# Cyberspace and governance - a primer

Klimburg, Alexander; Mirtl, Philipp

Österreichisches Institut für Internationale Politik
Austrian Institute for International Affairs

# Cyberspace and Governance—A Primer*

Alexander Klimburg
Philipp Mirtl

Working Paper 65 / September 2012

* This is the revised version of an oiip Special Issue first published September 2011.

# Contents

**About the Authors:**

Alexander Klimburg is Fellow and Senior Adviser at the oiip.

Philipp Mirtl is Fellow and Adviser at the oiip.

# 1. Abstract (English)

This working paper has a threefold purpose: first, it proposes a better understanding of the difference between the *Internet* (interconnecting computers) and the *World Wide Web* (managing information). Against this background, a four-layer model of cyberspace is presented including a physical, logical, informational, and social layer. Second, the paper splits the national cybersecurity debate in five distinct subject areas, or mandates. These include *Military Cyberactivities*, *Counter-Cybercrime*, *Intelligence and Counter-Intelligence*, *Critical Infrastructure Protection and National Crisis Management*, and *Cyberdiplomacy and Internet Governance*, each of which is typically covered by a distinct government department. Third, as one of the most understated and least understood mandates on this list, Internet Governance is described at more length in the final section.

# 2. Abstract (Deutsch)

Die Zielsetzung dieses Arbeitspapiers gliedert sich in drei Kernpunkte: Erstens wird versucht, den Unterschied zwischen dem *Internet* (Vernetzung von Computern) und dem *World Wide Web* (Informationsverwaltung) herauszuarbeiten. Vor diesem Hintergrund soll der Cyberspace als ein Vierschichtenmodell aufgespannt werden, das eine physische, logische, informationelle und soziale Schicht beinhaltet. Zweitens teilt dieses Papier die nationale Debatte zur Cybersicherheit in fünf unterschiedliche Themenbereiche, oder auch Mandate. Diese umfassen *Militärische Cyberaktivitäten*; *Bekämpfung von Cyberkriminalität*; *Nachrichtendienstliche Aktivitäten*; *Schutz Kritischer Infrastrukturen und Nationales Krisenmanagement*; sowie *Cyberdiplomatie und Internet Governance*. Im Allgemeinen kann jedes dieser fünf Mandate von unterschiedlichen Ministerien abgedeckt werden. Drittens soll in einem abschließenden Teil Internet Governance, als eines der am wenigsten beachteten Mandate in diesem Zusammenhang, ausführlicher betrachtet werden.

# 3. Grasping the Difference

*Cyberspace* is the “world behind your screen.”[1] However, when computers started talking to each other, this world started to expand. Historically, this process had already begun in 1969, when the *Universities of California* (UCLA) and *Stanford* (SRI)—the first two nodes of what would later come to be known as the *Internet*, or the Net—exchanged their first host-to-host message.[2]

## 3.1. The Net

The Internet has played a crucial role for the expansion of cyberspace. By using a combination of different data transmission mechanisms, such as the *Transmission Control Protocol* (TCP) and the *Internet Protocol* (IP) as the two most important protocols within the *Internet Protocol Suite,* an increasing number of computer users have been empowered by receiving unprecedented access to information.

Although the Internet is the most recent technology in a long series of communication technologies (such as telephone, teleprinters, or the radio), today internet technology is nearly all-encompassing. This is especially due to the fact that Information and Telecommunications Technology (ICT) is increasingly being dominated by the *Internet Protocol* (IP) as the main technical standard for communication between devices.[3] This can be attributed in a large part to bottom-up non-governmental stakeholders, such as the members of the *Internet Engineering Task Force* (IETF), who have developed many key software protocols and technical fixes that the Internet depends upon today.[4] This is why the development of internet standards can best be described as a self-regulatory process.[5]

[1] John Naughton, *A Brief History of the Future. The Origins of the Internet* (London: Phoenix, 1999). 311.
[2] See, for instance, Barry M. Leiner et al., “A Brief History of the Internet,” ISOC, http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet.
[3] Jovan Kurbalija, An Introduction to Internet Governance, (Genève: DiploFoundation, 2010), http://archive1.diplomacy.edu/poolbin.asp?IDPool=1060. 6.
[4] See, for instance, Paulina Borsook, “How Anarchy Works: On location with the masters of the metaverse, the Internet Engineering Task Force,” *Wired*, October 1995.
[5] OECD, “Working Party on Telecommunication and Information Services Policies. Internet Infrastructure Indicators (DSTI/ICCP/TISP(98)7/FINAL),” (Paris 1998).

Measured by regular surveys,[6] the number of global Internet users (defined as persons who have available access to an Internet connection point,[7] and the basic knowledge required to use web technology[8]) grew from 16 million in 1995 to more than 2.1 billion in 2011.[9] This is an astounding increase of around 13,000%. However, one should keep in mind that in 2011 more than ¾ of the world's Internet users came from Asia (44%), Europe (22.7%), and North America (13%).[10]

In general, an *internetwork*, or simply *internet* (with a lowercase "i"), evolves from interconnecting computer networks. These generic *networks of networks* can vary in size. The interconnection of two *Local Area Networks* (LANs), for instance, forms a smaller internet than two interconnected *Wide Area Networks* (WANs).[11] The *Internet* (with an uppercase "I"), however, is the unique "global network of computer networks."[12]

Internet capitalization conventions should not be overlooked in political discourse. For instance, when in 2006 the *International Telecommunication Union* (ITU) changed its policy in officially spelling out "internet" (with a lowercase "i"), US ambassador David A. Clark reacted disconcertedly, not knowing whether this would be of any concern for US interests.[13] In contrast, *The Economist* changed its editorial policy in 2003, arguing that the "internet" was no longer one particular network but has transformed to a generic technology comparable to the *telephone* or the *radio*.[14]

The Internet is essentially a collection of networks, and devices on these networks, which agree to communicate with each other. This communication depends on the

[6] See, for instance, UNSTATS, "UN Millennium Development Goals Indicators. The official United Nations site for the MDG Indicators," http://unstats.un.org/unsd/mdg/Metadata.aspx?IndicatorId=0&SeriesId=608.
[7] Internet connection points are usually provided by Internet service providers (ISPs) against payment.
[8] See Internet World Stats, "Surfing and Site Guide," http://www.internetworldstats.com/surfing.htm#1.
[9] See Internet World Stats, "Internet Growth Statistics," http://www.internetworldstats.com/emarketing.htm.
[10] See Internet World Stats, "Internet Users in the World. Distribution by World Region," http://www.internetworldstats.com/stats.htm; NewScientist, "Exploring the exploding Internet," http://www.newscientist.com/gallery/mg20227061900-exploring-the-exploding-internet/5.
[11] A LAN usually connects computers and devices within relatively limited areas (such as office buildings, universities or power plants), while a WAN covers a broader terrain (such as a city, region or even a state). Today, for instance, *Supervisory Control and Data Acquisition* systems (SCADA) increasingly monitor and control industrial production or infrastructure over IP-based LAN-WAN connections.
[12] Naughton, *A Brief History of the Future. The Origins of the Internet*: 314.
[13] Victoria Shannon, "What's in an 'i'? Internet governance," *New York Times*, 3 December 2006.
[14] See Kurbalija, *An Introduction to Internet Governance*. 6.

so-called *Internet Protocol* (IP).[15] Internet protocol numbers represent the most basic identifier on the Internet, which is why they are also referred to as an *IP address*. Every device connected to the Internet has its own IP address; if it does not have an IP address, it is not connected to the Internet.

An IP address is a complex string of values used to identify the physical location of a computer connected to the Internet (e.g., PCs, servers, smartphones). In the early 1980s, a total number of 4.3 billion (4.3x10^9) IP addresses (referred to as *IPv4*)[16] were considered to be enough for the foreseeable future.[17] However, the explosive demand for IP address blocks over the last thirty years, as well as the vision of an *Internet of Things* (IoT), in which everyday objects (such as home appliances or clothing) are made accessible over the Internet, have proven the original quantity of IP addresses allotted was, in fact, inadequate.

In the 1990s, therefore, IP version 6 (referred to as *IPv6*)[18] was developed. IPv6 would provide enough address space for around 340 undecillion (a trillion, trillion, trillion, or 3.4x10^38) Internet connection points. With an estimated world population of 6.8 billion living human beings,[19] the potential number of IPv6 addresses would enable each individual to connect around 1.2 billion devices to the Net; or, to elucidate these numbers in a more comprehensible analogy, "if all the IPv4 addresses could fit within a Blackberry, it would take something the size of Earth to contain IPv6."[20]

IPv4 reached its "depletion date" in the spring-summer of 2011,[21] which made the shift to IPv6 a necessity. With IP addresses, not a restricted commodity anymore, this

[15] Sometimes also written as TCP/IP.

[16] For a better overview, IPv4 addresses are usually not displayed in a long line of zeros and ones, but in four groups of decimal numbers, separated by dots and ranging from 0 to 255 (e.g., 208.80.152.2).

[17] See, for instance, ICANN, "To 4,294,967,296 and Beyond – Under 10% of IPv4 Space Remains: Adoption of IPv6 Is Essential," http://www.icann.org/en/announcements/announcement-29jan10-en.htm.

[18] Similar to IPv4 addresses, IPv6 addresses are usually not written in long lines of zeros and ones, but in eight groups of four-digit, case insensitive hexadecimal values (0-9 and A-F/a-f), separated by colons (e.g., 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A).

[19] World Bank, "World Development Indicators 2011," http://databank.worldbank.org/ddp/home.do?Step=12&id=4&CNO=2.

[20] ICANN, "IPv6 Factsheet," http://www.icann.org/en/announcements/announcement-26oct07.htm. 3.

[21] There are different dates depending on what regions of the world "exhausted" their stock of IPv4 addresses. Indeed, the United States government is said to hold a very large amount of unassigned IPv4 addresses "in reserve", so in some cases it can be said there has not yet been a true exhaustion of all IPv4 addresses.

will allow the true IoT to occur, meaning literally all of human possessions (now, and for the foreseeable future) could potentially be “tagged” and made accessible over the Internet. The new Internet is therefore just beginning.

## 3.2. The Web

As one of the most important applications on the Net, the *World Wide Web* played a crucial role in the expansion of cyberspace. It was developed between 1989 and 1990 by British software engineer Tim Berners-Lee while working at the *European Centre for Nuclear Research* (CERN). What initially started as a project to aid CERN physicists navigate a wealth of information was eventually released to the wider public in 1991.[22] However, the Web only had its breakthrough in 1993, when Mosaic—the first major graphics supporting browser—entered the market.[23]

In order to guarantee both a uniform language in which information could be presented on websites, and a functioning device by which this information could be transferred and identified safely, Berners-Lee had to invent the *Hypertext Markup Language* (HTML), as well as the *Hypertext Transfer Protocol* (HTTP), and the *Uniform Resource Locator* (URL). Today, the standards for the Web are developed by a non-governmental *World Wide Web Consortium* (W3C) established in 1994.

In August 2011, there were more than 463 million websites (including subpages) with domain names and content on the Net.[24] Compared to just 18,000 in August 1995,[25] this is a total increase of more than 2.5 million percent over the last 16 years. However, a significant share of this increase was only generated over the last two years.[26]

As regards web server software, since May 1996, the open-source *Apache HTTP Server* software, developed by an open community under the auspices of the non-profit *Apache Software Foundation*, has been the most popular HTTP server software

[22] CERN, “The website of the world’s first-ever web server,” http://info.cern.ch/.
[23] W3C, “A Little History of the World Wide Web. From 1945-1995,” http://www.w3.org/History.html.
[24] Netcraft, “August 2011 Web Server Survey,” http://news.netcraft.com/archives/2011/08/05/august-2011-web-server-survey-3.html.
[25] Marsha Walton, “Web reaches new milestone: 100 million sites,” *CNN.com*, 1 November 2006.
[26] Netcraft, “August 2011 Web Server Survey”.

in use. As of August 2011 Apache was estimated to serve 65.18% of all websites, followed by *Microsoft Internet Information Services* (IIS) with 15.86%, the Russian *nginx* with 7.67%, and *Google Web Server* with 3.68%.[27]

The *Web* and the *Net* have always been inseparable. This often leads to the misconception that these two terms can be used interchangeably. However, the Web is just one of many different applications "on" the Net. The Net's structure can be visualized by looking at the layered network architecture model called the *Internet Protocol Suite*.[28] Here, for instance, the Internet Protocol (IP) lies on the *Internet Layer*, the Transmission Control Protocol (TCP) on the overlying *Transport Layer*, and the Hypertext Transfer Protocol (HTTP) on the top, which is called *Application Layer*. A similar organization can be observed in the *Open Systems Interconnection Model* (also referred to as the *OSI model*).[29] All this means Web services can only be used properly if the underlying services (e.g., TCP/IP) work correctly.

In this context, the Net's overall idea is to *interconnect computers* in a global network of computer networks, while, building upon this interconnection, the Web's essential aim is to *manage information* in a global Web of human-readable documents that can be defined as "content supplied in response to a request."[30]

This emphasize on content (or information) becomes obvious when looking at different definitions for the Web. For instance, on the world's first-ever website Berners-Lee characterized the Web as "a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents."[31] Elsewhere, the Web was also referred to as a "hypermedia system linking text, graphics, sound and video on computers distributed all over the world."[32]

[27] Ibid.

[28] IETF RFC 1122, "Requirements for Internet Hosts – Communication Layers," October 1989, http://tools.ietf.org/html/rfc1122.

[29] ISO/IEC 7498-1:1994, "Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model."

[30] W3C, "W3C Glossary/Dictionary," http://www.w3.org/2003/glossary/alpha/D/80.

[31] W3C, "World Wide Web," http://www.w3.org/History/19921103-hypertext/hypertext/WWW/TheProject.html.

[32] Naughton, *A Brief History of the Future. The Origins of the Internet*: 319.

## 3.3. Cyberspace—A Four Layer Model

In the introduction to this section, cyberspace has been referred to as the *world behind your screen*. However, since the 1960s, this world's horizons have expanded considerably. This is due, in no small part, to internet technologies developed by a self-regulated, non-governmental community.

While differentiating the *Internet* (interconnecting computers) from the *World Wide Web* (managing information), the aim of the previous two subsections was to provide a better understanding of their contribution to the expansion of cyberspace. The aim of this section, however, is to define cyberspace as a somewhat wider framework, in which the Net plays an essential, albeit not exclusive, role.

Over the last years, the term *cyberspace* has gained considerable attention. Science fiction author William Gibson is credited with first mentioning it in his short story *Burning Chrome* (1982).[33] Two years later, in his famous 1984 cyberpunk novel called *Neuromancer*, the author described Cyberspace as a "consensual hallucination."[34]

Years later Gibson labeled the term an "effective buzzword" that seemed "evocative and essentially meaningless" when it first emerged on his pages.[35] However, today *cyberspace* is not only popular among different strands of cyberpunks or computer enthusiasts. Moreover, it has made its way into a variety of disciplines of which political science is just one.

In contrast to land, sea, air and space, cyberspace is a human construct with components that can change over time. Today, a wide variety of distinct definitions of cyberspace have been proposed.[36] One of which was first used in the aftermath of 9/11, when the 2003 *US National Strategy to Secure Cyberspace* described cyberspace as a national "nervous system" which controls the country's critical infrastructure. While highlighting the role of public-private engagement, the strategy stated:

[33] William Gibson, "Burning Chrome [1982]," in *Burning Chrome* (New York: HarperCollins Publishers Inc., 2003).

[34] William Gibson, *Neuromancer*  (New York: Ace Books, 2000 [1984]). 67.

[35] Scott Thill, "March 17, 1948: William Gibson, Father of Cyberspace," *Wired*, 17 March 2009.

[36] For a first overview see Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin Kramer et al. (Washington, DC: National Defense UP, 2009), 26-7.

> "Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security."[37]

Five years later, in 2008, a similar definition was put forward in US President George W. Bush's *National Security Presidential Directive 54*, also known as *Homeland Security Presidential Directive 23* (NSPD-54/HSPD-23).[38] This document established the *Comprehensive National Cybersecurity Initiative* (CNCI),[39] a partially classified USD 17 billion program designed to protect Federal Government systems against intrusion attempts.[40] In this context, the directive defines cyberspace as

> "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people."[41]

Under the Obama administration, this definition has been adopted by the 2009 *60-Day Cyberspace Policy Review*.[42]

Nonetheless, there is still no standard, universally accepted definition for cyberspace, and for this reason, it is useful to think about ways how to approach the concept comprehensively. One way to do so is to conceptualize cyberspace in terms of multiple interdependent layers of activities. There are varied conceptualizations of the different numbers and names of layers present in current academic discourse.[43] How-

[37] White House, "The National Strategy to Secure Cyberspace," (Washington, DC: White House, 2003).

[38] *National Security Presidential Directive 54: Cyber Security and Monitoring (NSPD-54) / Homeland Security Presidential Directive 23: Cyber Security and Monitoring (HSPD-23)*.

[39] White House, "The Comprehensive National Cybersecurity Initiative," (Washington, DC: White House, 2008).

[40] Victoria Samson, "The Murky Waters of the White House's Cybersecurity Plan," *Center for Defense Information*, 23 July 2008.

[41] Public Safety and Homeland Security Bureau, "Tech Topic 20: Cyber Security and Communications," FCC, http://transition.fcc.gov/pshs/techtopics/techtopics20.html.

[42] White House, "Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure," (Washington, DC: White House, 2009).

[43] See, for instance, Martin C. Libicki, *Conquest in Cyberspace. National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007). Chapter 10.; and Franklin D. Kramer, Stuart

ever, this paper argues in favor of the following four-layer model of cyberspace:[44]

1. **The physical layer** contains all the *hardware devices,* which include routers, switches, storage media, satellites, sensors, and other technical conduits, both wired and wireless. The physical infrastructure can be located geographically in "real space" and is thus subject to different national jurisdictions. If it were removed, the overlying layers would disappear as well, as happened in 2011 in Armenia, where reported 90% of all Internet services crashed due to a retired 75-year-old woman who single-handedly sliced through an underground fiber optic cable with her spade.[45]
2. **The logical layer** generally refers to the *code*, which includes both the software and the protocols incorporated within that software.[46] Generally speaking, a protocol defines the rules or conventions necessary to obtain a certain goal (e.g., communication). Formalizing a protocol makes it a standard. Software, in contrast, is the computer program that implements these protocols. In this respect, protocols "are not considered to be satisfactory standards until interoperable independent implementations [within different computer programs] have been demonstrated. (This is the embodiment of the "running code" slogan.)"[47] Networking protocols are commonly segmented by their function, and how close (or how far) away they work from the "end user"—the average computer user. In the most common of segmentation, known as the *OSI Model*, basic everyday client-side applications (such as Windows Internet Explorer) operate at the top of the model (level 7), while the aforementioned TCP works on Level 4 (the Transport layer) and IP works on Level 3 (the Internet layer). Built upon the Web, for instance, more complex applications often combine certain aspects of services, which can be eventually combined and applied by other applications on even higher levels. This flexibility presents inexhaustible

H. Starr, and Larry Wentz, eds., *Cyber Power and National Security* (Washington, DC: National Defence UP, 2009), Chapter 2.

[44] See David Clark, "Characterizing cyberspace: past, present and future," *MIT/CSAIL Working Paper*, 12 March 2010.

[45] Tom Parfitt, "Georgian woman cuts off web access to whole of Armenia," *The Guardian*, 6 April 2011.

[46] See, for instance, Lawrence Lessig, The Future of Ideas. The Fate of the Commons in a Connected World, (New York: Random House, 2001), http://www.the-future-of-ideas.com/download/lessig_FOI.pdf. 23.; and Lawrence Lessig, Code, (New York: Basic Books, 2006), http://codev2.cc/download+remix/Lessig-Codev2.pdf.

[47] IETF RFC 4677, "The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force," September 2006, http://tools.ietf.org/html/rfc4677.

possibilities to create new services, which, today, include search engines, Weblog, social networking sites, podcasts, Internet telephony, Web mapping, etc. Yet, this abundance of capabilities also has a dark side: *malware*. Essentially, *malware* (also *malicious logic*) includes a variety of different *Trojans*, *viruses* and *worms*.[48] Similar to "benign" services, more complex malware often combines certain aspects of existing logic (software code).[49] In the past, one of the first major logic incidents occurred in 1982 when the CIA purportedly corrupted the software of a Soviet gas pipeline computer control system which was said to result in "the most monumental non-nuclear explosion and fire ever seen from space."[50] Other threats include attacks on the basic infrastructure of the Net itself, for instance the *Domain Name System* (DNS). In April 2010, for example, a Chinese ISP introduced the wrong information into their routing tables. This caused around 10% of the Internet traffic (theoretically) routed to be mapped through China.[51] DNS spoofing is usually conducted by intentionally corrupting the information in the Internet routing tables, so that users, who are passed from one router to the other, have to traverse a certain target network. Potential consequences could have been dire, as, for instance, all webpages (e.g. for a bank or webmail service) could have been successfully faked and therefore all login details could have been compromised. However, this very case was reported to be "probably unintentional."[52]

3. **The content layer** describes all the *information* created, captured, stored and processed within cyberspace. Information is defined as "knowledge concerning objects, such as facts, events, things, processes, or ideas".[53] It contains all human-readable messages delivered by social media Websites or email; content of articles and books kept on memory sticks and virtual databases; news broadcasted via blogs and Websites; and music, movies and pictures consumed online. However, access to information can also be systematically lim-

[48] Vangie Beal, "The Difference Between a Computer Virus, Worm and Trojan Horse," *Webopedia*, 29 June 2011.

[49] Alexander Klimburg and Heli Tirmaa-Klaar, Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU, (Brussels: European Parliament, 2011), http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/EP_Study_FINAL.pdf. 48.

[50] Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War* (New York: Random House Publishing Group, 2004). 269.

[51] The difference here is between theoretical and actual route propogation – in fact while 10% of the Internet traffic could have gone through China, only a small fraction of it actually did.

[52] See Robert McMillan, "A Chinese ISP Momentarily Hijacks the Internet," *PCWorld*, 8 April 2010.

[53] ISO/IEC 2382-1:1993, "Information technology – Vocabulary – Part 1: Fundamental terms."

ited. Blocking or removing online content from the Web happens for reasons such as protecting intellectual property rights, securing national order or social identity. In fact, in recent years, online censorship and content restrictions have risen rapidly as demonstrated by the *OpenNet Initiative*.[54] Moreover, information may take a more abstract form; if computers, for instance, direct connected printers on how to print a certain document, it is done by using printer control strings. These can be considered to be informational in form but logical in purpose.[55] The content layer is the focus of the very wide-ranging data protection debate and encompasses issues such as to what extent even "anonymous" information can be extracted from analyzing user behavior. This contextual setting is also why the content layer is sometimes referred to as a semantic layer.

4. **The social layer** is made up of all the *people* using and shaping the character of cyberspace. It is the actual Internet of people and potential relationships, rather than the implied Internet of hardware and software. Essentially, the social layer includes governments as well as private sector, civil society and technical community actors. However, all share a specific characteristic: while in "real" life (*extra cyberspace*) people can ultimately be identified by their unique DNA code, attribution is much more difficult on the Net (*intra cyberspace*). In contrast to the "meat" world, individuals in cyberspace facilitates establishment of multiple identities for the user. And alternatively, one single virtual identity can have multiple human users (e.g., the same NYT online office account being used by different employees). This has not only important implications in terms of security or copyright protection but also raises interesting questions about how the cyber world plays into the real world. In reference to last year's revolutions in Tunisia and Egypt, for instance, it has been argued that the exchange via Facebook played an important role in giving birth to "a pan-Arab youth movement dedicated to spreading democracy in a region without it."[56] The protests in Tunisia, Egypt, Libya, Yemen, and Syria have even been characterized as a "'global political awaking'—a movement for change that is

[54] See http://opennet.net/.

[55] Martin C. Libicki, *Cyberdeterrance and Cyberwar* (Pittsburgh: RAND Corporation, 2009). 12.

[56] David D. Kirkpatrick and David E. Sanger, "A Tunisian-Egyptian Link That Shook Arab History," *New York Times*, 13 February 2011.

> enabled and accelerated by modern technology'."[57]

This way of thinking about cyberspace does not deliver a single best definition. Rather, it tries to make the concept more accessible. In fact, for a comprehensive understanding, all four layers must be considered equally. Cyberthreats, for instance, might arise at the physical layer (destruction of wires) as well as on the logical (malicious software), informational (compromising information), or social layer (corrupting people). In the end, however, all cyberattacks ultimately seek to influence the "social layer".

[57] David Ignatius, "What Happens When the Arab Spring Turns to Summer?," *Foreign Policy*, 22 April 2011.

# 4. The Five Mandates of National Cybersecurity

Within the general context of discussing "national cybersecurity," it is very important to keep in mind that this is not *one* single subject area; rather, it is possible to split the issue of national cybersecurity into five distinct perspectives or "mandates", each of them usually covered by different government departments, and this is not an ideal state. Unfortunately, there is frequently a significant lack of coordination between these organisations, and this lack of coordination is perhaps one of the most serious organisational challenges within the domain of national cybersecurity.

Furthermore, overlap between themes and ambiguity is the rule, not the exception, in cybersecurity. The physical reality of national cybersecurity is that all these topics are largely overlapping. However, the bureaucratic reality, as lived in nearly all national governments, is that these subject areas are kept separate from each other in distinct "mandates". Each mandate has developed its own emphasis and even its own lexicon, despite the fact that they are all simply different facets of the same problem.

1. **Military Cyberactivities:** The term "cyberwar" is being used in a number of inappropriate or misleading contexts (for instance, when referring to cyber-espionage). Therefore, it is true to say "cyberwarfare is a loaded term".[58] Consequently, this mandate has been entitled "military cyberactivities" and encompasses a range of actions (both *offensive* and *defensive*) sometimes also covered by non-military organisations (such as the intelligence community). From an academic point of view, however, the term "cyberwar" is useful to distinguish it from all other cyberattacks, in particular ones using sophisticated cyberweapons.[59] The Internet security company McAfee has warned since 2007 that, in its opinion, a "virtual arms race" is occurring in cyberspace with a number of countries deploying cyberweapons.[60] Many governments are building capabilities to wage cyberwar,[61] while some NATO reports have claimed

[58] See William Jackson, "How can we be at cyberwar if we don't know what it is?," *Washington Technology*, 22 March 2010.

[59] The term "cyberweapons" is equally contentious, as it can range from an email program to something like Stuxnet. In this context, a "cyberweapon" is understood not to be an "attack-kit" (i.e., a program decided to produce a "cyberweapon") but a finished product.

[60] See Zeenews, "US, China, Russia have 'cyber weapons': McAfee," *Zeenews.com*, 18 November 2009.

[61] See, Michael W. Cheek, "What is Cyber War Anyway? A Conversation with Jeff Carr, Author of 'Inside Cyber Warfare'," *The new new Internet*, 2 March 2010.

that up to 120 countries are developing a military cybercapability.[62] These capabilities can be interpreted as simply one more tool of warfare, similar to airpower, which would be used only within a clearly defined tactical military mission (for instance, for shutting down an air-defence system). This is called here "battlefield cyberwarfare," and the effects are limited to the operational-tactical environment. Alternatively, the emphasis can lie on "strategic cyberwarfare"—the ability to strike at the heart of an (advanced) nation by undermining its economy and its basic ability to function. There is no legal definition of cyberwar, although since 2010 there has been an increasing international understanding on two key issues regarding cyberwar: first, that the Laws of Armed Conflict apply also in cyberspace and, second, that a "cyberwar attack" is said to have occurred if "the level of damage is approximate to a physical attack."[63] Military Cyberactivities, therefore, encompass three different mandates: enabling *Network Centric Warfare* (NCW) capabilities, *Battlefield Cyberwarfare*, and Strategic Cyberwarfare.

2. **Counter-Cybercrime**: Cybercrime is increasingly considered the most advanced and profitable of all criminal enterprises. Estimates of the cost of cybercrime to business range as high as 1 *trillion* dollars for 2009,[64] and by some estimates it has long since overtaken the drug trade in terms of business volume.[65] Cybercrime activities can include a wide swath of activities that impact both the individual citizen directly (e.g., identity theft) and corporations (e.g., the theft of intellectual property). At least as significant for national security, however, is the logistical support capability cybercrime can offer to anyone interested in conducting cyberattacks. This includes hosting services, the sale of stolen identities and credit card numbers, money-laundering services,[66] and even the provision of entire hacking tools and attack-kits to enable large-scale

[62] See Julian Hale, "NATO Official: Cyber Attack Systems Proliferating," *DefenceNews*, 23 March 2010.

[63] This was agreed at the 'Cyber 15' deliberations conducted at the UN in the summer of 2010.

[64] See Elinor Mills, "Study: Cybercrime cost firms $1 trillion globally," *CNET News*, 28 January 2009.

[65] See John Leyden, "Cybercrime 'More Lucrative' than Drugs. At least phishing fraudsters don't have Uzis," *The Register* 2005. These numbers have increasingly been called into question, and studies from 2011 and 2012 have provided much lower estimates – which have proven to be equally contentious.

[66] See Jeremy Kirk, "5 Indicted in Long-running Cybercrime Operation," *CSO Online*, 2 September 2009.

cyber-campaigns.[67] There are convincing indications that Russian cybercrime syndicates played a role in the cyberattacks on Georgia and Estonia,[68] to name but two examples. This is also where cybercrime interacts not only with military cyberactivities, but also with cyberterrorism. Cyberterrorism is a highly contentious term. There is a prevalent concern the term could be used to severely criminalize not only "minor acts of cybercrime" (often called *hacktivisim*), but also any type of online expression critical of a government. These concerns are largely overplayed, as there is a relatively clear acceptance that the difference between all forms of "crime" is the effect—a minor nuisance is certainly not an act of terrorism. Cyberterrorism is considered to be an act of terrorism solely carried out with "cyber" means and the destruction from which rises to the level of a conventional terrorist attack. As of 2012, there has not been anything approaching the classification of a "cyberterrorist" attack, despite, for instance, threats by the hacker group *Anonymous* to "bring down the Internet."[69] This said, there have been a rising number of criminal acts, including attempts at mass disruption of communications, and this suggests cyberterrorism will be an issue for the future.

3. **Intelligence and Counter-intelligence**: Distinguishing cyberespionage from cybercrime and military cyberactivities is not uncontroversial. In fact, they all depend on similar vectors of attack and similar technology. In practice, however, serious espionage cases (both regarding intellectual property as well as government secrets) are a class of their own, while at the same time it can be very difficult to ascertain for sure if the perpetrator is a nation-state or a criminal-group operating on behalf of a nation-state, or indeed operating on its own. Whoever is actually behind the attack, cyberespionage probably represents the most damaging part of cybercrime (if included in the category). Lost intellectual property, for instance, was said to have cost the British economy in 2011 UKP 9.2 billion a year.[70] Cyberespionage, when directed toward states,

[67] For an early mention of this see BBC, "Cyber crime tool kits go on sale," *BBC News Online*, 4 September 2009.

[68] See Jeff Carr et al., "Phase I Report: Russia/Georgia Cyber War – Findings and Analysis," *Project Grey Goose*, 17 October 2008.; Jeff Carr et al., "Project Grey Goose Phase II Report: The evolving state of cyber warfare," *Project Grey Groose*, 20 March 2009.; and US Cyber Consequences Unit, "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008," *US-CCU Special Report*, August 2009.

[69] Tyler Holman, "Anonymous threatens to bring down the internet," *Neowin.net*, 27 March 2012.

[70] Michael Holden, "Cyber crime costs UK $43.5 billion a year: study," *Reuters*, 17 February 2011.

also makes it necessary to develop specific foreign policy response mechanisms capable of dealing with the inherent ambiguity of actor-nature in cyberspace. At the same time, counter-intelligence activities (i.e., detecting and combating the most sophisticated cyberintrusions) very often will depend upon other types of intelligence activity, including offensive intelligence collection but also extensive information sharing between international partners.

4. **Critical Infrastructure Protection and National Crisis Management**: *Critical Infrastructure Protection* (CIP) has become the catch-all term that seeks to involve the providers of essential services of a country within a national security framework. As most of the service providers (such as public utilities, finance, or telecommunications) are in the private sector, it is necessary to extend some sort of government support to help protect them and the essential services they provide from modern threats. While the original focus of these programs was often terrorism, today the majority of all CIP activity is directly connected to cyber—usually cybercrime and cyberespionage. In this context, *National Crisis Management* must be extended by an additional cyber component. This includes institutional structures which enhance the cooperation between state and non-state actors both nationally and internationally, as well as a stable crisis communication network and an applicable legal framework to exchange relevant information.[71]
5. **Cyberdiplomacy and Internet Governance**: Claiming that the “pursuit of classical diplomacy will no longer suffice,” in 2002 Evan H. Potter suggested that *cyber*diplomacy was about “how diplomacy is adapting to the new global information order.”[72] Taking the information revolution as point of departure, Potter claimed that information technology was the “primary mover”[73] behind this change. However, more recent accounts dealing with the impact of information technology on the overall conduct of diplomacy seem to avoid any reference to the term cyberdiplomacy.[74] Interestingly, in a 2010 paper cyber-

[71] See, for instance, Austrian Federal Chancellery, “National ICT Security Strategy Austria,” (Vienna: Digital Austria, 2012), 14-5.

[72] Evan H. Potter, ed. *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century* (Quebec: McGill-Queen’s University Press, 2002), 7.

[73] Ibid.

[74] See, for instance, Joseph S. Nye, *The Future of Power* (New York: PublicAffairs, 2011). 100-9.; Keith Hamilton and Richard Langhorne, *The Practice of Diplomacy. Its evolution, theory and administration.* (New York: Routledge, 2011). 229-54.; and Philip Seib, *Real-Time Diplomacy. Politics and Power in the Social Media Era* (New York: Palgrave Macmillan, 2012).

> diplomacy has even been alternatively defined as being "about managing a world that is not just borderless but can function best when connectivity is almost seamless."[75] The paper was prepared in response to bilateral efforts between the US and Russia in fostering their cooperation on cybersecurity in 2009. Conveniently, this definition also applies to multilateral efforts to promote norms and standards for cyber behavior in fora such as the United Nations, or processes intended to establish "cyber confidence building measures" similar to those which have been initiated by the *Organization for Security and Co-operation in Europe* (OSCE) in 2012. In this context, cyberdiplomacy becomes similar to other diplomatic efforts on topics such as arms control and counter-proliferation. Internet Governance, in contrast, is largely a multi-stakeholder activity, and probably the most international of all mandates. It is generally referred to as the process by which a number of state and non-state actors interact to manage what, in effect, is the logical layer of cyberspace. As one of the most understated and least understood aspects of national cybersecurity, it is described at more length below. Internet Governance, in contrast, is largely a multi-stakeholder activity, and is probably the most international of all mandates.

As said in the introduction to this chapter, the reality of these different mandates is that they are each dealt with by different organizational groups not only within government, but also within the non-state sector. This is not a positive development. Normatively speaking, all of these mandates need to be holistically engaged, with overall coordination, if one is to develop a comprehensive national cybersecurity perspective. However, developing this "comprehensive" view is often a luxury most practitioners of cybersecurity can simply not afford due to resource restraints. The reality is each of these mandates has developed its own specialized terms, priorities, and even basic principles and it is unusual to interact with more than one other mandate. The "silofication" of national cybersecurity is, therefore, not a challenge for government departments, but indeed overall for the field as a whole.

[75] Franz-Stefan Gady and Greg Austin, Russia, The United States, and Cyber Diplomacy. Opening the Doors, (New York: EastWest Institute, 2010), http://www.ewi.info/system/files/USRussiaCyber_WEB.pdf. 16.

# 5. Cybersecurity in Internet Governance

Cyberspace only exists within parameters constructed and regulated by human beings. These parameters have, until now, not been created directly by governments, but have rather arisen from the "bottom-up" in a process that is often referred to as the self-regulation of the Internet.[76] The process is often transcribed as "Internet governance", which has been defined as "the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."[77]

The Internet is a relatively new environment for human activities, and it was created with other purposes in mind than that for which it is now used. The basic Internet was never intended to be "secure"; security was always more of an afterthought than an original design feature.[78] In essence, the DNA of the Internet was to be a "trusting, open" system. It did not appear feasible twenty years ago that not only would critical infrastructures partially come to depend on the Internet, but the Internet itself would be, at least in part, considered critical for everyday societal needs.

The debate related to Internet governance issues dates at least back to the early 1990s, when the *Harvard Information Infrastructure Project* (HIIP)[79] brought together experts from government, industry, and academia to elaborate on emerging policy issues related to the development, use and growth of the global information infrastructure (most notably the Internet).[80] The HIIP was intended to serve as an interdisciplinary forum for economists, lawyers, political scientists and technologists, and culminated in a series of different publications. Their basic assumption was that the Internet had an unprecedented impact on our existing world order. As HIIP key researcher Brian Kahin and Charles Nesson put it:

[76] See, for instance, Peng Hwa Ang, "Self Regulation after WGIG," ed. William J. Drake, *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance* (New York: United Nations ICT Task Force, 2005), http://www.wgig.org/docs/book/toc2.html.

[77] WGIG, "Report from the Working Group on Internet Governance (WSIS-II/PC-3/DOC/05)," (Geneva: ITU, 2005), 3.

[78] See, for instance, Jeanette Hofman, "The Libertarian Origins of Cybercrime: Unintended Side-Effects of a Political Utopia," *CARR Discussion Paper*, April 2010.

[79] See http://ksgnotes1.harvard.edu/IIP/HIIP_PG.nsf.

[80] Thanks to Prof. Wolfgang Kleinwächter for this point.

> "Our experience of geographic space has been transformed by the information revolution, as it was by the railroad and air travel. But the transformation now underway on the Internet is not only greater and qualitatively different. It has collapsed the world, transcending and blurring political boundaries in the process. It gives individuals instant, affordable access to other individuals, wherever they may be, and it enables each to publish to the world."[81]

However, transcending national borders does not simultaneously imply the dissolution of the state. With physical power over people and infrastructure, states will remain important actors. What is clearly changing is the way this power is exercised. In an environment where the (trans-border) interaction between people can hardly be confined to the sole jurisdiction of a single state-actor, overlapping responsibilities will make it necessary for governments to collaborate with the private sector and with civil society actors.[82]

In the course of the 1990s, the rather academic debates over Internet governance reached a broader public. When it became clear that the global DNS was not only a single point of technical failure, but also a single point for policy decisions about surveillance and control of access to cyberspace, questions about the difference between technical management on the one hand, and regulatory control on the other were posed. For instance, was the decision to enter a TLD into the root zone file a mere technical issue or is it a public policy issue? For Milton Mueller, "[t]he uncomfortable fact is that the two meanings of 'Internet governance' are inseparably linked."[83]

Increasingly, state actors became aware they did not really understand the concrete subject matter of Internet governance. Therefore, in the final document to the 2003 *United Nation's* (UN) *World Summit on the Information Society* (WSIS-I), "the representatives of the peoples of the world"[84] called for setting up a collaborative *Working Group on Internet Governance* (WGIG). The WGIG should be composed of states as

[81] Brian Kahin and Charles Nesson, eds., *Borders in Cyberspace: Information Policy and the Global Information Infrastructure* (Cambridge, MA: MIT Press, 1997).
[82] See Joel R. Reidenberg, "Governing Networks and Rule-Making in Cyberspace," in *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, ed. Brian Kahin and Charles Nesson (Cambridge, MA: MIT Press, 1997).
[83] Milton Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace,* (Cambridge, MA: MIT Press 2002). 10.
[84] WSIS, "Geneva Declaration of Principles (WSIS-03/GENEVA/DOC/0004)," (Geneva: ITU, 2003).

well as the private sector and civil society actors. It had the aim to "investigate and make proposals for action, as appropriate, on the governance of [the] Internet by 2005."[85] After four meetings and with full and active participation of multiple stakeholders, including governments (44%), the private sector (28%) and non-governmental actors (28%) from both developing (59%) and developed countries (41%)[86]—the WGIG delivered a report[87] (and an accompanying background report[88]) which served as input for the 2005 WSIS in Tunis (WSIS-II).[89] The main recommendation of the WGIG was the creation of a forum which

> "could address [. . .] issues, that are cross-cutting and multidimensional and that either affect more than one institution, are not dealt with by any institution, or are not addressed in a coordinated manner."[90]

This recommendation fundamentally inspired WSIS-II and led to the creation of a multi-stakeholder *Internet Governance Forum* (IGF), which should "identify emerging issues, bring them to the attention of the relevant bodies and the general public, and, where appropriate, make recommendations."[91]

However, WGIG did not only recommend the creation of an Internet-related forum, but also provided a working definition of *Internet governance* eventually adopted by WSIS-II. By clearly reflecting the multi-stakeholder nature behind WGIG and the IGF the definition reads as follows:

> "Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."[92]

This definition is intentionally broad in scope and touches upon a myriad of different

[85] Ibid., para. 50.
[86] John Mathiason, *Internet Governance. The new frontier of global institutions* (New York, NY: Routledge, 2009). 118.
[87] WGIG, "Report from the Working Group on Internet Governance (WSIS-II/PC-3/DOC/05)," 3.
[88] WGIG, Background Report, (Geneva: WGIG, 2005), http://www.wgig.org/docs/BackgroundReport.doc.
[89] For the website of WSIS-II, see: http://www.itu.int/wsis/tunis/index.html.
[90] WGIG, "Report from the Working Group on Internet Governance (WSIS-II/PC-3/DOC/05)," 10f.
[91] WSIS, "Tunis Agenda for the Information Society (WSIS-05/TUNIS/DOC/6(Rev. 1)-E)," (Tunis: ITU, 2005), para. 72-82.
[92] Ibid., para. 34.

issue areas[93] and actors. This is also why, in Internet governance, one cannot speak of one single Internet governance regime, but of multiple regimes (including the DNS regime, intellectual property regime, etc.).[94] The key issue here is that these regimes are of highly diverse and sometimes contradicting nature—the interests of human rights and intellectual property, for instance, are not always aligned—but also need to be set in both policy and technical contexts. Both these larger contexts are themselves largely in flux, depending on current political affairs or the state of the technological evolution.

Internet governance can therefore be considered not only a young, highly dynamic but also an essentially reactive policy field that seeks to reconcile the technical and policy heritage of the Internet with its ever-growing modern-day importance. Governments as a whole have been relative latecomers to Internet governance, despite its obvious political importance. The EU has considerable potential to play a formative role in evolving Internet governance, and help promote the development of a more secure Internet.

## 5.1. Technical Internet Governance: *Ad Hoc*

Internet governance can be subdivided into two domains: the *technical domain* and the *policy domain*. The technical domain predominantly consists of volunteers and civil society, and it can be described as completely “ad hoc”. One of the most important organizations is the *Internet Engineering Task Force* (IETF), which has, since 1986, developed many of the key software protocols and technical fixes the Internet depends upon today. The IETF is famously anarchic, not having any official laws, membership criteria or indeed much more than a basic organization. The members of the IETF “reject: kings, presidents, and voting. We believe in: rough consensus and running code.”[95] Normally meeting three times a year, the 300 to 1,300 software engineers do not vote on proposals; instead, they hum. Whichever group is perceived to

[93] See, for instance, William H. Dutton and Malcolm Peltu, “The emerging Internet governance mosaic: connecting the pieces,” *Information Polity* 12, no. 1-2 (2007).
[94] Thanks to Prof. William Dutton for this point.
[95] Attributed to Dave Clark (see, for instance, Borsook, “How Anarchy Works: On location with the masters of the metaverse, the Internet Engineering Task Force.”).

have “hummed louder” carries the (non) vote.[96] Other groups, such as the *Institute for Electrical and Electronics Engineers* (IEEE), are more organized, but work in a similar “bottom-up” approach with absolutely minimal governmental influence. The IEEE has over 350,000 members and addresses issues regarding connectivity (such as Bluetooth, Wireless and broadband). Groups such as the IETF and the IEEE can justifiably claim to have built the Internet, one protocol at a time. Governments have mostly played only a supportive role in this process.

## 5.2. Policy Internet Governance: *Institutionalized*

The policy domain of Internet governance is considerably more organized. ICANN, the *Internet Corporation for Assigned Names and Numbers* is the one organization that comes closest to having an assigning, coordinating or regulating function (and especially a policy function) on the Internet. ICANN is a “nonprofit public-benefit corporation,” according to the laws of the US State of California, and is based at the University of Southern California. Its purpose is to “coordinate, at the overall level, the global Internet's systems of unique identifiers.”[97] Founded in 1998 on the basis of preexisting technical organizations, ICANN was the direct result of President Clinton’s promise to move the Internet out of the government structures[98] and to open it to the public and to private commerce. Under a contract with the US Department of Commerce, ICANN was to “manage Internet names and addresses,” a relatively innocuous-sounding mission encompassing three of the most vital functions of the Internet: first, the allocation of Internet Protocol (IP) number resources for individual computers or machines, and directly corresponding to these, Domain Name Service (DNS) “names,” and the allocation of the so-called Top Level Domains (TLDs)[99] to registries which  assign these identifiers to individual users and organizations across

[96] In its very existence, the IETF is “unofficial”—it does not legally exist, and is officially part of the Internet Society (ISOC), which itself is one of the “founding organizations” of the Internet.

[97] See, for instance, ICANN, “Bylaws for Internet Corporation for Assigned Names and Numbers. A California Nonprofit Public-Benefit Corporation,” 16 March 2012, http://www.icann.org/en/general/bylaws.htm.

[98] See, for instance, Milton Mueller, “Dancing the Quango: ICANN and the Privatization of International Governance,” in *Conference on New technologies and International Governance* (School of Advanced International Studies, Johns Hopkins University, Washington, DC, 11-12 February 2002).

[99] There are a number of different TLDs. The “generic Top Level Domains” (gTLD) include all Internet addresses that, for instance, end with .com, .org, or .info. National domains are known as “country code Top Level Domains” (ccTLD) and, for instance, end with .de, .fr, or .uk.

the globe. Taken together, these three functions represent a considerable segment of Internet functionality.

ICANN has grown with the Internet[100]—from a marginal budget in 1999 to USD 60 million in 2010. Its nature has changed considerably as well. On the one hand, governments have shown increasing interest in the formative work of ICANN, and the Government Advisory Council (GAC) has become especially active. While ICANN was "released" from US government control in October 2009, the US government still retains significant influence—more than other countries represented on the GAC. The increased interests of governments in ICANN, the rise in relative strength of national and generic registries, technical developments as well as the general "need for a mission" has meant ICANN has increasingly positioned itself as a security actor. This is especially evident in the rollout of DNSSEC (the new DNS protocol of the Internet), which is one of ICANN's main functions. Furthermore, the increasing likelihood of attacks on the core infrastructure of the Internet (e.g., DNS and BGP Protocols) has made a case for the establishment of a global DNS-CERT, an idea that ICANN has been very interested in promoting. However, the International Telecommunications Union (ITU) has also showed considerable interest in assuming this role.

The ITU has often sought to challenge ICANN's position as the principal body in Internet governance. As an UN-agency, it has played a key role in many of the UN initiatives in cyberspace, including helping to organize the *Internet Governance Forum* (IGF) and the *World Summit of the Information Society* (WSIS) Process. The IGF has become an annual event for the global stakeholder community, where governments, private sector stakeholders and other interested groups present their views and proposals for Internet-related issues. The ITU has mainly contributed to Internet governance within the technical domain. An ITU *High Level Expert Group on Cybersecurity* was established in 2007. It serves as a consultation forum for information security experts from different regions and produces reports on cybersecurity. It has also sought to promote its own dedicated cyber-centre, IMPACT, located in Malaysia. In 2008, the controversial ITU-T *Resolution 69*[101] on "Non-discriminatory access and use of the Internet resources" effectively called for an "internationalization" of the In-

[100] See Alexander Klimburg, "Ruling the Domain: (Self) Regulation and the Security of the Internet," in *11th Meeting of the ICANN Studienkreis* (Hilton Budapest, 28-29 April 2011).

[101] See World Telecommunication Standardization Assembly, "Resolution 69 – Non-discriminatory access and use of Internet resources," (Johannesburg: ITU-T, 2008).

ternet and was principally backed by Arab states, Russia and China. Around the same time, ITU Secretary General Touré referred to participation in the IGF as a "waste of time." In fact, he has often indicated that the 192-memberstate "ITU family" was a more appropriate forum for many of the looming global issues in cybersecurity.[102] While the EU initially was a strong supporter of the ITU in calling for a better "internationalization" of Internet governance, it also welcomed the US decision to "free" ICANN[103] in 2009, and acknowledged that a significant step had been taken.[104] Recently, a number of EU Member States have been much less active in supporting ITU's ambitions. In a landmark summit in Guadalajara, Mexico, in October 2010, these countries joined the US and other OECD nations in limiting an expansion of the ITU's role in Internet governance.

National governments have shown a growing interest in Internet governance. What was previously described as operating under a "multi-stakeholder model" (including governments, private corporations and the civil society) is coming under increased pressure from national governments trying to expand their relative importance in the domain at the expense of the other stakeholders, according to some academics.[105] The GAC is also trying to upgrade its importance to a body which can influence decisions of the ICANN board. Interestingly, the present US proposal to this mirrors that of European delegates 2005, which was blocked by the then US administration. The Internet Governance Forum is also attempting to redefine itself as part of the renewal of its five-year mandate, a redefinition process governments initially tried to reserve for themselves as their own prerogative. But, as the ITU General Meeting showed, there is still substantial support for the multi-stakeholder approach, and signs that Western OECD nations in particular are joining together to support it.

[102] See Monika Ermert, "Controversy Over Internet Governance: ITU Families And ICANN Cosmetics?," *IP-Watch*, 18 November 2008.

[103] From the Joint Project Agreement (JPA) that effectively made ICANN subordinate to the Secretary of Commerce.

[104] See European Commission, "European Commission welcomes US move to more independent, accountable, international internet governance (IP/09/1397)," *Press Releases*, 30 September 2009.

[105] Including comments made by Prof. Viktor Mayer-Schönberger of the Oxford Internet Institute (OII) at the Domain pulse 2011 conference in Vienna (see http://www.domainpulse.de/de/programm).

# 6. References

Ang, Peng Hwa. "Self Regulation after WGIG." In *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance,* edited by William J. Drake New York: United Nations ICT Task Force, 2005. http://www.wgig.org/docs/book/toc2.html.

Austrian Federal Chancellery. "National ICT Security Strategy Austria." Vienna: Digital Austria, 2012.

BBC. "Cyber crime tool kits go on sale." *BBC News Online*, 4 September 2009.

Beal, Vangie. "The Difference Between a Computer Virus, Worm and Trojan Horse." *Webopedia*, 29 June 2011.

Borsook, Paulina. "How Anarchy Works: On location with the masters of the metaverse, the Internet Engineering Task Force." *Wired*, October 1995.

Carr, Jeff, Andrew Conway, Billy Rios, Derek Plansky, Greg Walton, Jeremy Baldwin, Preston Werntz, and Rafal Rohozinski. "Phase I Report: Russia/Georgia Cyber War – Findings and Analysis." *Project Grey Goose*, 17 October 2008.

Carr, Jeff, Billy Rios, Derek Plansky, Greg Walton, Matt Devost, Ned Moran, Rebecca Givner-Forbes, and Shannon Silverstein. "Project Grey Goose Phase II Report: The evolving state of cyber warfare." *Project Grey Groose*, 20 March 2009.

CERN. "The website of the world's first-ever web server." http://info.cern.ch/.

Cheek, Michael W. "What is Cyber War Anyway? A Conversation with Jeff Carr, Author of 'Inside Cyber Warfare'." *The new new Internet*, 2 March 2010.

Clark, David. "Characterizing cyberspace: past, present and future." *MIT/CSAIL Working Paper*, 12 March 2010.

Dutton, William H., and Malcolm Peltu. "The emerging Internet governance mosaic: connecting the pieces." *Information Polity* 12, no. 1-2 (2007): 63-81.

Ermert, Monika. "Controversy Over Internet Governance: ITU Families And ICANN Cosmetics?" *IP-Watch*, 18 November 2008.

European Commission. "European Commission welcomes US move to more independent, accountable, international internet governance (IP/09/1397)." *Press Releases*, 30 September 2009.

Gady, Franz-Stefan, and Greg Austin. *Russia, The United States, and Cyber Diplomacy. Opening the Doors*. New York: EastWest Institute, 2010. http://www.ewi.info/system/files/USRussiaCyber_WEB.pdf.

Gibson, William. "Burning Chrome [1982]." In *Burning Chrome*. 179-204. New York: HarperCollins Publishers Inc., 2003.

———. *Neuromancer*. New York: Ace Books, 2000 [1984].

Hale, Julian. "NATO Official: Cyber Attack Systems Proliferating." *DefenceNews*, 23 March 2010.

Hamilton, Keith, and Richard Langhorne. *The Practice of Diplomacy. Its evolution, theory and administration.* New York: Routledge, 2011.

Hofman, Jeanette. "The Libertarian Origins of Cybercrime: Unintended Side-Effects of a Political Utopia." *CARR Discussion Paper*, April 2010.

Holden, Michael. "Cyber crime costs UK $43.5 billion a year: study." *Reuters*, 17 February 2011.

Holman, Tyler. "Anonymous threatens to bring down the internet." *Neowin.net*, 27 March 2012.

ICANN. "Bylaws for Internet Corporation for Assigned Names and Numbers. A California Nonprofit Public-Benefit Corporation." 16 March 2012, http://www.icann.org/en/general/bylaws.htm.

———. "IPv6 Factsheet." http://www.icann.org/en/announcements/announcement-26oct07.htm.

———. "To 4,294,967,296 and Beyond – Under 10% of IPv4 Space Remains: Adoption of IPv6 Is Essential." http://www.icann.org/en/announcements/announcement-29jan10-en.htm.

IETF RFC 1122. "Requirements for Internet Hosts – Communication Layers." October 1989, http://tools.ietf.org/html/rfc1122.

IETF RFC 4677. "The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force." September 2006, http://tools.ietf.org/html/rfc4677.

Ignatius, David. "What Happens When the Arab Spring Turns to Summer?" *Foreign Policy*, 22 April 2011.

Internet World Stats. "Internet Growth Statistics." http://www.internetworldstats.com/emarketing.htm.

———. "Internet Users in the World. Distribution by World Region." http://www.internetworldstats.com/stats.htm.

———. "Surfing and Site Guide." http://www.internetworldstats.com/surfing.htm#1.

ISO/IEC 2382-1:1993. "Information technology – Vocabulary – Part 1: Fundamental terms."

ISO/IEC 7498-1:1994. "Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model."

Jackson, William. "How can we be at cyberwar if we don't know what it is?" *Washington Technology*, 22 March 2010.

Kahin, Brian, and Charles Nesson, eds. *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*. Cambridge, MA: MIT Press, 1997.

Kirk, Jeremy. "5 Indicted in Long-running Cybercrime Operation." *CSO Online*, 2 September 2009.

Kirkpatrick, David D., and David E. Sanger. "A Tunisian-Egyptian Link That Shook Arab History." *New York Times*, 13 February 2011.

Klimburg, Alexander. "Ruling the Domain: (Self) Regulation and the Security of the Internet." In *11th Meeting of the ICANN Studienkreis*. Hilton Budapest, 28-29 April 2011.

Klimburg, Alexander, and Heli Tirmaa-Klaar. *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the*

*EU*. Brussels: European Parliament, 2011. http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/EP_Study_FINAL.pdf.

Kramer, Franklin D., Stuart H. Starr, and Larry Wentz, eds. *Cyber Power and National Security*. Washington, DC: National Defence UP, 2009.

Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by Franklin Kramer et al. Washington, DC: National Defense UP, 2009.

Kurbalija, Jovan. *An Introduction to Internet Governance*. Genève: DiploFoundation, 2010. http://archive1.diplomacy.edu/poolbin.asp?IDPool=1060.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. "A Brief History of the Internet." ISOC, http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet.

Lessig, Lawrence. *Code*. New York: Basic Books, 2006. http://codev2.cc/download+remix/Lessig-Codev2.pdf.

———. *The Future of Ideas. The Fate of the Commons in a Connected World*. New York: Random House, 2001. http://www.the-future-of-ideas.com/download/lessig_FOI.pdf.

Leyden, John. "Cybercrime 'More Lucrative' than Drugs. At least phishing fraudsters don't have Uzis." *The Register*, 2005.

Libicki, Martin C. *Conquest in Cyberspace. National Security and Information Warfare*. Cambridge: Cambridge University Press, 2007.

———. *Cyberdeterrance and Cyberwar*. Pittsburgh: RAND Corporation, 2009.

Mathiason, John. *Internet Governance. The new frontier of global institutions*. New York, NY: Routledge, 2009.

McMillan, Robert. "A Chinese ISP Momentarily Hijacks the Internet." *PCWorld*, 8 April 2010.

Mills, Elinor. "Study: Cybercrime cost firms $1 trillion globally." *CNET News*, 28 January 2009.

Mueller, Milton. "Dancing the Quango: ICANN and the Privatization of International Governance." In *Conference on New technologies and International Governance*. School of Advanced International Studies, Johns Hopkins University, Washington, DC, 11-12 February 2002.

———. *Ruling the Root: Internet Governance and the Taming of Cyberspace,* . Cambridge, MA: MIT Press 2002.

US Executive Office of the President. *National Security Presidential Directive 54: Cyber Security and Monitoring (NSPD-54) / Homeland Security Presidential Directive 23: Cyber Security and Monitoring (HSPD-23)*.

Naughton, John. *A Brief History of the Future. The Origins of the Internet*. London: Phoenix, 1999.

Netcraft. "August 2011 Web Server Survey." http://news.netcraft.com/archives/2011/08/05/august-2011-web-server-survey-3.html.

NewScientist. "Exploring the exploding Internet." http://www.newscientist.com/gallery/mg20227061900-exploring-the-exploding-internet/5.

Nye, Joseph S. *The Future of Power*. New York: PublicAffairs, 2011.

OECD. "Working Party on Telecommunication and Information Services Policies. Internet Infrastructure Indicators (DSTI/ICCP/TISP(98)7/FINAL)." Paris 1998.

Parfitt, Tom. "Georgian woman cuts off web access to whole of Armenia." *The Guardian*, 6 April 2011.

Potter, Evan H., ed. *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*. Quebec: McGill-Queen's University Press, 2002.

Public Safety and Homeland Security Bureau. "Tech Topic 20: Cyber Security and Communications." FCC, http://transition.fcc.gov/pshs/techtopics/techtopics20.html.

Reed, Thomas C. *At the Abyss: An Insider's History of the Cold War*. New York: Random House Publishing Group, 2004.

Reidenberg, Joel R. "Governing Networks and Rule-Making in Cyberspace." In *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, edited by Brian Kahin and Charles Nesson. 84-105. Cambridge, MA: MIT Press, 1997.

Samson, Victoria. "The Murky Waters of the White House's Cybersecurity Plan." *Center for Defense Information*, 23 July 2008.

Seib, Philip. *Real-Time Diplomacy. Politics and Power in the Social Media Era*. New York: Palgrave Macmillan, 2012.

Shannon, Victoria. "What's in an 'i'? Internet governance." *New York Times*, 3 December 2006.

Thill, Scott. "March 17, 1948: William Gibson, Father of Cyberspace." *Wired*, 17 March 2009.

UNSTATS. "UN Millennium Development Goals Indicators. The official United Nations site for the MDG Indicators." http://unstats.un.org/unsd/mdg/Metadata.aspx?IndicatorId=0&SeriesId=608.

US Cyber Consequences Unit. "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008." *US-CCU Special Report*, August 2009.

W3C. "A Little History of the World Wide Web. From 1945-1995." http://www.w3.org/History.html.

———. "W3C Glossary/Dictionary." http://www.w3.org/2003/glossary/alpha/D/80.

———. "World Wide Web." http://www.w3.org/History/19921103-hypertext/hypertext/WWW/TheProject.html.

Walton, Marsha. "Web reaches new milestone: 100 million sites." *CNN.com*, 1 November 2006.

WGIG. *Background Report*. Geneva: WGIG, 2005. http://www.wgig.org/docs/BackgroundReport.doc.

———. "Report from the Working Group on Internet Governance (WSIS-II/PC-3/DOC/05)." Geneva: ITU, 2005.

White House. "The Comprehensive National Cybersecurity Initiative." Washington, DC: White House, 2008.

———. "Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure." Washington, DC: White House, 2009.

———. "The National Strategy to Secure Cyberspace." Washington, DC: White House, 2003.

World Bank. "World Development Indicators 2011." http://databank.worldbank.org/ddp/home.do?Step=12&id=4&CNO=2.

World Telecommunication Standardization Assembly. "Resolution 69 – Non-discriminatory access and use of Internet resources." Johannesburg: ITU-T, 2008.

WSIS. "Geneva Declaration of Principles (WSIS-03/GENEVA/DOC/0004)." Geneva: ITU, 2003.

———. "Tunis Agenda for the Information Society (WSIS-05/TUNIS/DOC/6(Rev. 1)-E)." Tunis: ITU, 2005.

Zeenews. "US, China, Russia have 'cyber weapons': McAfee." *Zeenews.com*, 18 November 2009.

oiip Österreichisches Institut für Internationale Politik
Austrian Institute for International Affairs

Berggasse 7
A-1090 Wien

info@oiip.ac.at.
www.oiip.ac.at

Tel. +43/(0)1/581 11 06
Fax. +43/(0)1/581 11 10

## Aktuelle Publikationen des oiip

(ab 2009 bis Herbst 2012, Gesamtübersicht: www.oiip.ac.at)

Die Publikationen des oiip sind das Ergebnis individueller oder kollektiver Arbeiten, die das Forschungsprogramm des Institutes in fachlicher und allgemeinverständlicher Form ergänzen. Für die in den Schriften zum Ausdruck gebrachten Meinungen sind die jeweiligen VerfasserInnen verantwortlich.

### Buchpublikationen in diversen internationalen Verlagen

Zu beziehen über den Fachbuchhandel.

*ADD ON. 2011.* Jahrbuch oiip. Wiener Beiträge zur Internationalen Politik Yearbook oiip. Viennese Contributions to International Affairs. Hrsg. v. Katrin Alas, Cengiz Günay und Jan Pospisil. Facultas.wuv, Wien 2012.

*Obama and the Bomb. The Vision of a World Free of Nuclear Weapons*. Ed. by Heinz Gärtner, Reihe Internationale Sicherheit, Peter Lang - Internationaler Verlag der Wissenschaften, 2011.

Heinz Gärtner, *USA - Weltmacht auf neuen Wegen.* LIT-Verlag Wien – Zürich 2010.

Nico Prucha, *Die Stimme des Dschihad. "Sawt al-gihad": al-Qaidas erstes Online-Magazin.* Verlag Kovac, Juni 2010.

John Bunzl, Farid Hafez (Hrsg.), *Islamophobie in Österreich*, StudienVerlag, 2009.

Jan Pospisil, *Die Entwicklung von Sicherheit. Entwicklungspolitische Programme der USA und Deutschlands im Grenzbereich zur Sicherheitspolitik*, Reihe Global Studies, transcript Verlag, Bielefeld 2009.

Heinz Gärtner, *Obama – Weltmacht auf neuen Wegen*, 2. veränderte Auflage, LIT Verlag, Wien 2009.

### oiip – Arbeitspapiere

Eigenverlag, zu beziehen über das oiip: www.oiip.ac.at

AP 65 Alexander Klimburg/Philipp Mirtl, *„Cyberspace and Governance—A Primer“*, September 2012.

AP 64 Hakan Akbulut, Heinz Gärtner, Daphne Warlamis u.a., *„Nuklear-radiologische Proliferation: Gefährdungspotential und Präventionsmöglichkeiten für Österreich.“* Dezember 2011.

AP 63 Paul Luif, “*Challenges for Integrated Peacekeeping Operations.”* Dezember 2010.

AP 62 Stefan Khittel und Jan Pospisil, *„Früherkennung von bewaffneten Konflikten? Ein Vergleich standardisierter Konfliktanalyseverfahren*“, April 2010.

AP 61 Paul Luif, *„Strategien kleinerer europäischer Staaten in der Technologiepolitik als Antwort auf die Herausforderung durch China und Indien“: Die Entwicklung von Strategien in Finnland,* *Schweden, der Schweiz und den Niederlanden, mit einem Anhang zur F & E – Politik der Europäischen Union*, September 2009.

AP 60 Hakan Akbulut, *Die zivil-militärischen Beziehungen in der Türkei: zwischen Putschbestrebungen und Demokratisierungsbemühungen*, September 2009.

## oiip – Policy Paper und Kurzanalysen

zu beziehen über das oiip: www.oiip.ac.at

Heinz Gärtner, *Die NATO nach dem Gipfel in Chicago 2012*, Kurzanalyse, Juni 7/2012.

Vedran Dzihic, *Serbien nach den Wahlen – Neue Konstellation, gleiche Problemlagen*, Kurzanalyse, Juni 6/2012.

Hakan Akbulut, *Von der Vormundschaft zur Normalisierung in den zivil-militärischen Beziehungen in der Türkei,* Kurzanalyse, Mai 5/2012.

Gerhard Mangott: *Putin 2.012*, Kurzanalyse, März 4/2012.

Cengiz Günay, *Ägypten – von der Revolution zur islamischen Demokratie?,* Kurzanalyse, März 3/2012.

Heinz Gärtner, *Deterrence and Disarmament,* Kurzanalyse, März 2/2012.

Jan Pospisil, *Eiskalte Interdependenzen: Der Südsudan radikalisiert seine politische Neuorientierung an der Erdölfront,* Kurzanalyse, Februar 1/2012.

Gerhard Mangott, *Ämtertausch und kontrollierte Wahlniederlage. Russland an der Schwelle zu neuer Instabilität*, Policy Paper, Dezember 2011.

Tobias Lang und Cengiz Günay: *Regionale Auswirkungen der Entwicklungen in Syrien am Beispiel des Libanon*, Kurzanalyse, November 2011.

Bernardo Mariani,*Starting to Build? China's Role in UN Peacekeeping Operations*, Policy Paper, November 2011.

Melanie Pichler, *Sustainable Palm-Based Agrofuels? Current Strategies and Problems to Guarantee Sustainability for Agrofuels within the EU*, Policy Paper, November 2011.

Hakan Akbulut, *Der Zypernkonflikt und seine Auswirkungen auf die EU-Ambitionen der Türkei,* Kurzanalyse, Oktober 2011.

Heinz Gärtner, *Die österreichische Sicherheitsstrategie (ÖSS) im globalen Kontext*, Kurzanalyse, Oktober 2011.

Daniela Härtl, *Kolumbien zwischen Gewalt und Hoffnung.* Analytische Betrachtungen und Eindrücke vor Ort. Report, September 2011.

Cengiz Günay and Maria Janik, *Egypt in Transition – Ready for Democracy?,* Current Analysis, September 2011.

Alexander Klimburg and Philipp Mirtl, *Cyberspace and Governance—A primer*, Special Issue, September 2011.

Heinz Gärtner, *The Responsibility to Protect (R2P) and Libya*, Kurzanalyse, Juli 2011.

Gerhard Mangott, *Putin 2.0. Russland vor den Präsidentenwahlen 2012*. Kurzanalyse, Juli 2011.

John Bunzl, *Die Umwälzungen in der arabischen Welt und der Palästinakonflikt*, Kurzanalyse, Juni 2011.

Heinz Gärtner, *A Nuclear-Weapon-Free Zone in the Middle East*, Kurzanalyse, April 2011.

Nico Prucha, *Eyeballing Libya – al-Qa'ida's New Foothold?*, Policy Paper, April 2011.

Henriette Riegler, *Kroatien: Demonstrationen mit ungewissen Folgen*, Kurzanalyse, April 2011.

Gerhard Mangott*, Nordafrika und die Rohölversorgung der Europäischen Union*, Kurzanalyse, März 2011.

Cengiz Günay, *Transformationen in der arabischen Welt Kontinuität versus Wandel und Folgen für die Region*, Kurzanalyse, März 2011.

Cengiz Günay, *This was Mubarak's Egypt*, Hintergrundinformationen, Februar 2011.

Cengiz Günay, *Ägypten – Der Zweite Dominostein?* Kurzanalyse, Januar 2011.

Jan Pospisil, *Visionen, Realitäten und Risken eines unabhängigen Südsudan: Implikationen des Referendums vom Jänner 2011*. Kurzanalyse, Januar 2011.

Paul Luif, *Die „neue" Gemeinsame Außen- und Sicherheitspolitik der Europäischen Union: Was hat Lissabon gebracht?* Kurzanalyse, Dezember 2010.

Heinz Gärtner, *IAEA: Y. Amano´s first year as Director General.* Kurzanalyse, November 2010.

Otmar Höll, *Sudan – Mögliche österreichische Beiträge zur gesellschaftlichen Entwicklung.* Policy Paper, September 2010.

Heinz Gärtner, *NATO zwischen Tradition und Modernisierung.* Stellungnahme zum Bericht „NATO 2020: Assured Security; Dynamic Engagement. Analysis and recommendations of the group of experts on a new strategic concept for NATO," 17 May 2010. Kurzanalyse, Oktober 2010.

John Bunzl, *Frieden oder Friedensprozess? Zum Treffen von Netanyahu, Abbas und Obama in Washington.* Kurzanalyse, September 2010.

Heinz Gärtner, *Die Bedeutung von internationalem Engagement der österreichischen Sicherheitskräfte für Österreich.* Kurzanalyse, Juli 2010.

Markus Schwarz-Herda, *Die Präsidentschaftswahlen in Kolumbien.* Kurzanalyse, Juli 2010.

Henriette Riegler, *Kroatien: Ivo Josipović´ erste hundert Tage. Ein Präsident zeigt sein Profil.* Kurzanalyse, Juni 2010.

Heinz Gärtner, *Kann sich Österreich im Mittleren Osten erneut engagieren? Zur Schaffung einer nuklearfreien Zone in dieser Region.* Kurzanalyse, Juni 2010.

Heinz Gärtner, *Obamas neue Strategie: Abkehr von Bush.* Stellungnahme zur „National Security Strategy,“ President of the United States. Kurzanalyse,  Juni 2010.

Heinz Gärtner, *Amerika und Europa: transatlantische Beziehungen oder globale Verantwortung?* Policy Paper, April 2010.

Heinz Gärtner, *Disarmament – Non-Proliferation – Deterrence.* Policy Paper, März 2010.

Heinz Gärtner, *Nonproliferation and Engagement:Iran and North Korea should not let the opportunity slip by.* A comment on the actual state of affairs. Kurzanalyse, November 2009.

Heinz Gärtner, *Die Ereignisse im Iran, die USA und das iranische Nuklearprogramm*. Kurzanalyse, Juni 2009.

Stefan Lehne, *Resolving Kosovo's Status*. Policy Paper, Juni 2009.

John Bunzl und Cengiz Günay, *Obama: A New Beginning?* Kurzanalyse, Juni 2009.

Heinz Gärtner, *Apropos NATO: Was verändert sich mit Obama?* Kurzanalyse, Juni 2009.

Cengiz Günay, *Die Türkei : Der Besuch von Präsident Obama. Hintergrund, Auswirkungen, die außenpolitische Rolle der Türkei und ihr Verhältnis zur EU.* Kurzanalyse, Mai 2009.

## Working Paper in Progress

Alexander Klimburg, *Ruling the Domain: (Self) Regulation and the Security of the Internet*, paper informally distributed at the 11th Meeting of the ICANN Studienkreis, 28./29. April 2011, Hilton Budapest.

Wien, Österreichisches Institut für Internationale Politik – oiip, 2012