international level (Maurer and Morgus 2014). Even in a well-integrated regional organisation such as the EU, member states do not agree on some points, and differ considerably in terms of know-how, strategy and even policy in cyber issues. Diplomatic efforts should therefore zero in on the countries with 'swing' potential. From all appearances, this is the time to forge new coalitions to complement existing ones. This is especially urgent given that the ICANN debate – while the best-known and most symbolic discussion on Internet governance – is unlikely to be the last debate to focus on the future of the Internet or its component parts.

As mentioned earlier, the Snowden leaks have dented the moral leadership of the US, something that has become very obvious in the ICANN debate. In April 2014, Brazil – one of the countries whose top officials had been targeted by the NSA – convened the two-day NetMundial meeting in São Paulo. Dismay over the Snowden revelations dominated the meeting, whose final resolution vigorously advocated the multistakeholder model for Internet governance. NetMundial boosted the search for a new way to truly globalise the tasks of ICANN without putting the stability of the net at risk. All sorts of parties have now joined the discussion. The European Commission, for example, stated in a Communication (2014) that it supported a 'genuine multistakeholder approach for Internet governance', arguing explicitly that contracts concerning domain names and IP addresses should not need to be concluded under California law. At times, typical state traditions resurface in proposals. The French Senate, for example, joined in the debate in July 2014 by issuing a lengthy report on the future of Internet governance. The report makes far-reaching recommendations to transform ICANN into W(orld)ICANN, make it subject to international rather than California law, and accountable to a World Internet Council whose members would be appointed by the UN member states (Sénat Français 2014). Some of these proposals were designed to increase the EU's influence in international Internet governance. While France's suggestion of replacing the political influence of a single state – the United States – by a multilateral executive is certainly an improvement, the proposal is also vulnerable to a policy of divide and conquer by states that would rather nationalise than internation-

alise the Internet. Despite the report's many references to the multistakeholder model, the French proposal to set up a political council would mainly end up increasing the power of states in Internet governance.

Many commentators see the ICANN debate as symbolic (see e.g. Zittrain 2014). ICANN has not really 'done that much wrong', and in fact has only two tasks related to the operation of the Internet (although they are crucial ones). The first task concerns the IANA functions, which roughly means administering the register of domain names and IP addresses and updating and maintaining the DNS (also known as root zone management). The second task is to expand and 'market' new top level domains (TLDs). This distinction leads Mueller and Kuerbis (2014) to draw an important conclusion: political interference in the first task should be kept to an absolute minimum, since it basically consists of technical and operational work. The second task is much more 'political' in nature. It involves determining which domain names are acceptable, how many IP addresses are required, and who or what should administer them. How the second task should be handled politically is a matter of preference and a sensitive issue, but it is – or should be – beyond dispute that the first task must remain outside the realm of political wrangling and influence so as to ensure the integrity and consistency of the technical system. Or, as Muller and Kuerbis (2014) put it: 'Many observers of the IANA controversy believe that root zone management is an appropriate site for public oversight and policy intervention. This is a mistake'. The IANA stewardship transition thus requires states to exercise the necessary restraint.

3.3.3 NET NEUTRALITY

The third debate that touches on the Internet's technical operation concerns net neutrality. Net neutrality is the principle that all data transmitted over a network should be treated equally. It is related to the end-to-end principle, based on the idea of a neutral or 'dumb' network that simply passes along data as it receives them. Net neutrality is a principle – the default setting for the IP and the Internet – and not an established protocol. The main question is whether an ISP (operating one of the networks that together comprise the Internet) may differentiate between different types of data that pass through its network by blocking, throttling or, conversely, prioritising it. Since net neutrality is mainly concerned with the speed at which data reach the end user – in most cases, the customer (the so-called last mile access) – it is often a regional or even national issue. Nevertheless, it is a point of concern in a host of different countries, has led to fiery debates in national and European political arenas, and influences how the Internet is perceived, how data traffic is handled, and how money is made on the Internet.

A critical point in the net neutrality debate is whether network operators are capable of inspecting data packet content. Without that capability, they cannot meaningfully distinguish one packet from another. For a long time, it was technically

impossible to scan the content of passing packets in real time, but Deep Packet Inspection (DPI) and other technological advances have changed that. Network operators are now able to scan packet content and – if they so desire – to slow down or block their passage based on the type of application, the protocol used (such as the BitTorrent protocol, which is associated with piracy), the user or the content (DeNardis 2014: 135). There may be many reasons for wanting to do so, including network management or security considerations, and all sorts of political and economic arguments in favour of blocking or pricing content. Net neutrality is one of the founding principles of the Internet, making it an article of faith for many who are involved in the discussion. It is bound up with the idea of the Internet as a place free of politics. In that sense, as DeNardis (2014: 149) argues, 'net neutrality is not neutral but represents a set of values. Many of these are historical values embedded in the design of the Internet's architecture, such as engineering user choice about what information to access and creating a level playing field for the introduction of new information products'.

Three different logics intertwine in the debate about net neutrality. The first is a technical logic that is concerned with network management and quality of service; the second is an economic logic that relates to revenue models in cyberspace and the answer(s) to the question 'What is a level playing field?'; and the third is a political logic about using DPI to facilitate political control and censorship on ISP networks. A study by Asghari et al. (2013) on ISP use of DPI worldwide shows that DPI is common but amenable to regulation. It is more unusual in countries with strong opinions and strict laws on privacy, and more commonplace in those with a tradition of censorship. DPI use for network management purposes is less controversial but is also not very clearly defined.[4] There are good and legitimate reasons to differentiate between data streams and ensure that the network offers the majority of users maximum quality. It is difficult enough to draw the line between legitimate network management and violations of net neutrality – a concept that has also not been clearly defined – but even harder when economic or political motives start to play a role.

Since the Internet is a network of largely private networks (ISPs), various economic interests play a role. The two that are most in competition with each other are ISPs and providers of digital services. That may be because such providers introduce new services that rival the core tasks of the ISPs, many of which have merged activities in different branches into a single company. Wearing its ISP hat, for example, the Netherlands' former state-owned telephone company KPN must be less than pleased to handle calls made on Skype, which competes directly with its telephony services. In the opposite corner are Internet-based services and businesses; the most successful of these, whether it be Netflix or Facebook, are huge traffickers of data. The process of uploading photographs and film clips and streaming videos takes an enormous chunk out of the bandwidth that network operators use to

'guarantee' the quality of the connection for all their users. Network operators would like to charge Netflix and other digital service providers extra in exchange for guaranteed, priority treatment of their data streams. Both users and Internet businesses object to this idea, however. Users are afraid that prioritisation will slow down traffic on the rest of the Internet, while businesses think that ISPs should simply get on with their work and optimise data transmission across the board. In addition, it is the users who pay the ISPs for data use, not the providers of Internet services.[5] One frequently heard argument in this connection to net neutrality debates concerns innovation and the level playing field. If the Internet were to consist largely of private highways paid for by the Googles, Netflixes and Facebooks of this world, how could any new innovative company grow and succeed on the slow-moving secondary roads that remain? A start-up would no longer have the same opportunities that Google had when it started out. But the ISPs want to see more incentives and compensation to cover the costly investments needed to meet the ever-expanding appetite for bandwidth. They would rather get big companies to cover these investments than their own customers, who may react by taking their business to the competition.

Policymakers sometimes align themselves with the net neutrality camp. The Netherlands and Slovenia, for example, have codified the principle of net neutrality. The EU is discussing a new Regulation governing the single market for telecommunications,[6] but whether it will elaborate on the principle of net neutrality is unclear. In April 2014, the European Parliament included net neutrality in the proposal for the regulation at the last minute, but the Council, i.e. the member states, has effectively dismantled the proposal on the issue of net neutrality in 2015. The mandatory nature of a European Regulation, which replaces national law, means that EU meetings are a battlefield in the European war of net neutrality. Like the Netherlands, Peru, Chile and Brazil have also laid down net neutrality in legislation (De Filippi and Belli 2014), but it remains a highly controversial subject, both politically and economically. Specifically, major economic interests are at stake, with heavyweights such as cable companies and telecom operators fiercely resisting stricter regulation because it would rule out tiered pricing. President Obama's recent proposals to regulate net neutrality in the US were immediately dismissed by cable and broadband companies in scathing language ('a 1930s regulation').[7] They want the leeway to develop new revenue models.

Because net neutrality is a negative rule – it regulates what an ISP may *not* do – it is difficult to determine where the exact boundary lies. The boundary between ISP network management and quality of service interventions (often considered legitimate and useful) and ISP interventions that are discriminatory and/or tend towards censorship is blurred and very difficult for regulators to define (DeNardis 2014; Brown and Marsden 2013). In this debate, too, ISPs take centre stage. Thanks to DPI technology, these increasingly important players in cyberspace are

able to intervene in data streams running through their networks. Their reasons for doing so range from technical maintenance to financial profit (a key point in the net neutrality debate) or censorship, for economic (blocking copyright-protected content) or political reasons (blocking politically unwelcome content). These latter two forms of what is referred to as 'intermediary censorship' (Zuckerman 2010; Brown and Marsden 2013) will be discussed in Chapter 4.

3.3.4 INTERNET SECURITY

Now that the Internet has become central to our lives, it has also become a vulnerability. It is a 'backbone of backbones' (Choucri 2012), with all the associated consequences and risks. As a result, the concept of what security means on the Internet has changed. When the basic mechanisms of the Internet were first set up, security was not an overriding concern. The end-to-end principle and the 'dumb pipe' nature of the network imply that security is the responsibility of the endpoints. Viruses can spread like wildfire across the network precisely because the Internet sends data as efficiently as possible at the user's command, regardless of the content of that data. That is true even if the command is hidden in an attachment that the user has to open (e.g. the I LOVE YOU virus) or picked up on a dubious website ('drive by downloads'). The power of the Internet – the rapid distribution of information – can also be its weakness. The engineers who wrote the core protocols in the early years were not really concerned about security in the sense of protection against malicious individuals intent on using the power of the Internet for their own gain. The relatively small, homogenous and closed community that built and nurtured the early Internet focused on good intentions, not abuse. As the number of users grew, however, the online world began to resemble the offline world with its crime, vandalism, political disputes and other security issues. Every day, newspapers report new cases of cyberattacks, phishing, malware, digital espionage, mass surveillance and DDoS attacks. These risks have become a greater concern than network overload and redundancy, which belong to a more technical approach to the Internet.

In cyberspace, security has traditionally been the responsibility of the end user, who is responsible for installing the right software to ward off viruses and other attacks. The order of scale has naturally increased in recent decades, with businesses securing their own networks and network operators spending a lot of money on security. Operating at a higher, collective, level are the Computer Emergency Response Teams (CERTs). These operate in many different countries around the world. In the Netherlands, for example, there is a government CERT, GovCERT, now part of the National Cyber Security Centre, as well as CERTs of a number of large companies and universities. Most digitally advanced countries have one or more national CERTs, although their quality and expertise vary widely (see for a typology Skierka et al. 2015: 11-12). The national CERTs work together at the international level as well, though international agreements are often less important

than mutual trust between the technicians. All these organisations and many others work together on Internet security. But what we mean by Internet security is changing. Not only have the actual threats become more multifaceted, but so has our interpretation of them and the tools that we use or can use against them. The rise in Distributed Denial of Service (DDoS) attacks, in which a botnet so overloads a website that it crashes, looks different to a law enforcement officer working in a High Tech Crime Unit of the police than it does to a CERT technician. The officer sees cybercrime, looks for a motive and 'weapons', and wants to arrest and prosecute the perpetrator. The CERT technician sees an overloaded website and network and wants to resolve the problem. The easiest way to do that is to increase bandwidth. Both want to get rid of the botnet, of course, but engineers do not immediately think in terms of crime and punishment. Our point is that there are many different concepts of Internet security that influence each other back and forth, not always for the better.

These different attitudes towards cybersecurity are at odds with each other, as they have been before. The side feeling the most pressure is the one that views cybersecurity from the perspective of the Internet engineer. Its biggest challenge is the growing tendency to frame cybersecurity in terms of *national* security. Intelligence and security agencies, military cyber commands and, to a lesser extent, law enforcement agencies are increasingly dominant in the public and political debate about the Internet. The work of the international technical community, however, is carried out largely on the basis of mutual trust built up over the course of many years. That is especially true of the CERTs, where private and public parties often share information about problems and solutions on an informal basis (Skierka et al. 2015). Yurie Ito of Japan's CERT (JPCERT) issued the following warning at the Internet Governance Forum on Bali in 2013:

> The involvement of the national security organisations can potentially break down in trust, in CERT and technical communities if we were seen as an instrument of state focused competition. … So the result may be a significant rise in cybersecurity risk level because of the lack of transparency and the collaboration at the technical and, you know, CERT level, operational level.[8]

Several authors have pointed out the contradiction between national security, whose rationale is based by definition on the interests of a state, and the collective security of the Internet as a public good. Dunn Cavelty (2014), for example, has referred to the 'cybersecurity dilemma', in which using cyberspace as a tool for national security has detrimental effects on the level of collective cybersecurity globally (see also section 4.4). There is little scope for making mistakes in national security, however, and that becomes evident in the way that politicians address the subject. Van Eeten and Bauer (2009) compared 'precluded event security' and 'marginal security cost' in this connection. The first involves an absolute security

standard to which almost everything else must give way; the second weighs the benefits of security against the cost to society. Such costs go beyond the financial – security is an expensive affair – to include intangible costs, for example the values of the rule of law (AIV 2014) or a different view of Internet security and the critical issue of trust between the organisations and individuals involved. The first approach is becoming more dominant in the cybersecurity discourse.

In their efforts to neutralise the 'national security' logic, and particularly its consequences, the technical and CERT community are attempting to reframe the issue of Internet security and reorganise the response to it. One interesting example is the Cyber Green Initiative, which applies a public health model to global cybersecurity rather than a national security model (JPCERT/CC 2014). Building on the concept of the Internet as an ecosystem, this initiative views cybersecurity as a question of 'cyber health', with the point being to fight off and prevent botnets and malware that threaten that ecosystem. A crucial first step in this approach is for stakeholders around the world to standardise, share and disclose information about cyber threats, DDoS attacks and other threats. The result should be more accurate and realistic estimates of cyber threats and a more level playing field in terms getting information to policymakers and cybersecurity professionals. At a time of threat inflation, it can be very useful to have a better grasp of what the real cyber threats are and to move the discussion about network security out of the shadow of national security.

3.4 CONCLUSION

The Internet's public core is in good health and good hands, but pressure on it is building from different quarters. In some respects, it is a victim of its own overwhelming success. Its exponential growth has exhausted the stock of IPv4 addresses in some parts of the world and made the Internet community so enormous (billions of users) that the mass transition to IPv6 can no longer be based on the notion of 'doing what is right for the network's overall good'. Its success has created a collective action problem that will likely only be solved after things take a turn for the worse. The lax attitude of both the industry and governments suggests that it may take a crisis to spur them into action.

The pressure also comes from outside the Internet's core in a number of the issues discussed above. Political and economic interests and differences of opinion – sometimes combined with new technologies – are challenging the collective nature of the Internet. Important economic interests – for example copyright protection and revenue models for data transport – are putting pressure on policymakers to abolish or, conversely, offer legislative protection to net neutrality, previously the Internet's technical default setting. Some countries have clearly chosen sides in this matter, but even then, monitoring the actions of ISPs is a point of con-

cern. These issues show that the Internet is masterful at blurring boundaries. It is difficult to decide where the dividing line lies between 'network management' on the one hand and slowing or blocking data traffic for 'improper reasons' on the other. ISPs have become key actors and the gatekeepers of international data traffic. They have been manoeuvred into a position of gatekeeper by states and other parties, but questions of legitimacy are complicating this – often unwanted –status.

The political pressure on Team Internet is closely related to changes in international politics and the rise of national security as a key paradigm for how governments relate to cyberspace. In analysing both trends, we should be aware that the Internet is inextricably bound up with the internationalisation of the economies and societies of a growing number of countries. In other words, there is much at stake for these states. The fact that they have a very limited say in matters of Internet governance has raised questions about the existing governance arrangements. The domain name and IP address issue is a good example of how a technical function can become overly politicised. Removing oversight of these IANA functions from the US's direct sphere of influence is logical from the vantage point of international politics: after all, the Internet has become vital to virtually every country, not just the US. But that in itself does not clarify what shape future oversight will take and how and whether state interests should be taken into account. Two matters are of crucial importance in this regard. First, the transition process should separate the administrative tasks from the more political aspects, with the technical community at the helm of the first and with more scope to accommodate political and economic interests in the second. Most countries would benefit greatly from technical management that is as 'agnostic' as possible, as it would do most to ensure the operation of the Internet as a collective infrastructure in the long term. Second, while the ICANN debate may be symbolic to some extent, that may make it all the more critical. It is the most visible and, to some degree, the most tangible discussion about the relatively vague notion of 'Internet governance'. There are likely to be many more such discussions about this subject in the future, but in those discussions, seemingly small changes in the technical substructure may have huge implications. This is why the ICANN debate serves as an important test case for cyber diplomacy. Are new coalitions possible that look beyond the 'usual suspects' of the transatlantic axis? We know roughly which side of the debate many countries come down on, and those poised at the extreme ends of the spectrum are not likely to change their positions. We cannot be as certain about another, large group, whose members include many states in which the Internet still has enormous growth potential. Their stake in the Internet will only increase as time passes, and their ideas about Internet governance have not yet become rigid. A diplomatic effort is needed to forge new international coalitions focused on securing the public core of the Internet in the longer term.

A preoccupation with national security is taking over in cyberspace, affecting the way in which we perceive the Internet and, in particular, which actors states are facilitating to promote Internet security. The many new actors in cyberspace focusing on national security, for example the military, intelligence and law enforcement agencies, are beginning to interfere with the more traditional technical approach of the CERTs and their long track record of international cooperation. It would be unwise to combine the logics of the two sides, for two reasons. First, national security is always an individual interest, whereas Internet security – the security of the network as a whole – is a collective interest. Confusing the two logics, or letting the first dominate, could seriously impair the trust that the technical community has managed to accrue over the course of many years. It is therefore extremely important to differentiate tasks. Second, the logic of national security implies a much lower tolerance of risk. There is little political scope for 'residual risk' and 'trial and error' in the realm of national security, since a single error could be fatal. That logic brushes aside other opinions about security in which the stability and reliability of the Internet as a global public good are at least as important, if not more so. It is precisely in matters of national security versus the interests of the collective Internet that states must exercise restraint and reserve. That is the only way to guarantee the stability of the net in the long term. In reality, however, those entrusted with national security are more likely to want to extend their reach than show restraint. That is why it is important to put the issue of Internet security versus national security on the international agenda and to try to disentangle the various attitudes towards Internet security. Chapter 5 provides a first attempt to do so.

NOTES

1 Even the most basic protocol, IP, received staunch support in 1982 when Vint Cerf and his colleagues threatened the users of what was still a very small Internet with exclusion: 'If you don't implement TCP/IP, you're off the net' (quoted in Wu 2011: 202).

2 See the statistics at: http://www.google.com/intl/nl/ipv6/statistics.html#tab=per-country-ipv6-adoption, accessed 5 November 2014.

3 Interview with Prof. Erik Huizer, 21 January 2015.

4 Network management is about the efficient use of bandwidth and has at least two aspects to it. Should scores of users be made to 'suffer' poor access and service because of the data-intensive practices of a few? Or should those few users have their transmission speeds reduced? Connected with this issue is the fact that certain applications, for example Voice over IP, online gaming and streaming music and video are much more data-intensive and more sensitive to bandwidth loss. No one is bothered whether the packets containing an e-mail message arrive at their destination in bursts or if it takes somewhat longer to download an e-mail. The slightest delay in a VoIP connection, however, makes conversation almost impossible. In both cases, there are legitimate reasons to differentiate between data streams and ensure that the network offers maximum quality to the majority of users.

5 This does not mean that major Internet companies like Netflix and Google do not invest heavily in improving and guaranteeing user access – they certainly do.

6 Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013PC0627.

7 Dominic Rushe (2014) 'Net neutrality: cable companies 'stunned' by Obama's 'extreme' proposals', *The Guardian*, 11 November 2014. See: http://www.theguardian.com/technology/2014/nov/10/cable-companies-obama-net-neutrality-proposals-fcc-fight.

8 8th Internet Governance Forum, Bali, Indonesia. Session number 143, 22 October 2013. See: http://www.intgovforum.org/cms/igf-2013-transcripts/1501-ws-143-emerging-cyber-security-threats-, accessed 13 December 2013.

4 NATIONAL INTERESTS AND THE INTERNET AS A GLOBAL PUBLIC GOOD

> Invite states in, and along with them comes their fragmentation and their stifling political constraints; shut them out entirely, and there is a risk that accountability will disappear and rights will be lost.
> Milton Mueller (2010: 240)

4.1 INTRODUCTION: WHERE NATIONAL INTERESTS INTERSECT WITH THE INTERNET'S CORE PUBLIC INFRASTRUCTURE

This chapter focuses on a number of controversial developments in which the Internet's public core has been or is at risk of being violated. Such incidents threaten the underlying values of the Internet as a global public good, something that could have serious consequences for its technical and socioeconomic operation. Someone who messes with the DNS, for example, messes with the Internet as a whole. In other words, such developments involve infringements of the principles of universality, interoperability and accessibility owing to actions, policy and legislation that place national and/or economic interests above the interests of the Internet's collective public core. The repercussions of such interventions can be great. It is technically possible to 'break' the Internet, certainly if that means damaging the integrity and reliability of its central protocols and, as a result, its operation as a whole.

This chapter reviews four situations in which policymakers have chosen to develop and implement a particular policy 'using' the Internet's public core. This type of governance, which utilises the Internet's infrastructure, is harmful to that core. Such harm could have well been the outcome of a number of recent legislative bills and treaties that were meant to protect copyright and intellectual property rights on the Internet. Section 4.2 considers the driving forces behind such legislation – in many instances classic examples of what economists call 'regulatory capture', in which industry actually writes the law – and the consequences of some of these bills. Several of them, for example SOPA, PIPA and ACTA, are now off the agenda in their current form, but that removes neither the problem nor the forces driving such legislation. As long as politicians are ignorant of the consequences of certain technical interventions, it is likely that we will see new legislation that is potentially damaging to the public core of the Internet. Section 4.3 considers one of the biggest online controversies from a human rights perspective: censorship and restrictions on freedom of expression. However, this book emphasises the consequences of technical measures that affect the operation of the Internet's public core rather than human rights violations in the global digital context. Sections 4.2 and 4.3 both stress the key role of ISPs as the preferred intermediary actors with the ability to control and regulate the behaviour of consumers, the public and busi-

nesses. Governments and corporate powers such as the entertainment industry turn to ISPs to safeguard their interests by enlisting their help through legislation and/or by applying pressure through legal liabilities and the threat of lawsuits. The risk, of course, is that this will push surveillance and censorship into the back office of cyberspace, beyond the range of legal and democratic oversight. Section 4.4 concentrates on the growing influence of actors in the national security domain on the Internet. The rising online presence of security and intelligence agencies and the military has implications not only for privacy but also for the integrity of the Internet's technical operations. Section 4.5, finally, looks at attempts by states to nationalise parts of the Internet and explores what this means for its operation as a whole. While authoritarian regimes have long nurtured ambitions in this direction (the Great Firewall of China or Iran's National Internet), they have recently been joined by democratic states such as Germany and Brazil, responding to Edward Snowden's revelations about NSA surveillance by laying out plans to nationalise data traffic, clouds and hardware (subsea cables). But moves to nationalise the net that require interventions in routing protocols, for example, are severely at odds with the way in which the Internet normally operates and transmits information.

4.2 IP VERSUS IP[1]

"The Internet is a gigantic, globally distributed always-on copying machine" (Mueller 2010: 131). Users can consult, download and share content regardless of their location. The rise of person-to-person (P2P) software has allowed more and more people to share copyright-protected music, film, games and books illegally. That naturally violates the protection offered by intellectual property rights and copyright law. With a powerful lobby and an army of lawyers, the film, music and entertainment industry has spent many years fighting for stricter national laws and international treaties prohibiting the unauthorised sharing and downloading of copyright-protected digital content (Breindl and Briatte 2010). Increasingly, the legal regimes and measures deployed and advocated by the industry interfere with the Internet's critical technical infrastructure, for example IP addresses or the DNS. But this strategy, which uses the Internet itself to protect intellectual property, is meeting with growing resistance from users, Internet companies, civil society and the technical community. They argue that the measures are ineffective, ignore the basic principles of the rule of law, and last but not least are damaging to the Internet's very operation. The protection of intellectual property has become one of the key issues in the battle for governance of the Internet, succinctly summarised by Mueller (2010: 129) as 'IP versus IP', or Intellectual Property versus Internet Protocol.

The clash between the two IPs can be attributed to two diametrically opposed processes that initially had almost nothing to do with each other. The first was the liberalisation of the telecommunications industry. Cyberspace benefited enormously from this process, which made a decentralised, competitive and global Internet possible. The second involved attempts to regulate the global protection of intellectual property rights, leading to various international treaties such as the Agreement on Trade-Related Aspects of Intellectual Property Rights, or TRIPS (WTO 1994), the WIPO Copyright Treaty, or WCT, the WIPO Performances and Phonograms Treaty, or WPPT (WIPO 1996) and the European Union Copyright Directive (2001). The dizzying growth of the Internet led to a clash between these two processes, and attention soon shifted from protecting software patents to tackling online 'piracy'.

It is difficult to protect intellectual property on the worldwide Internet, however. In order to profit from intellectual property, access to it has to be restricted. But because digital content can be reproduced an infinite number of times and distributed around the world at marginal cost, without the owner even noticing, it is almost impossible to protect (Boyle 1997). Digitisation had already destabilised laws and policies pertaining to copyright. It made it much easier for users to share copyright-protected material, especially once P2P file sharing began to take off on Napster, LimeWire, Torrentz, Pirate Bay and other sites. The early years of the twenty-first century saw a series of lawsuits filed against organised forms of P2P file sharing, for example against Napster in the US (2001) and MMO in Japan (2002). A recent similar case in the Netherlands led to the prohibition of Pirate Bay. Such prohibitions have not had any real long-term effect, however (Poort et al. 2014; Danaher et al. 2013), as these websites tend to be replaced by new and smarter versions of P2P tools almost overnight. In addition, so many people now download material from illegal sources that we can genuinely say that the practice has been 'democratised'. In the Netherlands alone, more than a quarter of the population aged between 18 and 65 years download files illegally (Poort and Leenheer 2012). With lawsuits being expensive and time-consuming, not to mention the PR risks involved ('Rich Entertainment Industry Ruins Downloading Teenager'), the entertainment industry decided many years ago to focus on political lobbying. Its aim is to advocate new laws that (a) target Internet intermediaries such as ISPs and (b) impose rules that use the Internet's architecture. A number of such regulations have been already been implemented in practice.

One of the interesting features of these laws is that they require private Internet companies to take action. There are two kinds of legislation. The most common is the 'notice and take down' regime, with Internet companies being made responsible for blocking access to specific content. In return, their legal liability for having hosted or transferred illegal content is reduced. For example, the US Digital Millennium Copyright Act (1998) indemnifies ISPs but requires that they remove content

at the request of the copyright holder. We can gain an idea of the scale by noting that in 2012, Google received more than 6.5 million requests to remove copyright-protected material within the space of just one month (DeNardis 2014: 178). The risk here is that content monitoring – and, by extension, censorship – will shift to the anonymous layer of ISPs and other Internet intermediaries, characterised by Zuckerman (2010) as the rise of 'intermediary censorship'. When governments – in this case backed and prodded by a powerful industry – succeed in forcing Internet companies to follow these rules and enforce them among their own users, implementation and censorship have been 'effectively outsourced to private industry' (MacKinnon 2011: 197). Things are taken to the next level if these companies start to reject content preventively in order to avoid damage claims and lawsuits or conflicts with governments. In that case, government has not only contracted out the letter of the law to private parties, but the spirit of the law as well.

A more radical approach is the 'graduated response' mechanism, as implemented by law in France, South Korea, Chile and Taiwan, and as the product of a private agreement between an ISP and the entertainment industry in the United Kingdom, the United States and Ireland (Brown and Marsden 2013; DeNardis 2014; Van Eeten et al. 2014). In this system, the user receives a number of warnings before their Internet connection is disabled or its speed is reduced so drastically that it is impossible to download large files. Access to certain services can also simply be blocked. In practice, Internet companies are usually the ones to impose this measure because they are in the best strategic position to confront users and also have the technical know-how to do so. Their role has been laid down in law and/or user agreements in many countries. Now that DPI has made it possible for ISPs to analyse Internet traffic, some parties have argued that they should be forced to actively monitor data traffic on behalf of copyright owners. The European Court of Justice rejected this notion with its judgment in Scarlet v. SABAM (C-70/10) in November 2011.[2] Once again, the tendency is to shift surveillance and policy implementation to the Internet's private back office, gradually removing it from public oversight.

Most proposals to regulate copyright online came about under severe pressure from the media and entertainment industry. They are classic examples of 'regulatory capture', a situation in which legislation is heavily influenced by a specific group of stakeholders. This changed some years ago when global mass protests arose against two new US bills, the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA), as well as against the international Anti-Counterfeiting Trade Agreement (ACTA). Following large-scale protests, ratification of ACTA by the EU member states was shelved after the European Parliament rejected it. The Juncker European Commission – in office since November 2014 – has placed it on the list of proposals that will be withdrawn. The protests against SOPA, PIPA and ACTA are regarded as a turning point in the history of copyright legislation (Benkler 2012;

Hofmann 2012; Dubuisson 2012). Because it was the first time that the online community had organised itself and taken collective action, that turning point has also been described as a battle between the 'old' and the 'new' economy': 'PIPA and SOPA became nothing less than a referendum on who controlled the evolution of digital life' (Downes 2012, cited in Hofmann 2012: 74-75). Both US bills would have extended the 'notice and take down system' of the Digital Millennium Copyright Act (1998) to payment and advertisement networks. The bills also offered private parties immunity against damage that they might cause by erroneously blocking certain content and payments (Hofmann 2012). The scope of SOPA and PIPA was not limited to the United States, but also covered websites abroad or sites that could be accessed through domain names registered abroad. This was one of the reasons for the worldwide interest in the two bills. A vast amount of that interest was generated by Wikipedia, Reddit and WordPress, which protested by going 'black' for one day, on 18 January 2012, making parts of the Web inaccessible. Wikipedia asked its visitors to 'Imagine a World Without Free Knowledge' and Google placed a censor bar over its logo. The protest pitted freedom of speech and information against excessive copyright protection.

The Internet's technical community also criticised SOPA and PIPA because they undermined the operation of the Internet by interfering with its deeper technical architecture. Since the bills would have impinged on the most basic Internet protocols, DNS and IP, 'Don't Break the Internet' became another key slogan of the protests. Many of the Internet's pioneers took up their pens to write to their elected representatives in Congress, stating that, 'regardless of recent amendments to SOPA, both bills will risk fragmenting the Internet's global domain name system (DNS) and have other capricious technical consequences'.[3] They were joined by scientists, who argued that 'directing the remedial power of the courts towards the Internet's core technical infrastructure in this sledgehammer fashion has impact far beyond intellectual property rights enforcement – it threatens the fundamental principle of interconnectivity that is at the very heart of the Internet' (Lemley et al. 2011). In other words, introducing either law could cause serious harm to the Internet's backbone. The DNS is one of the main building blocks of the Internet and, along with certain other protocols, constitutes the basis for virtually all other protocols and countless applications that allow the Internet to function properly and reliably (Lemley et al. 2011). Blocking content for reasons of intellectual property and copyright protection would mean that users could no longer trust the search results of DNS servers. Interfering in basic protocols would not only make the Internet less reliable and universal, it would also make it less secure.

Whether such measures would be effective is also very much open to debate. Even trivial changes are enough to circumvent Internet blockages, for example typing in an IP address (rather than a domain name) to avoid consulting the DNS server. Readily available, easy-to-install software plug-ins can also link users auto-

matically with DNS servers that are not blocked (Crocker et al. 2011). Such tricks tend to spread quickly among unapologetic uploaders and downloaders. Illegal content also resurfaces quickly after a blockage, as the prohibition of P2P networks has demonstrated. The decline of one usually heralds the rise of another.
More worrying is that 'overblocking' can also cause considerable collateral damage. Online interdependence – for example virtual hosting or a website offering services and e-mails that run through other domains – can easily lead to a larger section of the DNS being blocked than the law had intended. Incidents in which tens of thousands of subdomains are blocked accidentally show how very real this problem is. It is for this reason that Yu (2012; 2014) calls such measures 'highly disproportional'.

The threat of interference in the deep layers of the Internet remains, however. Similar new proposals have been put forward to enforce copyright law (Masnick 2014), and although technical filtering is imperfect and inevitably results in too much or too little content being blocked (Zittrain and Palfrey 2008), it has become a common means of protecting intellectual property (Sellars 2014; Breindl 2013). This is mainly the result of the unilateral and uneven involvement of stakeholders in decision-making about intellectual property regulations. A second shortcoming is that those who make or approve such legislation know little about the Internet's technical aspects. In the battle over SOPA and PIPA, more and more publications appeared arguing that it 'was no longer OK' for Members of Congress not to understand how the Internet works (McDiarmid and Sohn 2013). This criticism is certainly not restricted to American politics. Such ignorance allows the economic interests of the entertainment industry to override those of the Internet's collective core, thereby putting pressure on the public Internet.

4.3 CENSORSHIP AND SURVEILLANCE

Left to its own devices, the Internet is a platform where people can express even the most extreme ideas. But its very appeal as a bastion of free speech means that it has from the outset been regarded with suspicion by regimes wishing to exercise strict control over the information that reaches their populations. Authoritarian regimes allow their populations access to cyberspace, but only under conditions of surveillance and censorship. Today, some of the optimistic ideals held at the birth of the Internet, i.e. the predominantly Western notion that cyberspace and censorship were incompatible and that technology would inescapably encourage and facilitate freedom of speech, have been largely abandoned. Digital freedom of speech and other digital manifestations of traditional human rights now feature prominently on the diplomatic agendas of many Western countries. In 2010, Hillary Clinton put 'Internet freedom' on the State Department's agenda; in 2011, the Netherlands took the lead in setting up the Freedom Online Coalition[4] of states working together to protect and support freedom of speech in the digital

domain. But when Clinton resigned as Secretary of State, the American agenda for Internet freedom was put on the back burner, and since the Snowden revelations the US has lost much of its remaining credibility as a leader in this regard.

Governments the world over are monitoring and controlling Internet traffic more actively than ever before (Howard et al. 2011; for relevant overviews, see Deibert et al. 2008; 2010; 2011). Authoritarian regimes go furthest in that regard, but liberal democracies are not entirely innocent either. From the very start, China connected to the worldwide Internet with the idea of controlling its own population. China has 'state-owned hardware servers, state-owned fibre optics via state-owned switches, boiling down to the idea that "China is not on the Internet, it's basically an intranet"' (Herold 2011: 5). China has built a wall around 'its' Internet with only a few gates leading to the outside; it installs content-control software on PCs (Green Dam Youth Escort) and regularly shuts down certain services such as Wikipedia in order to install filters that block content automatically based on keyword recognition (Zuckerman 2010). All incoming and outgoing Internet traffic in Saudi Arabia also passes through a single, filtered gateway (Zittrain and Palfrey 2008), and the plans for Iran's national Internet follow the same logic.[5]

The scope of censorship has increased, and states also have access to a growing array of digital censorship tools and strategies to monitor their populations. In the early days of cyberspace, people often thought that slow-moving authoritarian regimes would never be agile enough to keep up with the fast-paced young world of the Internet. But these sluggish giants became digitally adept sooner than expected, and censorship also became more technologically refined and intelligent. Although states still block content in emergency situations, many countries now permit Internet use under surveillance because it is an important source of information for their police and intelligence agencies. While it is impossible to 'switch off' the Internet as a whole, there are numerous 'kill-switches' (DeNardis 2014: 207-213). They range from blocking specific content to DNS blockages, and from DDoS attacks on specific websites to forcing ISPs to deny users access to their networks, leading to outages in parts of cyberspace. That is what happened in Egypt in 2011, when the Internet went black for several days during the uprising against the Mubarak regime. Before that, outages took place in Libya, Burma, Nepal and Iran (DeNardis 2014). Budish and Kumar (2013) call these strategic blockages 'just in time censorship', used before an election, for example, to block information from or in support of the opposition. Sometimes, however, content blocking can have wider implications because those taking action interfere with the DNS or routing protocols. The most famous example is Pakistan's blocking of YouTube, which had worldwide repercussions. In 2008, the Pakistani Ministry of Information ordered YouTube to be blocked in Pakistan, accusing it of carrying blasphemous material. Pakistan Telecom went about complying with the order in a rather clumsy manner, however; the change it made to the routing protocol not only affected Pakistani

ISPs, but was broadcast and adopted globally, causing YouTube to become inaccessible across the entire Internet (DeNardis 2014: 96; Deibert 2013b: 40). Although the error was quickly corrected, this example shows just how tightly interwoven the Internet is through its core protocols, and how vulnerable those protocols are to national actions motivated by a specific idea about what is and is not permissible in cyberspace.

Western states are also joining in, with filtering now being common as a means of combating extremist or terrorist content, for example. The Charlie Hebdo attacks in Paris have led some officials to argue that the private sector should work with government to remove extremist content from the net, but they mention the detection and removal of illegal content in general almost in the same breath.[6] States around the world have different reasons – political, religious and societal – for blocking the Internet, and use different tools to do so (Zittrain and Palfrey 2008). Western democracies use filtering primarily to (a) combat genocidal, terrorist and racist content, although countries also differ widely in their opinions about this (Breindl 2013); and (b) to prevent infringements of intellectual property rights. And like other regimes, liberal democracies attempt to make the Internet and the activities that take place in cyberspace subject to national legislation. The fight against cybercrime and the dissemination of child pornography are at the top of the agenda in many countries, for instance. An older but well-known example is the French government's lawsuit against Yahoo to force it to remove Nazi paraphernalia from an auction site. More recently, various private companies – including Every DNS, Amazon, MasterCard, Visa and PayPal – ceased providing services to WikiLeaks following the 'Cablegate' affair, making WikiLeaks unfindable and unable to generate revenue (Brown and Marsden 2013). Benkler (2011) believes there is a direct relationship between their 'spontaneous' decisions and calls by US Senator Joseph Liebermann and others to pull the plug on WikiLeaks. The companies, however, claim that they were not responding to political pressure or to any official government or court request. This situation raises questions about the role of private parties in protecting and/or restricting freedom of speech.

Increasingly, Internet companies are faced with a dilemma with regard to freedom of speech. On the one hand, governments expect them to uphold strict human rights standards while competing for a share of the Internet's growing international market. While she was US Secretary of State, for example, Hillary Clinton (in 2010) expected Silicon Valley to assist in the fight against censorship and the battle to protect human rights, saying that, 'American companies need to make a principled stand. This needs to be part of our national brand. I'm confident that consumers worldwide will reward companies that follow those principles.' On the other hand, when Western governments are themselves eager to intervene in cyberspace for reasons that they consider legitimate in their own national context, it is to these companies that they turn for access, information and even implemen-

tation of policy. Nowadays, those reasons are often related to security and national security (see section 4.4). Governments are submitting more and more requests for information. In late 2012, for example, the Netherlands set up Clean IT, an EU project that it has undertaken jointly with Belgium, the UK, Germany and Spain to purge the Internet of terrorist content based on informal cooperation with ISPs, i.e. without any binding government directives. The project has been completed, but the intentions expressed by the EU ministers in Riga in January of 2015 indicate that it will have a follow-up. The important role that Internet companies play in global cyberspace raises questions about their responsibility and autonomy. As yet, international law applies mainly to the behaviour of states; the idea of applying it directly to international enterprises is relatively new (Scherer and Palazzo 2011: 911). John Ruggie, the UN Secretary-General's Special Representative for Business and Human Rights between 2005 and 2011, commented that international corporations mainly utilise self-regulatory processes in which the interpretation of rights can be 'so elastic that they lose all meaning' (Ruggie 2007: 836). The 'Ruggie principles', which he recommended to the UN and which the UN adopted in 2011, marked the start of a discussion about the role of businesses in human rights protection. These principles merit more attention in the digital domain, for example within the context of the UN Human Rights Council resolution recommending the establishment of a working group on a legally binding international instrument on transnational corporations and human rights.

Internet companies do not simply comply unquestioningly with all requests to block content. They have some leeway to consider all the factors and interests involved. But in many respects they do cooperate – sometimes voluntarily, sometimes not – with requests submitted by competent authorities. The transparency reports that Google,[7] Twitter[8] and Microsoft[9] publish to account for their actions to the Internet community reveal that it is mainly liberal democratic regimes that request the most data (at least openly) (Deibert 2013). Many of these requests and website 'blocklists' are not in the public domain and therefore subject to little if any democratic oversight (Zittrain and Palfrey 2008; Brown and Marsden 2013). The same applies to blockages arising from agreements between private parties (Van Eeten et al. 2014). Most censorship is therefore laid squarely in the lap of the Internet companies. Their response is to comply in some situations, to resist the express wishes of the authorities in others (especially if they are companies who count their public reputation among their most prized assets), and in yet other circumstances to stay one step ahead by taking preventive action, as appeared to be the case with Cablegate and WikiLeaks. DeNardis (2014: 158-159) refers in this connection to 'discretionary censorship', but it is not clear to what extent these companies have discretion and what choices the various enterprises make in that regard. All of this is part of a broader movement towards what Zuckerman (2010) calls 'intermediary censorship', with private businesses undertaking public tasks without public oversight. Strategies of this kind may have a negative radiating

effect and undermine the credibility of Western countries which condemn censorship by authoritarian regimes (Yu 2012; 2014). Filtering, the collateral damage associated with overblocking, the lack of transparency and the potential for abusing technical interventions all come at a price; according to Mueller (2010: 209-211), they are nibbling away at the free and open communication that has made the Internet a success.

4.4 INTERNET SECURITY VERSUS NATIONAL SECURITY

In Chapter 3, we touched briefly on the rise of the national security mindset in cyberspace. Over time, cybersecurity has increasingly become a matter of national security. The Netherlands is no exception in that regard. Five years ago, it was the Ministry of Economic Affairs that was largely responsible for most Internet-related policy, which focused on e-commerce and establishing statutory frameworks for telecom and Internet companies. Today, however, the centre of gravity has shifted to the issue of cybersecurity, which is the responsibility of the Ministry of Security and Justice, or more precisely the National Coordinator for Security and Counterterrorism (NCTV). The Ministry of Defence is right behind them with an operational Cyber Command and the official authority to conduct both defensive and offensive military operations in cyberspace. A similar shift from economy to security has also taken place within the EU. The European Commission's Directorate-General for Communications Networks, Content & Technology (DG CONNECT) is by no means the only DG that concerns itself with the Internet; the DGs for Justice and for Home Affairs and the Commission's diplomatic corps (the European External Action Service, EEAS) have also prioritised cybersecurity on their policy agendas.

Whilst there is no denying that the Internet is not as secure as it once was, it is difficult to say precisely how big the threat is and who is being threatened. In addition, the question is whether states are putting the right agencies and organisations forward to combat the right threats (Dunn Cavelty 2014). Many researchers warn about the danger of 'threat inflation' and the unhelpful language of national security and warfare (Brito and Watkins 2011; Betz and Stevens 2011; Libicki 2012; Rid 2013; Lawson 2013). This does not mean that all of the Internet has been securitised or militarised, but policymakers are increasingly looking at cyberspace through different eyes. Today, the Internet of economic opportunities is also the Internet of threats, vulnerable critical infrastructures and national security. Indeed, the emphasis may have even swung towards the latter.

And that has consequences, as became painfully clear when Edward Snowden revealed that the NSA and its British counterpart, GCHQ (among others), had spied on large swathes of global Internet traffic in the interests of national security (Greenwald 2014). The various surveillance programmes that Snowden exposed,

including PRISM, MUSCULAR and BULLRUN,[10] reveal intelligence agencies with a voracious appetite for data collection, legal frameworks that failed to rein them in, inadequate judicial and democratic oversight, and the wholesale violation of personal privacy – and all for seemingly very few gains in terms of national security (Landau 2013; Glennon 2014; Van Hoboken and Rubinstein 2014; Mueller and Stewart 2014). Thanks to new technology and generous budgets, the reality of these intelligence and security agencies is a far cry from more traditional views on national security and their role in that context.

> In prior generations, the cost of surveillance and data acquisition constituted a useful buffer between state surveillance and privacy; resource constraints forced law enforcement to focus on a limited number of targets on a scale where judicial oversight was a practical— if imperfect— deterrent against overreach
> (Faris and Gasser 2013: 21).

In addition to the mass violations of privacy that evoked such a fierce global response, Snowden revealed that the agencies had interfered with the deep technical infrastructure of the Internet that we all use every day, all in the name of national security. Tim Berners-Lee, the man who invented the WWW, called the decision by the NSA and GCHQ to break encryption software that protects the transfer of data on the Web 'appalling and foolish', as it directly contradicted the US and UK's efforts to fight cybercrime and increase cyber security, which both countries had identified as national security priorities. He also called it a betrayal of the technology industry.[11] In January 2014, a large group of US cryptography and information security researchers wrote an open letter to the US government concurring with Berners-Lee's views and stating: 'The choice is not whether to allow the NSA to spy. The choice is between a communications infrastructure that is vulnerable to attack at its core and one that, by default, is intrinsically secure for its users'.[12]

The tension between the 'needs' of the intelligence community and the interests of the IT and Internet industry had already surfaced during the 'cryptowars' of the 1990s. These disputes were about the encryption of American commercial software, and in particular about placing restrictions on the export of cryptography outside the US. The software concerned was destined for the vast majority of ordinary computer and Internet users worldwide. The IT industry wanted to export products with high-quality encryption, but the US intelligence community was fiercely opposed because it did not want to have restrictions imposed on its ability to break into Internet communications and IT systems around the world (Van Hoboken and Rubinstein 2014; Landau 2010; 2014). In other words, the intelligence agencies wanted to guarantee access for themselves by weakening encryption standards, by obtaining cryptographic master keys, or by inserting secret 'backdoors' and other vulnerabilities into software supplied to users worldwide.

After a long battle between the intelligence agencies and the industry, the restrictions on exports were ultimately lifted. We now know that the agencies have continued their campaign, however. In the post-Snowden era, the big Internet companies and cloud services, which – knowingly or unknowingly – had 'delivered' massive amounts of data on their users to the NSA, responded to the scandal by improving the cryptography of their own data centres. Their hope was that they could win back the trust of customers both within the US and, especially, beyond. After the Charlie Hebdo attacks in Paris, the FBI and the NSA warned against the 'dangers' of the increased use of cryptography, and there are growing calls in both the US and Europe to introduce statutory powers to break encryption. The FBI is openly critical of Apple and Google, which have recently toughened the security of their smartphones.[13] The director of GCHQ also accused American technology companies of being 'command-and-control networks of choice for terrorists and criminals' because they had improved their encryption (cited in Faris and Heacock Jones 2014: 34).

But the ambitions of security agencies go even further when it comes to accessing data and communications, or even laying the groundwork to guarantee such access. Snowden revealed that the NSA has not only attempted to crack cryptography, but also did its best to deliberately weaken the official standards issued by the National Institute of Standards and Technology (NIST). It has tried building vulnerabilities into cryptographic standards to ensure that it can always get inside systems through a backdoor. This did not only hurt the reputation of NIST – a US federal agency – but also sabotaged general security in cyberspace as well as international political relations. As Landau explains, 'It appears that the NSA's SIGINT division viewed corrupting cryptography standards as a goal. If other governments had done such a thing, the US would have been outraged' (Landau 2014: vii). The impact of interfering with standards naturally radiates outwards. Because protocols are certified standards, they are widely disseminated. That means that the arm of the NSA extends a very long way in terms of access, but it also makes the Internet extremely vulnerable and puts users at a high level of risk. Or, as cybersecurity expert Bruce Schneier put it, 'You can't build a back door that only the good guys can walk through'.[14]

This latter aspect is especially pertinent in the international market for *cyber insecurity* that has matured in recent years. Every cyberattack – whether its nature is determined by crime, espionage, cybervandalism or military goals – depends on there being one or more vulnerabilities in the target's software that provides access to its systems. Known as 'zero-day vulnerabilities', these are software flaws unknown to either the user or the software vendor, meaning that there are no immediate patches available. The software vendor has 'zero days' to repair the vulnerability if a hacker discovers and exploits it. Hackers can turn these vulnerabilities into cyberweapons by writing code that exploits them to damage systems or

to use systems to cause damage (set off explosions, open dams, and so on). The latter are referred to as 'cyberexploits', or 'weaponized code'. Cyberweapons come in many shapes and sizes, from very simple ones with limited potential (such as a DDoS attack) to precision weapons with massive potential (Rid and McBurney 2012: 6). The most famous example of the latter is the Stuxnet attack on Iran. Stuxnet was a computer worm that tampered with Iran's nuclear centrifuges at the Natanz facility and caused a significant setback in its nuclear programme. In all probability the US and Israel were behind this cyberattack; it had all the hallmarks of a long-term military operation requiring meticulous preparation and intelligence and using an unprecedented four unknown zero-day vulnerabilities (Sanger 2012; Singer and Friedman 2014). US and Israeli military and intelligence probably discovered the zero-day vulnerabilities themselves, but it is equally likely that they purchased them on the growing international market for zero-day vulnerabilities.

The zero-day vulnerabilities market is divided into white, grey and black markets and has expanded dramatically in recent years (Fidler 2014; Ablon et al. 2013). In the early days of the WWW, hackers regarded it as a game to trace vulnerabilities in software and alert vendors to them. The glow of success and recognition of their achievement were often enough reward. For some, this form of 'responsible disclosure' still is an end in itself. Nowadays, however, hackers who track down vulnerabilities are usually paid, and paid well, by the same vendors. That is the white market. But the real money is in the grey and black markets. The black market operates online through websites such as Silk Road and its successors. Basically, anything that is prohibited can be acquired there. The grey market is populated by legitimate buyers – intelligence agencies and military cyberunits, although some of them may also venture into the black market (Fidler 2014). The grey market is an open and legal – but unregulated – market in which security specialists sell products on their websites and describe what they consider to be legitimate customers.[15] For example, the French company VUPEN sells only to 'approved government agencies (Intelligence, Law Enforcement, and Defence) in approved countries'.[16] Operators in the grey market do not sell to countries that are subject to an international arms embargo imposed by UN, the US or the EU (see also Stockton and Golabek-Goldman 2013). But since many of these companies may also supply the arms industry, their product distribution is probably much wider (Fidler 2014).

The problem is that governments buy vulnerabilities in the software that we all use (and which is used by our critical infrastructures, banks and clouds) and keep them secret in the name of national security so that they can exploit them later for military or intelligence purposes. Keeping these vulnerabilities secret is not without its risks, however, because 'their' security and 'our' security in cyberspace are intimately connected. It is once again Bruce Schneier (2014) who levels the sharpest criticism against the US intelligence and military 'stockpiling' of vulnerabili-

ties: 'There is no way to simultaneously defend U.S. networks while leaving foreign networks open to attack. Everyone uses the same software, so fixing us means fixing them, and leaving them vulnerable means leaving us vulnerable'.

The lively trade in zero-day vulnerabilities again points to the growing tension between *national* security in cyberspace and the security of cyberspace itself. Myriam Dunn Cavelty (2014) has taken the security dilemma described by Jervis (1978) and applied it to trends in the cyber domain, stating that, 'paradoxically, the use of cyber space as a tool for national security, both in the dimension of war fighting and the dimension of mass surveillance, has detrimental effects on the level of cyber security globally'. One state's efforts to strengthen its national security in cyber space evokes a response by another state, making the first state less secure. As a result, security in all of cyberspace declines. Deibert and Rohozinksi (2011) point out that China increased its military cyber capacity in response to the US's decision to install a military Cyber Command. At a 2014 conference on civil-military cooperation in cyberspace, an expert in military cyberstrategy suggested that that main fallout of the NSA revelations was that other states would now attempt to build the same capacities.[17] A cyber-Westphalian doctrine, with states prioritising their national security, would have huge implications for the collective backbone infrastructure of the Internet on which those states have built the cyber-version of their country, economy and society. In cyberspace, states have become so intimately intertwined with each other at the basic level of standards, encryption and software vulnerabilities that it is almost meaningless to think in terms of 'us' and 'them'.

The foregoing means that a certain level of restraint is needed in cyberspace – especially in the realm of cyber warfare and intelligence – but that immediately gives rise to an enormous problem. National security is grounded in the principle of national sovereignty and is thus enshrined in national law; international law plays only a very limited role. International law rarely addresses the topic of security and intelligence agencies; instead, these agencies operate purely within a national legislative and regulatory framework. Almost every country has (multiple) intelligence and security agencies, and they all carry out roughly the same work and operations, within the restrictions imposed by national law and, just as important, by their budgets. That is precisely what makes the debate about the role of these agencies so difficult, especially against the background of new technologies and unexpected clashes between national security and Internet security (and, in turn, national security again). Solutions are being considered in specified areas. For example, some argue that the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies should be extended to include cyberweapons and the trade in zero-day vulnerabilities (Stockton and

Golabek-Goldman 2013; Fidler 2014). Although that would regulate the international market to some extent, it would not really address the deeper cybersecurity dilemma.

4.5 TECHNOLOGICAL SOVEREIGNTY

Until recently, the idea of screening off a 'national' section of the Internet was one nurtured primarily by authoritarian regimes, with the Great Firewall of China and the National Internet in Iran as the most striking examples. In the post-Snowden era, however, it appears that more and more countries are looking for ways to better protect their 'own' Internet, data traffic and storage. The question of sovereignty has long been a factor in cyberspace, and even Western countries are not shy about enforcing their own national laws and rules in the digital domain. Recently, however, a number of countries have tested the waters with measures and initiatives that go a step beyond combating real-world crime – such as child pornography and copyright infringement – in cyberspace.

Many citizens and governments perceive the revelations about the NSA, the GCHQ and other intelligence agencies not only as a serious violation of privacy, but also as a challenge to sovereignty. It should be noted that almost all the states that feel compromised also have their own intelligence and security agencies with roughly the same mandate and powers. The difference between states seems to be more about budgets and technological capabilities than about the mandate and powers of the agencies themselves. Nevertheless, many countries were outraged by the scale and immensity of the NSA's surveillance and by its targets, whether political (friendly heads of state and government leaders such as Brazilian President Dilma Rousseff and German Chancellor Angela Merkel), intermediary (from Google to Belgacom) or economic (in some cases, spying in the name of national security bore a strong resemblance to economic espionage). Since intelligence agencies essentially operate outside any form of international regulation, and since such regulation is unlikely to emerge in future, the countries affected are looking for other ways to protect themselves against mass surveillance. Since many regard the US as the biggest digital infiltrator, and since it intercepted vast amounts of data mainly on websites, services, servers and clouds run by US corporations, they have contemplated or taken various steps to ensure that their data traffic circumvents the US or – if it runs via US platforms – to localise it where possible. 'Technological sovereignty', 'data sovereignty', 'data localisation' and 'national clouds' in fact all stem from the wish to avoid violations of privacy and prevent the surveillance of individuals, companies and governments by foreign powers.

Following the surveillance disclosures by Snowden, which began in June 2013, governments in various parts of the world debated new initiatives that qualify as attempts to achieve technological sovereignty and/or data localisation (see e.g.

Chander and Le 2014; Maurer et al. 2014; Polatin-Reuben and Wright 2014 for overviews). One well-known example is Brazil's plan to lay a new submarine cable that links it directly to Europe, so that Brazilian data no longer need to travel via American cables – and past the 'prying eyes' of the NSA. Europe has joined in with its own initiatives, although some proposals now appear to have been quietly removed from the agenda (Maurer et al. 2014). Some of these initiatives are based on the idea of mandatory local data storage and mandatory local data routing. The latter in particular clashes with the basic operation of the Internet Protocol, which assumes that data will take the route that the network considers most efficient at any given moment, depending on local data congestion. In addition, routing and storage are difficult to separate out in the era of cloud computing; storage or computing capacity is located wherever the cloud network is least congested at any given moment. Cloud data are therefore always in transit, a system inconsistent with localisation. In the EU, Germany has been the most vocal about increasing its technological sovereignty; it has proposed setting up national cloud services and has excluded foreign companies from contracts if they cannot guarantee that they will not share data with other governments. The German government's coalition agreement in fact explicitly states that it will make efforts to 'regain technological sovereignty' (CDU, CSU and SPD 2013: 103). In February 2014, French President François Hollande and German Chancellor Angela Merkel discussed setting up a 'European communications network' in which as much data as possible would be retained on a network of European servers (Maurer et al. 2014: 5). The press has referred to this as an 'EU cloud' or 'Schengen cloud'.[18] But data nationalism is also a rising trend in other parts of Europe and around the world.

Politicians and corporations in the US have been less than enthusiastic about the European proposals. Their resistance is politically and economically motivated (bad for Silicon Valley's global corporations, and excluding US firms is unfair competition), but also driven by worries about how the Internet will operate as a global network. The two arguments are sometimes combined in a way that suits the relevant party best, of course. The technical argument basically states that data sovereignty comes down to 'breaking the Web' (Chander and Le 2014) or 'the end of the Internet' (Goldstein 2014). That is an exaggeration, however. Local routing can certainly be implemented without impairing the Internet's infrastructure. Problems will only arise if users are forced to use local services because routing to other services has been blocked. In that case, localisation would undermine the distributed network that is the Internet, conflicting with the 'blind' operation of the Internet Protocol. If everyone wants as much of their data and data traffic as possible to circulate behind their own digital borders, then the nature of the global Internet will change. When Google's Law Enforcement and Information Security Director Richard Salgado testified before the US Senate in 2013, he warned of 'the creation of a "splinternet" broken up into smaller national and regional pieces with barriers

around each of the splintered Internets to replace the global Internet we know today'.[19] The question is whether the remedy is worse than the disease and – equally important – whether it will cure the disease at all.

A number of authors (Maurer et al. 2014; Chander and Le 2014) point out that local data storage and routing do not guarantee immunity from espionage, not least because intelligence agencies share quite a lot of information with each other internationally. The most prominent intelligence alliance, the 'Five Eyes', includes the UK, an EU member state. That means that the US already has easy access to a considerable amount of data captured by the British agencies. Using data localisation to shut the front door is useless unless we also look critically at the international exchange of bulk data between the various agencies. Recently, the Netherlands' Advisory Council on International Affairs (AIV) (2014: 61) recommended using the forthcoming reform of the Dutch Intelligence and Security Services Act (WIV 2002) to consider the provision of better privacy safeguards for citizens in the international exchange of data between national intelligence and security agencies. Purely local storage of crucial data obviously qualifies as an important security measure. Common sense tells us that some crucial data should be kept out of the cloud. But Maurer et al. (2014), Chander and Le (2014) and others favour a different solution to the problem of mass surveillance. *Encryption* of data traffic – both data in transit and stored data – would make it much harder and much more expensive for intelligence and security agencies to intercept data on a massive scale. It would force the agencies to make choices and to rein themselves in – something that scarcely seems necessary now, given the technology available to them. A rise in the costs would reinstate financial considerations as a buffer between state surveillance and privacy, in the manner described by Faris and Gasser (2013: 21) earlier in this chapter. It would force intelligence agencies to fine-tune and target their activities instead of throwing themselves into bulk data collection and other forms of 'dragnet surveillance' (Lyon 2014).

The final political argument favouring restraint in technological and data sovereignty stems from diplomatic considerations. The number of people using the Internet is set to increase exponentially in the years ahead, with most of the new users living in non-Western countries. Issues of sovereignty and misgivings about the Internet and its potentially liberating effect on the population play a much larger role in those countries than in the Netherlands and Europe. If Europe itself builds walls around the Internet that conflict with the operation of its core, then it undermines any attempts on its part to persuade other countries – countries starting out in the domain of Internet governance – of the importance of a properly operating public core. 'Practise what you preach' is usually the best motto in diplomacy, especially for those countries that need to win the day by the strength of their arguments.

4.6 CONCLUSION

This chapter has looked at how states are producing laws and policy measures which use the Internet's infrastructure to influence and regulate the behaviour of people, groups, businesses and other states. The main point to remember about the various trends described in this chapter is that states give their national or other private interests precedence over the collective interest of a reliable and functioning public core of the Internet. It should be noted that so far, any damage that may have been done to the Internet's public core has mostly been incidental in nature. However, if more and more states turn increasingly to policies that intervene in the Internet's core protocols – routing, DNS and IP, for example –their accumulated actions will ultimately do serious damage to the universality, interoperability and accessibility of the Internet. And once that has happened, it will be impossible to put the genie back in the bottle.

States are concerning themselves with the Internet's technical and logical core for a variety of reasons, including copyright protection and national security. Sometimes their actions affect the core protocols; at other times, high-risk vulnerabilities in software and protocols are 'kept secret' so that they can be exploited later. Such practices make the Internet as a whole less reliable, in the first place in the technical sense, but by extension in the economic and societal/cultural senses as well. After all, being unable to rely on the integrity, availability and confidentiality of the Internet will affect our willingness and ability to work with and on it. That in turn will affect the social and economic structure that we have built on that infrastructure, from online banking to communication. Some of these practices also simply make the Internet less secure. The overall security of cyberspace and the users that populate it is undermined when intelligence agencies 'preserve' vulnerabilities to facilitate cyber attacks, and when they deliberately build backdoors and weaknesses into the standards and software that everyone uses in order to give themselves easier access to data traffic. As Bruce Schneier put it, 'You can't build a back door that only the good guys can walk through'.

Our main conclusion is that governments need to exercise enormous restraint when considering policies, legislation and operational activities that intervene in the Internet's core protocols. At the same time, private parties must not be allowed to take liberties with the Internet's public core. Self-restraint is the biggest challenge in this respect. Ideally, the international norm should be non-intervention in the core protocols and basic technology of the public Internet. In Chapter 5, we will frame this idea as a core diplomatic challenge for the future. Restraint is a highly complex matter, however, as the benefits of policies serving the national interests accrue directly to national states, whereas the initial costs are borne collectively. But that logic only holds true in the short run. Everything that undermines the integrity and security of the Internet's global architecture will ulti-

mately boomerang on *every* national state, giving it the hallmarks of a collective action problem. It is also more difficult for states to exercise self-restraint if the policy in question is framed more in terms of a national security issue. Various pieces of legislation concerning online copyright protection bit the dust because, for the first time ever, freedom of speech and the Internet's operation as a whole were deemed to outweigh the economic interests involved. It was also one of the first times that a large online popular movement weighed in on the decision making. It is traditionally much more difficult to approach national security in this manner because it is shrouded in secrecy, is not subject to international law, and security quickly tends to trump other considerations. Just as in the non-virtual world, national interests often prevail in cyberspace. Even so, what we have here is an unadulterated digital version of the security dilemma, with cumulative interventions motivated by national security ultimately seriously undermining the security of the Internet.

In these border skirmishes between national security and the public Internet, restraint has little or no chance of succeeding without sufficient counterpressure. If we frame it in terms of Deibert's model of distributed security, what we lack is *mixture* and *division* – multiple actors with their own roles, powers and responsibilities. That is a serious problem when the issue is national security. The multi-stakeholder model is often put forward as a good way to give multiple relevant actors a role in governing the Internet, but a role cannot create counterpressure on its own if it is not accompanied by powers and responsibilities. That is in fact increasingly the case because states are demanding more responsibility and are pushing their own agendas. SOPA, PIPA and ACTA would probably have become law if they had not met with resistance from a broad coalition, including key figures in the technical community and major Internet companies and sites which forced politicians to acknowledge their responsibility for the governance of the global Internet. While outrage about the Snowden revelations and the implications for national security is widespread, there has been scarcely any organised marshalling of counter-power. We can explain this in part by the lack of international rules and the fact that almost all states grant their agencies the same powers. The question, however, is whether democratic and judicial oversight of these agencies is adequate in our high-tech, Big Data era. That question in on the table in the Netherlands, where the legislation underpinning its intelligence and security agencies (WIV) is currently under review. In the US, the Senate recently killed a bill (the USA Freedom Act) that would have introduced more oversight of the NSA and placed (somewhat) stricter limits on its surveillance. For the time being, then, nothing will change.[20]

There is some counterpressure from a number of the big Internet companies that were put on the spot by Snowden's leaks. Knowingly or unknowingly, they had delivered bulk data to the intelligence services. They are now responding by issu-

ing transparency reports disclosing – in so far as the law permits – which data or records governments request or demand. They are also improving their data encryption methods for users. The security agencies are working against them on both counts. And yet their response can be seen as a first move towards counter-power, with encryption raising the cost of mass surveillance and forcing the agencies to fine-tune their surveillance activities. Another example is the legal battle between the US and Microsoft in which the US government is demanding that Microsoft hand over data stored on a server in Ireland. Microsoft has refused because these data fall under Irish law, whereas the US reasons that it has the right to subpoena data held by a US company regardless of where they keep it.[21] Oddly enough, then, it is the major Internet companies that are battling government in defence of their customers' privacy, even though they themselves habitually transgress and push back the boundaries of privacy when it comes to managing their customers' data internally. Seeing how powerful these information giants are and the crucial role they play in digitising the lives of entire populations, governments can no longer avoid diplomatic dealings with them. These companies are more than potential investors that must be recruited, more than violators of privacy that must be tackled: they are parties that merit serious diplomatic attention owing to their vital role in digital life, with all the contradictions inherent in diplomacy.

In the same vein, governments must be clearer about what they expect of the many intermediaries in cyberspace that facilitate digital life, starting with the 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 ethically and responsibly with their customers, but also to comply with the demands of the competent authorities. In terms of Western standards, that may mean that Google can work with the US government but not with the Chinese. Although that may make sense from the perspective of human rights and the democratic rule of law, we are beginning to feel the absence of measured national strategies and a structured international discussion exploring what intermediaries may and may not do and what governments may and may not demand. When faced with a government request or subpoena (whether or not made in secret), intermediaries currently have three options: compliance, resistance and pre-emption. The last of these is undesirable from a rule-of-law perspective, and the first two are probably both necessary with a view to the separation of powers. Compliance alone or resistance alone would be problematic. We have yet to see the start of a structured discussion on this topic, certainly at international governmental level. A number of NGO's including the Electronic Frontier Foundation, the Centre for Internet Society India and Article 19 did launch the 'Manilla Principles'[22] in 2015, a framework that outlines clear, fair requirements for content removal requests and details how to minimize the damage a takedown can do.

NOTES

1 The title of this section hase been 'borrowed' from Milton Mueller (2010: 129).

2 The judgment in Case C-70/10 Scarlet v. SABAM states that EU Directives 2000/31, 2001/29, 2004/48, 95/46 and 2002/58 do not permit national courts to issue an injunction requiring an Internet service provider to install a filtering system blocking the transmission of copyright-protected electronic files on its network. A filtering system of this kind requires the provider to actively monitor all electronic communication on its network, which does not guarantee that a fair balance has been struck between the protection of intellectual property rights on the one hand and the freedom to conduct a business, the right to personal data protection and the freedom to receive or provide information on the other.

3 See: https://www.eff.org/deeplinks/2011/12/Internet-inventors-warn-against-sopa-and-pipa.

4 https://www.freedomonlinecoalition.com/.

5 Christopher Rhoads and Farnaz Fassihi, 'Iran Vows to Unplug Internet', *Wall Street Journal*, 28 May 2011, http://www.wsj.com/articles/SB10001424052748704889404576277391449002016.

6 See for example the Riga Joint Statement following the informal meeting of Justice and Home Affairs Ministers in on 29 January 2015, https://eu2015.lv/images/Kalendars/IeM/2015_01_29_jointstatement_JHA.pdf.

7 See: http://www.google.com/transparencyreport.

8 See: https://transparency.twitter.com.

9 See: http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency.

10 PRISM is a surveillance programme that the NSA uses to collect communications by foreign nationals at nine major companies, viz. Microsoft, Yahoo, Google, Facebook, Paltalk, YouTube, Skype, AOL and Apple. MUSCULAR is a surveillance programme operated jointly by the NSA and GCHQ which collects data from Yahoo and Google by secretly breaking into the links that connect the two companies' data centres. BULLRUN is a decryption program run by the NSA that decodes encrypted communication on the Internet in various ways, for example by influencing encryption standards so that they have weaknesses and 'backdoors'.

11 'Tim Berners-Lee: encryption cracking by spy agencies 'appalling and foolish'', *The Guardian*, 7 November 2013.

12 See: http://masssurveillance.info/openletter.pdf, accessed 10 December 2014.

13 Rob Lever, 'Crypto Wars 2.0 Have Begun After Privacy Moves By Apple And Google', *Business Insider*, 1 October 2014. See: , accessed 12 December 2014. See also: , accessed 12 December 2014.

14 See: https://www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html.

15 See for example the websites of VUPEN (http://www.vupen.com/english), Endgame (https://www.endgame.com), Revuln (http://revuln.com/index.htm), and Exodus Intelligence (https://www.exodusintel.com).

16 See: http://www.vupen.com/english/services/solutions-gov.php.

17 RSIS-Leiden, CTC Roundtable on civil-military relations in cyberspace, Singapore, 18-19 November 2014.

18 See: http://www.welt.de/politik/deutschland/article126343060/So-wuerde-Europas-Schengen-Internet-funktionieren.html.

19 See: http://www.judiciary.senate.gov/imo/media/doc/11-13-13SalgadoTestimony.pdf.

20 See: http://www.theguardian.com/us-news/2014/nov/18/usa-freedom-act-republicans-block-bill.

21 See for example: http://www.theguardian.com/technology/2014/dec/14/privacy-is-not-dead-microsoft-lawyer-brad-smith-us-government.

22 See: https://www.manilaprinciples.org/.

5 TOWARDS AN INTERNATIONAL AGENDA FOR INTERNET GOVERNANCE

5.1 INTRODUCTION: INTERNET GOVERNANCE BETWEEN THE TECHNICAL AND THE POLITICAL

Everyday life without the Internet has become unimaginable. It is rooted in our social lives, our purchasing behaviour, our work and our relationship with government, and is increasingly embedded in everyday objects and devices, from smart meters to the cars we drive and the moveable bridges that we cross *en route*. 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. And 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 interests, opportunities and vulnerabilities associated with the Internet have led governments to take much more interest in the governance of cyberspace. 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 are seeking to regulate their citizens' behaviour online, for reasons ranging from copyright protection and fighting cybercrime to censorship, surveillance and control of their own populations on and through the Internet.

Increasingly, governments view the core 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 (DeNardis 2012). States, for example, use DNS or IP protocols to block websites or make them unfindable. Such interventions may have huge implications for the backbone of the Internet, something that must be regarded as a global public good. As such, it should be protected against the interventions of states that are acting solely 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 simply 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 regarded as a global pub-

lic good – and thus safeguarded from improper interference – and what part should be seen as the legitimate domain of national states, where they can stake a claim and take up their role without harming the infrastructure of the Internet itself. Getting this question onto the international agenda and influencing the conduct of states will require new diplomatic efforts.

5.2 TOWARDS A NEW INTERNATIONAL AGENDA FOR INTERNET GOVERNANCE

5.2.1 THE NEED FOR CYBER DIPLOMACY

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 then allow the Internet to handle our private and work-related communications? 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 core protocols and infrastructures of the internet could lead to serious breakdowns in society and economy.

The integrity of the public core is a *conditio sine qua non* for the Internet's operation. Internet security is therefore one of the most fundamental of principles. For one thing, the aim of building a digital economy only makes sense if the Internet itself operates as it should. National and economic security also rest in part on a robust Internet infrastructure. Securing the Internet's public core will require much more coherent and political prioritisation of that goal than we see today, particularly where the international agenda is concerned. The Internet should be regarded as a critical priority in the foreign policy of all states whose economies and societies are interwoven with it. What is needed is the widespread international adoption of a diplomatic approach that gives precedence to the Internet's public core. The public core of the Internet's infrastructure not only requires states to take political action but also requires them to exercise restraint. That is a tall order for most countries in an uncertain (digital) world. Moreover, the diplomatic efforts that are needed to protect the public core of the Internet also require that states first put their own houses in order.

Smaller states are to some extent well placed to be in the vanguard of this diplomatic effort. Whereas large states often rely on 'hard' economic and military power, small states usually seek refuge in what Nye (2011: 20-21) calls 'soft power', i.e. influencing other states by formulating and framing the agenda, persuading others and generating positive interest in preferred outcomes (the good example). And whereas large and powerful states may benefit from 'strategic ambivalence', with the lack of clear-cut standards allowing scope for negotiation and room to manoeuvre, smaller states have a vested interest in channelling the discourse towards standardisation. Moreover, for a country such as the Netherlands, for example, protecting the Internet's public core follows from its own national interests. The reliable operation of the Internet is vital to the Dutch economy, long term economic growth and the functioning of Dutch society, both digital and real-world. The Netherlands has a lively Internet industry, and AMS-IX is one of the biggest Internet Exchange Points in the world (Deloitte 2014). The size of the overall Internet economy is difficult to measure, however, with new technologies emerging rapidly and with online and offline economy activity being closely intertwined (OECD 2014b). A recent estimate (Deloitte 2014) puts it at 5.3 percent of GDP. The Boston Consultancy Group (2014; 2011) has produced a somewhat lower figure of just over 4 percent, but it ranks the Netherlands among the top ten countries worldwide with the largest Internet economies, proportionately speaking. In other words, the Netherlands has much to gain when it comes to the functioning of the Internet's core infrastructures. It is however not alone in this. Many countries depend on the 'health' of the Internet, and as the digitisation of many parts of the world is still ongoing, their numbers are growing.

It is far from unusual for smaller states to assist at the birth of international standards or diplomatic breakthroughs. Developing and disseminating a new agenda for cyber diplomacy, based on the notion that the Internet's core must be safeguarded as a global public good, could be a task better suited to the leadership of the smaller rather than the bigger powers. The underlying principle – that safeguarding that public core also follows on from the national interests of other states – can serve to frame the international agenda. Diplomatic history offers an interesting example in this respect. The process towards the establishment of the Nuclear Non-Proliferation Treaty began when Ireland proposed banning the distribution of nuclear technology at a meeting of the UN's General Assembly. It was thus a small state with no nuclear capacity which took the initiative to formulate the first principles for a key international standard of restraint and, eventually, a regime of non-proliferation.

5.3 FRAMING THE AGENDA

This international agenda for Internet governance is grounded in Ronald Deibert's ideas about distributed security (see Chapter 2). That concept emphasises the need to organise power and counterpower in the international domain of Internet governance, the aim being to guarantee freedom. Deibert identifies three key principles of negarchy, borrowed from the context and tradition of national liberal democracy, which could be adapted to the international context. Those principles are *mixture, division* and *restraint*. *Mixture* refers to giving multiple actors roles and responsibilities in the system. *Division* is a design principle whereby none of these actors is able to control the system without the cooperation and consent of others. The principle of *restraint* involves reining in power by organising a system of checks and balances, for example in the form of oversight. Restraint can be both intrinsic – with parties placing checks on themselves – or enforced or monitored extrinsically through oversight by external parties or by means of administrative and legal arrangements.

These three principles cannot simply be transferred indiscriminately from the national to the international arena. Because institutions – with all their rules, procedures and responsibilities – play a more limited role internationally than in the national arena, the principles of mixture, division and restraint must allow for those parties that have the actual authority and/or power. In the cyber domain, these are often private parties. That does not mean that there are no formal and informal mechanisms in force that limit state sovereignty. There is a network of international and regional organisations in place – among them the UN and its subsidiaries, the EU, the AU, ASEAN etc. – which set boundaries for the conduct of states. Moreover, there is a body of international law that emerged both within and outside these organisations, which sets binding rules and standards for states and imposes obligations on them. But informal standards, mutual expectations, warnings and threats also play an important role in international relations. It is within the full breadth of this international political and legal context that Internet governance must ultimately be shaped. In some cases, that process can fall into step with ongoing international initiatives and take place within existing international legal and organisational contexts; in other cases, it will require the breaking of new diplomatic ground.

This section considers two main items for a cyber-diplomacy agenda that implicitly reflect Deibert's principles in various ways. The first is that the Internet's public core must be safeguarded against improper state interference driven by national interests. A standard of non-intervention should be adopted for the core architecture of the Internet. The second item focuses on de-securitising international cyberpolitics, for example by making a clearer distinction between different forms of security related to the Internet and to the parties involved.

5.3.1 THE INTERNET'S PUBLIC CORE SHOULD BE AN INTERNATIONAL NEUTRAL ZONE

This study has argued that the Internet consists of core protocols and technology that must be considered a *global public good*. If core protocols like TCP/IP, DNS and routing protocols do not operate 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 we send will arrive, that we can locate the sites we are searching for, and that those sites will be accessible. As a global public good, the Internet only works properly if its underlying values – universality, interoperability and accessibility – can be guaranteed and if it facilitates the main objectives of data security, i.e. confidentiality, integrity and availability. In 2008, the German Federal Constitutional Court formulated a new fundamental right to the 'confidentiality and integrity' of IT systems that clearly encompasses a number of these values.[1] It is vital that we – the users – can rely on the most fundamental Internet protocols to function properly. After all, those protocols underpin our entire online social and economic existence , and our confidence in that structure thus very much depends on them.

The need for worldwide agreement about the importance of properly functioning protocols seems obvious because it is these protocols that guarantee the reliability of the global Internet. However, recent international trends in policymaking and legislation governing the protection of copyright, defence and national security, espionage and various forms of censorship show that something else is afoot here. Some states see DNS, routing protocols, standards and the trend towards building in, keeping secret and manipulating software, hardware and protocol vulnerabilities as ideal 'tools' for national policy intent on monitoring, influencing and blocking the conduct of people, groups and companies. The external effects of such interventions in the core of the public Internet fall on the collective, however, and impairs the core values and operation of the Internet.

Within the scope of copyright, a dynamic coalition of engineers, Internet companies and websites, NGOs and users managed to block two US bills – the Stop Online Piracy Act (SOPA) and the PROTECT IP Act (PIPA) – and the Anti-Counterfeiting Trade Agreement (ACTA), all three of which would have permitted the use of vital Internet protocols to regulate and block content. These protests made politicians aware that such interventions actually involved tampering with the Internet itself. Crushing these bills has not wiped the ideas and technology behind this type of legislation off the map, however.

States take even greater liberties with the Internet's public core when it comes to their national security. Military cyber commands, intelligence and security agencies, and sometimes even law enforcement agencies are increasingly putting national security above the collective interest of a properly functioning Internet.

Because these policies concern national security – or at least are 'framed' in that way – most national legislatures have a strong tendency to support them. An additional factor with respect to intelligence agencies is that they are regulated solely at national level, as there is virtually no international law pertaining to them. Taken together, these trends could lead to a digital version of the security dilemma (Jervis 1978), 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 (Dunn Cavelty 2014). There is an enormous risk that the cumulative effect of national measures – with states increasingly engaged in a 'cyber arms race' – will introduce serious vulnerabilities into the core of the Internet as a public infrastructure. On top of this, there is the paradox that some parts of national government have made safeguarding a reliable and secure Internet their mission whereas other parts are increasing the risk in this area.

To some degree we are still at the start of this development. A number of powerful states have built up significant cyber capacity and are way ahead of the rest in this trend, which is a dubious one from the vantage point of the Internet as a global public good and global Internet security. But many countries are now in the middle of digitising their state, economy and society and are still building cyber capacity. When the next billion (or billions) of users go online in the years ahead, these 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 core protocols and infrastructure of the Internet instrumentally in those efforts. Some of these countries 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 core as their societies continue to digitise. In addition, 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 cutting edge today will be commonplace in five years' time. If in that same timeframe 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 global public good is likely to be very damaging. For this reason there is no time to lose in securing the public core of the Internet.

Given these developments, it should be an internationally shared priority to work towards establishing an international standard 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 (Knapen et al. 2011), i.e. a specific area where national interests and

global issues coincide for all states that 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 core – its main protocols and infrastructure, which are a global public good – must be safeguarded against intervention by governments.

In terms of distributed security, the main challenge in this context will be to organise negation and restraint of power at the international level, with restraint being the intrinsic task assigned to states (they must place restrictions on themselves) and negation being the task assigned to the collective (how can the standard be established and monitored?). The first task will be to get the drafting of such a standard onto the international political agenda, and that will require making governments all around the world aware of the collective importance of this neutral zone. Given the enormous differences between countries in terms of Internet access, overall digitisation and technological know-how, this will require a tremendous diplomatic effort. The task of restraint naturally goes beyond merely establishing a standard, but doing so is a vital first step and can provide an important reference point.

Operational strategy

One important question in this context is whether a standard of this kind should immediately take the form of a treaty or convention. Doing so, however, makes the substance of the convention subject to a multilateral negotiation game in which the outcome is often the lowest common denominator. There are advantages to dividing up the efforts into smaller steps instead of banking on a treaty governing the Internet or a convention that regulates cyber conflicts and cyber warfare. Standards have already been a topic of discussion at many conferences in the cyber domain, recently also attracting input from private parties such as Microsoft (2015), arguing mainly for norms that states should adhere to. They have also been the subject of a series of GGEs (Groups of Governmental Experts) on information security. Acting under the auspices of the UN but not under any treaty, these GGEs have attempted to establish standards, principles and Confidence-Building Measures (CBMs) pertaining to the Internet and international security (Kane 2014; Hurwitz 2014). In 2015 the most recent GGE delivered its report addressing issues such as the problem of backdoors in ICT products and requesting states to prevent their proliferation.[2] An international standard that designates the Internet's core protocols as a neutral zone would have a broader and more potent impact if it were negotiated and disseminated in parallel to the route of the GGE, which focuses on national security and on preventing escalations of cyber conflicts. Moreover, the advantage of a standard that defines the Internet as a global public good is that it avoids any direct attempt to regulate intelligence and security agencies interna-

tionally. Considerations of sovereignty are likely to make any such direct attempt impossible. The standard of non-intervention has an indirect effect because it limits what is and is not permissible on the Internet within the context of national security. Compliance with the standard would be subject to national democratic and legal oversight. Although disseminating this standard does not in itself guarantee compliance, it does create a benchmark for evaluating and judging the conduct of states – even those that have not recognised the standard officially.

The starting point would be to define and draft the standard and to disseminate it within international forums that are relevant for various aspects of Internet governance. It could be disseminated through relevant UN forums and bodies, as well as though regional organisations such as 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.

5.3.2 THE NEED TO DISENTANGLE INTERNET SECURITY AND NATIONAL SECURITY

The second item on the diplomatic agenda is the need to steer the debate about Internet governance away from the domain of national security and to disentangle the various forms of security that are relevant to and on 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 (Hansen and Nissenbaum 2009; Dunn Cavelty 2013; Singer and Friedman 2013). 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 legislated powers, especially in the United States. This could lead to a far-reaching militarisation of the cyber domain, the rise of a new cyber military-industrial complex and even an arms race in cyberspace. This is in spite of the fact that initial attempts to study how the law of armed conflict applies to cyber conflicts, 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'.

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

- It is therefore vital to advocate at the international level that a clear differentiation be made 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. At one end of the spectrum there is the notion of Internet security, i.e. ensuring that the network itself is secure and operational. At 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 agencies as the primary national, regional and international actors. Across the entire spectrum, private parties also play various roles: as developers and suppliers of technology, as businesses that protect their own networks, and as consultants which implement 'security' on or by means of the Internet, for clients ranging from Shell to the NSA.

Internet security relates to a technology-driven strategy, such as that of the Computer Emergency Response Teams (CERTs) which 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. 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 which safeguard the security of the Internet itself. The recent 2015 GGE report takes a similar line by urging states to neither harm the systems and activities of other (national) CERTs, nor to use their own to engage in malicious international activity.[3] The principle of division is of paramount importance here. Confusing the two logics, or allowing the national security logic to 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 (Broeders 2014).

Division is important as well because the logic of national security implies a much lower tolerance of risk and therefore a much higher risk of escalation. There is little political scope for 'residual risk' and 'trial and error' in the realm of national security, since a single error at the highest level of security could be fatal. That logic brushes aside other takes on security in which the stability and integrity of the Internet as a global public good are at least as important, if not more so. Van Eeten and Bauer (2009) compared 'precluded event security' and 'marginal security cost' in this connection. The first involves an absolute security standard to which almost everything else must give way; the second weighs security against the cost

to society. Such costs go beyond the financial– security is an expensive affair – to include intangible costs, for example fundamental rights and the rule of law (AIV 2014) and the level of trust between the organisations and individuals involved in internet security. The point would be to allow more room for the logic of residual risk in matters of cyber security and to apply the logic of national security more selectively in order to avoid or mitigate escalation.

Operational strategy

The debate concerning the highest levels of national security – military cyber commands and intelligence and security agencies – is simultaneously the most crucial and the most complicated from a perspective of restraint. Considerations of state sovereignty make regulating these actors through international law or agreements a highly complex affair. It should be noted, however, that this is a new area in which some issues will remain the same – and the offline rules should 'simply' be adapted to create online rules – and some will change considerably. As the fifth domain of warfare, cyberspace is not only an entirely man-made construct but is also largely in private hands. That raises new questions about what is and is not permissible and how much states, for example, are allowed to interfere in private hardware and software. The lively trade in 'zero-day vulnerabilities' – flaws in everyday software and hardware that intelligence agencies and military cyberunits can exploit to gain access to private systems and information – is taking place in a grey area. As complicated as it may seem, we can improve the regulation of this domain by launching a serious national and international political debate about what countries do and do not consider acceptable, and how to weigh their concerns against other views on cyber and Internet security. Unfortunately, it is an issue that has probably only made it onto the desk of government and the floor of the legislature in a very small number of capitals worldwide. In the business world, cyber security is now increasingly a matter for the CEO and his or her boardroom. Cyber and Internet security – and the external effects of favouring one take on security on the Internet over another – should also be discussed by the cabinet and in the legislature.

We are only at the start of this process in the international arena, despite existing international agreements to work on establishing 'norms, rules and principles of responsible behaviour of states' in the cyber domain, for example as stipulated in the Seoul Framework for and Commitment to Open and Secure Cyberspace.[4] There are, of course, various initiatives under way to arrive at common standards, but the discourse is taking place mainly *within* the context of the high politics of international security and is intended to prevent escalation between states. The Groups of Governmental Experts (GGE) and other similar initiatives emphasise codes of conduct and Confidence-Building Measures that are meant to prevent states from misinterpreting each other's conduct online. Such measures may result in information-sharing about national cyberstrategies, dialogues between various

states, and international assistance for weaker states in building cyber capacity for defensive purposes (Kane 2014; Hurwitz 2014). A clear division between different forms of security and the delineation of the domains of the various actors involved could be beneficial in these ongoing international discourses about standards in cyberspace and their regional versions, such as NATO and the OSCE in Europe and ASEAN in Asia. That is certainly true if the rationale behind these positions is the idea that improper intervention in the Internet's public core should be declared out of bounds. This standard can also help disentangle various forms of security, since some views on security do support the integrity of the public core – Internet security – whereas other forms of national security may avail themselves of instruments that in fact damage it. Another matter to consider is the need to determine what might be possible and acceptable forms of transparency with respect to the activities of the various parties. In terms of Internet security as viewed by the CERTs, the Cyber Green Initiative is one of several ongoing initiatives (see Chapter 3). In terms of national security, transparency has so far mainly resulted from the actions of whistleblowers such as Chelsea Manning and Edward Snowden. Transparency at a – necessarily – high and abstract level in domestic politics could make it easier to assess the usefulness and necessity of certain national programmes pursued by intelligence or security agencies and, by offering reassurance, could serve as a confidence-building measure internationally (see also Swire 2015). Robust systems of judicial and democratic oversight at the national level could be important building blocks for improving international relations in cyberspace, as well as institutional safeguards against domestic and international abuse of power by these agencies.

5.4 BROADENING THE DIPLOMATIC ARENA

The third item on the agenda for cyber diplomacy is more procedural in nature and focuses on the parties that should be involved in or be the subject of the diplomatic efforts. Broadening the diplomatic arena should be an important part of the international agenda for Internet governance. The demographic shift in engagement with the Internet and the rise of new large and mid-level powers in relation to the Internet, challenges the still very dominant transatlantic take on Internet governance. Also, the damage done to the US's moral leadership in Internet matters as a result of the Snowden revelations has undercut the 'Western' dominance in the debates about Internet governance. 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' – fully 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. Lastly, states should develop a realistic approach to the role of NGOs and other stakeholders.

5.4.1 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 public core. While the 'usual suspects' in the transatlantic axis, i.e. the EU and the OECD, are 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 (Hurwitz 2014: 330). That became clear during the 2012 World Conference on International Telecommunications in Dubai, when it was time to vote on the International Telecommunications Regulations (ITRs). 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 potentially open the door to its nationalisation, or balkanisation. In addition to countries that have opposing notions of the Internet and Internet governance, there is also a large group of countries that have not yet taken up a firm position on the issue of Internet governance. These states are developing their strategy, policies and capacity to engage with Internet governance issues, especially at the international level. As sovereign nations, they have a seat in relevant regional and international organisations, and many of them join in negotiations about certain specific matters, such as the IANA stewardship transition and the ITRs referred to above.
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. A demographic shift is taking place in cyberspace, with the centre of gravity moving from the North and West to the East and South. Voices other than European and American ones will grow louder in the near future and will emphasise other economic and political ideas.

The principle of restraint surfaces in various areas, for example in the debate about the transition process for the Internet Assigned Numbers Authority (IANA)stewardship. The question there is what form that stewardship – currently in the hands of the Internet Corporation for Assigned Names and Numbers, or ICANN (under contract with the US government) – should take. One good starting point would be to draw a clear distinction between oversight (the IANA stewardship) and ICANN's more politically controversial tasks, for example creating new domain names. As a densely networked country and the host of an important digital exchange, the Netherlands would benefit greatly from technical management that is as 'agnostic' as possible. The management of domain names and numbering facilities – the beating heart of the Internet address system – must keep the realm of politics at bay as far as possible. In the interest of maintaining the Internet in the

long term as a properly operating collective infrastructure, there is every reason to disseminate this viewpoint actively in the international arena and to broaden the coalition of states that subscribe to it.

Operational strategy

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. Diplomatic efforts focused on securing the public core 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 (2014) identified a 'top 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.

International dialogue on these subjects has already begun, but needs to be reinforced. For example, the EU also has a number of institutionalised strategic partnerships with important third-party countries with which it regularly engages in dialogue. In fact, it is already involved in 'cyberdialogues' with the USA, Brazil, China and India, although the nature of these discussions differs considerably in each case. It is also working to broach the subject of the Internet with other countries, including Japan, Mexico, Russia, South Africa and South Korea (Renard 2014).[5] A number of the EU's strategic partners – Brazil, Mexico, India, South Africa and South Korea – also appear on the list of swing states. Moreover, the EU Member States decided in early 2015 to develop and implement a 'common and comprehensive EU approach for cyber diplomacy at global level'.[6] Part of this decision involves developing 'norms for responsible state behaviour in cyberspace'. Multilateral initiatives such as these should be expanded where possible, but should not stop individual states from embarking on their own dialogues and developing their own initiatives where necessary or useful.

5.4.2 MAKE PRIVATE PARTIES PART OF THE DIPLOMATIC DIALOGUE

In the predominantly privately owned and run world of the Internet, Apple, Google, Huawei, 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 counterpower, and – as in diplomatic relations between states – the interests and agendas of such corporations will sometimes align and sometimes conflict with national and collective political 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 (AIV 2014).

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, but are not limited to, 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 weight is considerable, its gears grind slowly compared to the fast-paced Internet economy. That much became clear in the infamous case that the European Commission brought against Microsoft under EU competition law. While the fine was high and proportionate ($860 million), the proceedings took so long that it was tantamount to 'solving the antitrust problem long after the competitors have died' (Brown and Marsden 2013: 40). Nevertheless, the authority to impose 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 (Börzel and Risse 2010). Governments need to realise that being on the receiving end of a lobbying campaign by these powerful companies is not the same as – or a substitute for – engaging in a diplomatic dialogue with them.

Recently, Internet companies have pushed back both informally and formally against governments, and especially against the US. This was mostly the result of the Snowden revelations, which have seriously damaged the global reputation of a number of leading American Internet companies among Internet users. Snowden's files put these big Internet-based companies on the spot as they were – intentionally or unintentionally – the sources of masses of data collected by the intelligence services. Some of Silicon Valley's biggest Internet companies are responding by stepping up the use of transparency reports that disclose – as far as the law permits – what data or records governments request or demand, and by using increasingly sophisticated encryption of their data transport (Van Hoboken and Rubinstein 2014). Although opportunism and damage control explain much of this behaviour aimed at retaining and regaining customers, it is an interesting development in terms of power and counterpower. By raising the cost of mass surveillance

through better encryption, and thus putting pressure on intelligence services to fine-tune their surveillance, their response may be seen as a move towards counterpower. Microsoft is also taking on the US government in the courtroom, challenging its assertion that all data managed by a US company – even if it is held on servers in Ireland – can be commandeered by government.[7] In the light of their economic weight and their crucial role in shaping the information society on a global scale, governments can no longer avoid diplomatic dealings with these information giants. These companies are more than potential investors that have to 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 in diplomacy.

In similar vein, governments need to be more explicit about what they expect of the many intermediaries in cyberspace which facilitate digital life, starting with ISPs but also including search engines, cloud services, and so on. These companies often occupy a very uneasy middle ground between their customers and various governments. They are expected to deal with their customers ethically and responsibly, but also to comply with the legal requirements and demands of the authorities. In international terms, that may sometimes be seen to mean that Google should work with the UK government but not with the Russian government, depending on the case and the nature of the request. Although that may make sense from the perspective of human rights and the democratic rule of law, there is a manifest 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. When faced with a government request or subpoena, intermediaries currently have three options for their course of action: compliance, resistance and pre-emption. Pre-emption, where intermediaries take preventive action, such as blocking access to websites and content without being formally requested to do so, is undesirable from a rule-of-law perspective. Compliance and resistance are probably both necessary with a view to the division of power, although only compliance or only resistance would be problematic. The deputation of private companies comes at the price of what has been termed 'intermediary censorship' (Zuckerman 2010; MacKinnon 2011), meaning that decision-making on what is and is not allowed slowly shifts towards private parties. We have yet to see the start of a structured discussion on this topic, certainly at international governmental level. A number of NGO's including the Electronic Frontier Foundation, the Centre for Internet Society India and Article 19 did launch the 'Manilla Principles'[8] in 2015, a framework that outlines clear, fair requirements for content removal requests and details how to minimize the damage a takedown can do.

Operational strategy

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.[9] 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 develop a legally binding instrument on multinationals with respect to human rights.[10] The protection of the Internet as a global public good, and the role that private companies can play in this regard, could follow a similar trajectory. The framework should make the role and responsibilities of Internet-based companies clearer and ensure that they 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 core of the Internet.

5.4.3 REALISM IN RELATIONSHIPS WITH NGOS

While many countries formally embrace the multistakeholder model of Internet governance, this notion is at odds with the growing role that states are demanding for themselves in this domain. The Internet is in reality governed by an amalgam of private and semi-private parties, but with national and international regulatory pressure mounting, governments are increasingly redefining the boundaries. At the same time, a wide variety of different NGOs are working at the national and international level to safeguard the nature, the use, and the future of the Internet – as they see it. The topics they address and the interests they represent vary greatly, from the protection of human rights and dissidents online to the management of the technical part of the Internet. Broad coalitions of NGOs, concerned web users, Internet businesses and organisations and individuals representing the technical community can sometimes make a difference in policy development. That is what happened in the case of SOPA/PIPA and ACTA. Some NGOs have a high-profile presence and influence internationally, but when it comes to drafting agreements and drawing up conclusions at official conferences concerning the governance and future of the Internet, there is often no place for them at the table. For example, NGOs turned out in force at the two meetings of the UN World Summit on the Information Society, the first in Geneva in 2003 and the second in Tunis in 2005. But when the Declaration of Principles and Plan of Action were being drawn up, it was mainly the states who were allowed to take the floor and who tightly grasped the pen. The NGOs' input into the final texts and output documents was small (Dutton and Peltu 2010; Cogburn 2010), feeding their frustration. At this point, and especially after the NETmundial meeting in Brazil, which gave its full support to the multistakeholder model, states should facilitate productive input

by NGOs without raising false hopes. With Internet governance becoming more political and subject to increasing state intervention, their contribution to the formal process is more likely to decrease than increase. National states will need to develop new strategies to make productive use of their and other stakeholders' input – in addition to the autonomous public strategies that NGOs deploy at national and international level in their efforts to influence matters.

Operational strategy

In shaping national – and certainly international – policy, states would do well to make the most use of the knowledge of NGOs (for example about human rights in certain countries) and the technical community (for example about the technical consequences of proposed policy). Their input would be extremely useful when thinking through the effects of Internet governance on the technical operation of the Internet as a whole, because it is precisely in that area that it is vital to link diplomatic knowledge and skill on the one hand to technical knowledge and skill on the other.

5.5 NEW COALITIONS FOR THE PROTECTION OF THE INTERNET'S PUBLIC CORE

This book has argued that the Internet's core 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 a broadening of the diplomatic arena, as well as investment 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 their own national interests.

NOTES

1 See: https://www.axelarnbak.nl/2014/05/21/opinie-fd-en-lezing-eerste-kamer-nederland-als-Internetdokter-tussen-cybergrootmachten and http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.

2 See paragraph 13(i) of the Report of the Group of Governmental Experts On Developments in the Field of Information and Telecommunications In the Context of International Security, Report as adopted, Friday 26 June.

3 See paragraph 13(k) of the adopted GGE report of 26 June 2015.

4 See: https://www.gccs2015.com/sites/default/files/Seoul%20Framework.pdf.

5 See also the Outline for European Cyber Diplomacy Engagement, See also the Outline for European Cyber Diplomacy Engagement, http://data.consilium.europa.eu/doc/document/ST-9967-2014-INIT/en/pdf.

6 See: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

7 See for example: http://www.theguardian.com/technology/2014/dec/14/privacy-is-not-dead-microsoft-lawyer-brad-smith-us-government.

8 See: https://www.manilaprinciples.org/.

9 See: http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

10 http://business-humanrights.org/en/binding-treaty/un-human-rights-council-sessions.

BIBLIOGRAPHY

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

AIV/CAVV (2011) *Digitale oorlogsvoering*, nr. 77, AIV/ nr. 22, CAVV, The Hague.

Anders, G. (2014) 'The Right Way to Fix the Internet. Letting Go of an Obsession with Net Neutrality Could Free Technologists to Make Online Services Even Better', *MIT Technology Review*, 14 October 2014.

Ashgari, H., M. van Eeten, J. Bauer and M. Mueller (2013) 'Deep Packet Inspection: Effects of Regulation and its Deployment by Internet Providers', Paper presented at TPRC 2013, 25 September 2013.

Bauman, Z. et al. (2014) 'After Snowden: Rethinking the Impact of Surveillance', *International Political Sociology*, 8 (2): 121-144.

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.

Benkler, Y. (2012) 'Seven Lessons from SOPA/PIPA/Mega Upload and Four Proposals on Where We Go from Here', available at http://techpresident.com/news/21680/seven-lessons-sopapipamegauplaod-and-four-proposals-where-we-go-here, 25 January 2012.

Betz, D. and T. Stevens (2011) *Cyberspace and the State. Towards a Strategy for Cyber-power*, London: Routledge.

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

Boston Consultancy Group (2011) *Interned. Hoe het Internet de Nederlandse economie verandert*, Amsterdam: The Boston Consultancy Group.

Boston Consultancy Group (2014) *Connecting the World. Greasing the Wheels of the Internet Economy*, study commissioned by ICANN, The Boston Consultancy Group.

Boyle, J. (1997) 'A Politics of Intellectual Property: Environmentalism for the Net?', *Duke Law Journal,* 47: 87-116.

Bradford, A. (2012) 'The Brussels Effect', *Northwestern University Law Review*, 107 (1): 1-68.

Breindl, Y. and F. Briatte (2010) 'Digital Network Repertoires and the Contentious Politics of Digital Copyright in France and the European Union', *Internet, Politics, Policy 2010: An Impact Assessment,* sep 2010, Oxford, Untied Kingdom.

Breindl, Y. (2013) 'Internet Content Regulation in Liberal Democracies. A Literature Review', *DH Forschungsverbund – Working Papers zu Digital Humanities,* 2.

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.

Brown, I. and C. Marsden (2013) *Regulating Code: Good Governance and Better Regulation in the Information Age*, Cambridge (Mass.): MIT Press.

Budish, R. and P. Kuman (2013) 'Just in Time Censorship: Targeted Internet Filtering During Iran's 2013 Elections', pp. 32-33 in: U. Gasser, R. Faris and R. Heacock (eds.) *Internet monitor 2013: Reflections on a Digital World*, Cambridge (Mass): The Berkman Center for Internet and Society.

CBS (2014) *ICT, kennis en economie 2014,* The Hague: CBS.

CDU, CSU and SPD (2013) 'Deutschlands zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD', https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf.

Cerf, V. (2013) 'Revisiting the Tragedy of the Commons', *Communications of the ACM*, 56 (10): 7.

Chander, A. and U. Le (2014) 'Breaking the Web: Data Localization vs. the Global Internet', *Emory Law Journal* (forthcoming), available online at: http://ssrn.com/abstract=2407858.

Choucri, N. (2012) *Cyberpolitics in International Relations*, Cambridge (Mass.): MIT Press.

Clarke, R. and R. Knake (2010) *Cyber War: The Next Threat to National Security and What to Do About It,* New York: Harper Collins.

Clemente, D. (2013) *Adaptive Internet Governance: Persuading the Swing States*, CIGI Internet Governance Papers nr. 5 (October 2013).

Clinton, H. (2010) *Remarks on Internet Freedom*. Speech at the Newseum, Washington D.C., 21 January 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm.

Cogburn, D. (2010) 'Enabling Effective Multi-stakeholder Participation in Global Internet Governance Through Accessible Cyber-infrastructure', pp. 401-423 in A. Chadwick and P. Howard (eds.) *The Routledge Handbook of Internet Politics*, London: Routledge.

Council on Foreign Relations (2013) *Defending an Open, Global, Secure and Resilient Internet,* New York: Council on Foreign Relations.

Crocker, S., D. Dagon, D. Kaminsky, D. McPherson and P. Vixie (2011) 'Security and other Technical Concerns Raised by the DNS Filtering Requirements in the Protect IP Bill', http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf.

Czyz, J., M. Allman, J. Zhang, S. Iekel-Johnson, E. Osterweil and M. Bailey (2013) *Measuring IPv6 Adoption,* ICSI Technical Report TR-13-004, August 2013.

Danaher, B., M.D. Smith and R. Telang (2013) 'Piracy and Copyright Enforcement Mechanisms', *Innovation Policy and the Economy*, 14.

Degli Esposito, S. (2014) 'When Big Data meets Dataveillance: the Hidden Side of Analytics', *Surveillance and Society*, 12 (2): 209-225.

Deibert, R., J. Palfrey, R. Rohozinski and J. Zittrain (2008, eds.) *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge (Mass.): MIT Press.

Deibert, R., J. Palfrey, R. Rohozinski and 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 and J. Zittrain (2011, eds.) *Access Contested. Security, Identity, and Resistance in Asian Cyberspace*, Cambridge (Mass.): MIT Press.

Deibert, R. and R. Rohozinski (2011) 'Liberation versus Control: the Future of Cyberspace', *Journal of Democracy,* 21 (4): 43-57.

Deibert, R., J. Palfrey, R. Rohozinski and J. Zittrain (2011, eds.) *Access Contested. Security, Identity, and Resistance in Asian Cyberspace*, Cambridge (Mass.): MIT Press

Deibert, R. (2012) *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyber Space*, Calgary: Canadian Defense & Foreign Affairs Institute.

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. (2014) 'Divide and Rule. Republican Security Theory as Civil Society Cyber Strategy', *The Georgetown Journal of International Affairs*, 20: 45-56.

Deloitte (2014) *Digital Infrastructure in the Netherlands. Driver for the Online Ecosystem.*

DeNardis, L. (2009) *Protocol Politics. The Globalisation of Internet Governance*, 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) *Internet Points of Control as Global Governance*, CIGI Internet Governance Papers no. 2 (August 2013).

DeNardis, L. (2014) *The Global War for Internet Governance*, New Haven and London: Yale University Press.

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

Demchak, C. and P. Dombrowski (2014) 'Cyber Westphalia. Asserting State Prerogatives in Cyberspace', *The Georgetown Journal of International Affairs.* International Engagement on Cyber III. State Building on a New Frontier, 20: 29-38.

Dijck, J. van (2014) 'Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology', *Surveillance and Society*, 12 (2): 197-208.

Dubuisson, T. (2012) 'When the World Wide Web becomes the World Wild Web; PIPA, SOPA, OPEN Act, CISPA and the 'Internet Revolution', sssrn-id2373906.pdf

Dunn Cavelty, M. (2012) 'The Militarisation of Cyberspace: Why Less May Be Better', pp. 141-153 in: C. Czossceck, R. Ottis and K. Ziolkowski (eds.) *2012 4th International Conference on Cyber Conflict,* Talinn: NATO CCD COE 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.

Dutton, W. and M. Peltu (2010) 'The New Politics of the Internet. Multi-stakeholder Policy-making and the Internet Technocracy', pp. 384-200 in A. Chadwick and P. Howard (eds.) *The Routledge Handbook of Internet Politics*, London: Routledge.

Eeten, M. van and J. Bauer (2009) 'Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications, *Journal of Contingencies and Crisis Management*, 17 (4): 221-232.

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*, The Hague: Raad voor Maatschappelijke Ontwikkeling.

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

Faris, R. and U. Gasser (2013) 'Governments as Actors', pp. 19-24 in: U. Gasser, R. Faris and R. Heacock (eds.) *Internet monitor 2013: Reflections on the Digital World*, Cambridge (Mass.): The Berkman Center for Internet and Society at Harvard University.

Faris, R. and R. Heacock Jones (2014) 'Platforms and Policy', pp. 28-35 in: U. Gasser, J. Zittrain, R. Faris and R. Heacock Jomes (eds.) *Internet Monitor 2014: Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse,* Cambridge (Mass.): The Berkman Center for Internet and Society at Harvard University.

Fidler, M. (2014) *Anarchy or Regulation? Controlling the Global Trade in Zero-day Vulnerabilities*, Honors Thesis in International Security Studies, Stanford University.

Fillipini, P. de and L. Belli (2014) 'Introduction. Network Neutrality: An Unfinished Debate', pp. 3-16 in: L. Belli and P. De Fillipini (eds.) *Network Neutrality: An Ongoing Regulatory Debate*. 2nd Report of the Dynamic Coalition on Network Neutrality.

Garton-Ash, T. (2013) 'If Big Brother Came Back, He'd Be a Public-Private Partnership', *The Guardian*, 27 June 2013.

Glennon, M. (2014) 'National Security and Double Government', *Harvard National Security Journal,* 5 (1): 1-114.

Goldsmith, J. and T. Wu (2008) *Who Controls the Internet? Illusions of a Borderless World*, Oxford: Oxford University Press.

Goldstein, G. (2014) 'The End of the Internet? How Regional Networks May Replace the World Wide Web', *The Atlantic*, July/August, http://www.theatlantic.com/magazine/archive/2014/07/the-end-of-the-Internet/372301.

Graham, M. (2014) 'Internet Geographies: Data Shadows and Digital Divisions of Labour', pp. 99-116 in: M. Graham and W. Dutton (eds.) *Society and the Internet: How Networks of Information and Communication are Changing Our Lives*, Oxford: Oxford University Press.

Graham, M., De Sabbata, S., Zook, M. 2015. Towards a study of information geographies: (im)mutable augmentations and a mapping of the geographies of information *Geo: Geography and Environment*.2(1) 88-105. doi:10.1002/geo2.8

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

Guitton, C. (2013) 'Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?', *European Security*, 22 (1): 21-35.

Haas, P. (1992) 'Introduction: Epistemic Communities and International Policy Coordination', *International Organization*, 46 (1): 1-35.

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

Herold, D. (2011) 'An Inter-nation-al Internet: China's Contribution To Global Internet governance?', Paper Presented at Symposium 'A Decade in Internet Time', 22 September 2011, Oxford: Oxford Internet Institute.

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.

Hofmann, J. (2012) 'Narratives of Copyright Enforcement: The Upward Ratchet and the Sleeping Giant', *Revue francaise d'études Américaines*, 43: 4.

Howard, P., S. Agarwal and M. Hussain (2011) 'When Do States Disconnect Their Digital Networks? Regime Responses to the Political Uses of Social Media', *The Communication Review*, 14: 216-232.

Hughes, R. (2010) 'A Treaty for Cyberspace', *International Affairs*, 86 (2): 523-541.

Human Rights Watch (2012) *In the Name of Security. Counterterrorism Laws Worldwide since September 11,* http://www.hrw.org/sites/default/files/reports/global0612ForUpload_1.pdf, accessed 1 August 2012.

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.

Kitchin, R. (2014) *The Data Revolution. Big Data, Open Data, Data Infrastrcutures and Their Consequences*, London: Sage.

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. (2013) 'Making Sense of Snowden: What's Significant in the NSA Revelations', *IEEE Security & Privacy*, 11 (4): 54–63.

Landau, S. (2014) 'Making Sense of Snowden, Part II: What's Significant in the NSA Revelations', *IEEE Security & Privacy*, 12 (1): 62–64.

Lawson, S. (2013) 'Beyond Cyber-doom: Assessing the Limits of Hypothetical Scenario's in the Framing of Cyber-threats', *Journal of Information Technology and Politics*, 10: 86-103.

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

Lessig, L. (1999) *Code and Other Laws of Cyber Space*, New York: Basic Books. Lewis, J. (2013) *Internet Governance: Inevitable Transitions*, CIGI Internet Governance Papers nr. 4 (October 2013).

Lessig, L. (2006) *Code. Version 2.0*, New York: Basic Books.

Lewis, J. (2013) *Internet Governance: Inevitable Transitions*, CIGI Internet Governance Papers nr. 4 (October 2013).

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 Pretention, More Ambition. 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.

Lyon, D. (2014) 'Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique', *Big Data & Society*, July-September 2014: 1-13.

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.

Maher, K. (2013) 'The New Westphalian Web', *Foreign Policy Magazine Online*, 25 February 2013.

Marks, G. and L. Hooghe (2004) 'Contrasting Visions of Multi-level Governance', pp. 15-30 in Bache, I. and M. Flinders (eds.) *Multi-level Governance*, Oxford: Oxford University Press.

Masnick, M. (2014) 'The Rebranding of SOPA: Now Called 'Notice and Staydown'', *Techdirt,* 14 maart 2014. Available at: 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 no. 7 (May 2014).

Maurer, T., R. Morgus, I. Skierka and 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.

Mayer-Schönberger, V. and K. Cukier (2013) *Big Data. A Revolution That Will Transform How We Live, Work and Think*, London: John Murray Publishers.

McDiarmid, A. and D. Sohn (2013) 'Bring in the Nerds: The Importance of Technical Experts in Defeating SOPA and PIPA', pp. 133-139 in: D. Moon, P. Ruffini and D. Segal (eds.) *Hacking Politics. How Geeks, Progressives, the Tea Party, Gamers, Anarchists and Suits Teamed Up to Defeat SOPA and Save the Internet*, New York: OR Books.

Microsoft (2015) *Cybersecurity Norms. Advancing Persistent Security*. Microsoft Corporation.

Ministerie van Buitenlandse Zaken (2011) *Verantwoordelijk voor vrijheid. Mensenrechten in het buitenlands beleid*, The Hague, 5 april 2011.

Ministerie van Buitenlandse Zaken (2013) *Veilige wereld, veilige Nederland. Internationale veiligheidsstrategie,* The Hague, 21 juni 2013.

Ministerie van Defensie (2012) *Defensie Cyber Strategie*, The Hague, 27 juni 2012.

Ministerie van Defensie (2013) *In het belang van Nederland*, The Hague, 25 oktober 2013.

Ministerie van Economische Zaken, Landbouw en Innovatie (2011) *Digitale Agenda.nl. ICT voor innovatie en economische groei,* The Hague, 17 mei 2011.

Ministerie van Veiligheid en Justitie (2011) *De nationale cyber security strategie*, The Hague, 28 februari 2011.

Ministerie van Veiligheid en Justitie (2013a) *De nationale cyber security strategie 2. Van bewust naar bekwaam*, The Hague.

Ministerie van Veiligheid en Justitie (2013b) *Vrijheid en veiligheid in de digitale samenleving. Een agenda voor de toekomst*, The Hague.

Mueller, J. and M. Stewart (2014) 'Secret Without Reason and Costly Without Accomplishment: Questioning the National Security Agency's Metadata Program', *I/S: A Journal of Law and Policy for the Information Society*, 10 (2): 407-432.

Mueller, M. (2002) Ruling the Root. Internet Governance and the Taming of Cyberspace, Cambridge (Mass.): MIT Press.

Mueller, M. (2010) *Networks and states. The Global Politics of Internet Governance*, Cambridge (Mass.): MIT Press.

Mueller, M., A. Schmidt and B. Kuerbis (2013) 'Internet Security and Networked Governance in International Relations', *International Studies Review*, 15 (1): 86-104.

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.

NCTV (2014) *Tussen naïviteit en paranoia. Nationale veiligheidsbelangen bij buitenlandse overnames en investeringen in vitale sectoren.* Rapportage Werkgroep Economische Veiligheid, april 2014.

Nye, J. (2011) The future of power, New York: Public Affairs.

Nye, J. Jr. (2011) 'Nuclear Lessons for Cyber Security?', *Strategic Studies Quarterly*, 5 (4): 8-38.

OECD (2012) *OECD Internet Economy Outlook 2012*, Paris: OECD Publishing.

OECD (2014a) 'The Internet in Transition: The State of the Transition to IPv6 in Today's Internet and Measures to Support the Continued Use of IPv4', OECD Digital Economy Papers, No. 234, available at http://dx.doi.org/10.1787/5jz5sq5d7cq2-en.

OECD (2014b) *Measuring the Digital Economy: A New Perspective*, Paris: OECD Publishing.

Polatin-Reuben, D. and J. Wright (2014) 'An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet', Paper Presented at the 4th USENIX Workshop on Free and Open Communications on the Internet, August 18.

Poort, J. and J. Leenheer (2014) *Filesharing 2@12. Downloading from Illegal Sources in the Netherlands*, Tilburg: IViR.

Poort, J., J. Leenheer, J. van der Ham and C. Dumitru (2014) 'Baywatch: Two Approaches to Measure the Effects of Blocking Access to The Pirate Bay', *Telecommunications Policy*, http://dx.doi.org/10.1016/j.telpol.2013.12.008i.

Raymond, M. (2014) 'Puncturing the Myth of the Internet as a Commons', *The Georgetown Journal of International Affairs*. International Engagement on Cyber III. State Building on a New Frontier, 20: 53-64.

Renard, T. (2014) *The Rise of Cyber-diplomacy: the EU, Its Strategic Partners and Cyber-security,* European Strategic Partnerships Observatory, Working Paper 7, available at http://strategicpartnerships.eu/publications/the-rise-of-cyber-diplomacy-the-eu-its-strategic-partners-and-cyber-security.

Rid, T. and P. McBurney (2012) 'Cyber Weapons', *The RUSI Journal*, 157 (1): 6-13.

Rid, T. (2013) *Cyber War Will Not Take Place*, London: Hurst and Company.

Ruggie, J.G. (2007) 'Current Developments. Business and Human Rights: the Evolving International Agenda', *The American Journal of International Law*, 101 (4): 819-840.

Sanger, D. (2012) *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, New York: Broadway Books.

Scherer, A. and G. Palazzo (2011) 'The New Political Role of Business in a Globalized World: Review of a New Perspective on CSR and Its Implications for the Firm, Governance, and Democracy', *Journal of Management Studies*, 48 (4): 899-931.

Schmitt, M. (2013, ed.) *Talinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press.

Schneier, B. (2013) 'Power in Age of the Feudal Internet', pp. 10-14 in U. Gasser, R. Faris and R. Heacock (eds.) *Internet Monitor 2013: Reflections on the Digital World*, Cambridge (Mass.): The Berkman Center for Internet and Society.

Schneier, B. (2014) 'Should US Hackers Fix Cybersecurity Holes or Exploit Them?', *The Atlantic*, http://www.theatlantic.com/technology/archive/2014/05/should-hackers-fix-cybersecurity-holes-or-exploit-them/371197/, accessed 9 July 2014.

Sellars, A. (2014) 'SOPA lives: Copyright's Existing Power to Block Websites and 'Break the Internet'', pp. 36-39 in U. Gasser, J., Zittrain, R. Faris and R. Heacock Jomes (eds.) *Internet monitor 2014: Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse,* Cambridge (Mass.): The Berkman Center for Internet and Society at Harvard University.

Sénat Francaise (2014) Rapport d'information fait au nom de la mission commune d'information «Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet». Session extraordinaire de 2013-2014, 8 juillet 2014.

Severs, H. (2013) *The Cyber-industrial Complex: What Does the Militarisation of the 'Fifth Domain' Entail and What are the Consequences?*, http://theriskyshift.com/2013/03/the-cyber-industrial-complex-2, accessed 8 July 2014.

Singer, P. and A. Friedman (2014) *Cyber Security and Cyberwar. What Everyone Needs to Know*, Oxford: Oxford University Press.

Skierka, I., R. Morgus, M. Hohmann and T. Maurer (2015) *CSIRT Basics for Policymakers. The History, Typoes and Culture of Computer Security Incident Response Teams*. GPPi Working Paper, May 2015. Berlin: GPPi.

Stockton, P. and M. Golabek-Goldman (2013) 'Curbing the Market for Cyber Weapons', *Yale Law and Policy Review,* 32 (1): 101-128.

Swire, P. (2015) *The Declining Half-life of Secrets and the Future of Signals Intelligence*. New America Cyber Security Fellows Paper Series no. 1, July 2015. Washington: New America Foundation.

Taylor, L. and D. Broeders (2015) 'In the Name of Development: power, profit and the Datafication of the global South', *Geoforum*, vol. 64(4):229-237.

Went, R. (2010) *Internationale publieke goederen: Karakteristieken en typologie*, WRR webpublicatie 41, The Hague: WRR.

World Economic Forum (2014) *Global Risks 2014,* Ninth Edition, Insight Report, Geneva: World Economic Forum.

WRR (2003) *Waarden, normen en de last van het gedrag*, WRR rapporten aan de regering nr. 68, Amsterdam: Amsterdam University Press.

WRR (2010) *Minder pretentie, meer ambitie*, WRR rapporten aan de Regering nr. 84, Amsterdam: Amsterdam University Press.

WRR (2011) *Attached to the World. On the Anchoring and Strategy of Dutch Foreign Policy.* (Translation of *Aan het buitenland gehecht. Over verankering en strategie van Nederlands buitenlandbeleid*, WRR rapporten aan de regering nr. 85), Amsterdam: Amsterdam University Press.

Wu, T. (2010) 'Is Internet Exceptionalism Dead?', pp. 179-188 in B. Zsoka and A. Marcus (eds.) *The Next Digital Decade. Essays on the Future of the Internet*, Washington DC: Techfreedom.

Wu, T. (2011) *The Master Switch. The Rise and Fall of Information Empires*, New York: Vintage Books.

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 (forthcoming).

Yu, P.K. (2012) 'The Alphabet Soup of Transborder Intellectual Property Enforcement', *Legal Studies Research Paper Series.*

Ziewitz, M. and I. Brown (2014) 'A Prehistory of Internet Governance', pp. 3-26 in I. Brown (ed.) *Research Handbook on Governance of the Internet*, Cheltenham: Edward Elgar.

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 (ed.) *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge (Mass.): MIT Press.

Zittrain, J. (2008) *The Future of the Internet. And How to Stop It*, London: Penguin Books.
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.
Zuckerman, N. (2010) 'Intermediary Censorship', in: R. Deibert, J. Palfrey, R. Rohozinski and J. Zittrain (eds.) *Access Controlled. The Shaping of Power, Rights and Rule in Cyberspace*, Cambridge: MIT Press.

THE NETHERLANDS SCIENTIFIC COUNCIL FOR GOVERNMENT POLICY

The public core of the Internet

The growth and health of our digital economies and societies depend on the core protocols and infrastructure of the Internet. This technical and logical substructure of our digital existence is now in need of protection against unwarranted interference in order to sustain the growth and the integrity of the global Internet. The Internet's 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 'public core of the Internet' 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 core – its main protocols and infrastructure– should be considered a neutral zone, 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).**
- **To broaden the arena for cyber diplomacy to include new coalitions of states (including the so-called 'swing states') and private companies, including the large Internet companies as well as Internet intermediaries such as Internet Service Providers.**

Dennis Broeders is a senior research fellow at the Netherlands Scientific Council for Government Policy in The Hague and professor of Technology and Society at Erasmus University Rotterdam, the Netherlands.

ISBN 9789462981959

AUP.nl