



Special Issue

Cyberspace and Governance—A primer

**Alexander Klimburg
Philipp Mirtl**

September 2011

The aim of this policy paper is threefold: First, it suggests 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 cyberwarfare; cybercrime/-terrorism; cyberespionage; Critical Infrastructure Protection (CIP) and Information Assurance (IA); as well as Internet Governance; usually, each of which is covered by different government departments. 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.

Grasping the difference

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

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. That this has occurred at all is largely due 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.³ This is why the development of Internet standards can best be described as a self-regulatory process.⁴

Measured by regular surveys,⁵ the amount of global Internet users (defined as persons who have available access to an Internet connection point,⁶ and the basic knowledge required to use web technology⁷) has, in fact, risen from 16 million in 1995 to more than 2.1 billion in 2011.⁸ This is an outstanding 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%).⁹

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).¹⁰ The *Internet* (with an uppercase “I”), however, is the unique “global network of com-

¹ Naughton, John, *A brief History of the Future. The Origins of the Internet*, London, Phoenix, 1999, p. 311.

² See, for instance, Leiner, Barry M. et al., ‘A brief history of the Internet’, *ISOC*, 1997, <http://www.isoc.org/internet/history/brief.shtml>.

³ See, for instance, Borsook, Paulina, ‘How Anarchy Works. On location with the masters of the metaverse, the Internet Engineering Task Force’, *Wired*, October 1995, <http://www.wired.com/wired/archive/3.10/ietf.html>.

⁴ OECD, ‘Working Party on Telecommunication and Information Services Policies. Internet Infrastructure Indicators’, *DSTI/ICCP/TISP(98)7/FINAL, 1998*, <http://www.oecd.org/dataoecd/11/25/2091083.pdf>.

⁵ See, for instance, UNSTATS, *UN Millennium Development Goals Indicators*, 2011, <http://unstats.un.org/unsd/mdg/Metadata.aspx?IndicatorId=0&SeriesId=608>.

⁶ Internet connection points are usually provided by Internet service providers (ISPs) against payment.

⁷ See Internet World Stats, *Surfing and Site Guide*, 2011, <http://www.internetworldstats.com/surfing.htm#1>.

⁸ See Internet World Stats, *Internet Growth Statistics*, 2011, <http://www.internetworldstats.com/emarketing.htm>.

⁹ See Internet World Stats, *Internet Users in the World. Distribution by World Region*, 2011, <http://www.internetworldstats.com/stats.htm>; also see NewScientist, *Exploring the exploding Internet*, 2009, <http://www.newscientist.com/gallery/mg20227061900-exploring-the-exploding-internet/5>.

¹⁰ 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,

puter networks.”¹¹

Internet capitalization conventions should not be underrated in political discourse. For instance, when in 2006 the International Telecommunications Union (ITU) changed its policy in officially spelling out “internet” (with a lowercase “i”), US ambassador David A. Clark reacted disturbed, not knowing whether this was meant to be of any concern for US interests.¹² However, it should be noted that *The Economist* had already 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*.¹³

The Internet is essentially a collection of networks—and these networks’ devices—that agree to communicate with each other. This communication depends on the so-called Internet Protocol (IP).¹⁴ Internet protocol numbers represent the most basic identifier on the Internet. Every device connected to the Internet has its own¹⁵ IP number—if it does not have an IP number, it is not connected to the Internet.¹⁶ The binary system allows a theoretical maximum of 4,29 billion unique IP addresses, which in the 1970s was considered to be adequate for the foreseeable future. The explosive growth of the Internet since the mid-1990s and the conversion of the Internet to a „Internet of things“, with everyday applications such as household appliances and industrial goods accessible over the Internet, has meant that this number has proven to be inadequate. Indeed, since years it has been known that the finite IPv4 range would be exhausted within the near future. This point, known as the IPv4 depletion date, has constantly been moved forward, and finally occurred in early 2011.¹⁷

To prevent the Internet (or at least Internet growth) from coming to a crashing stop, the newest version of the Internet Protocol, called IPv6, has been introduced. The 128-bit IPv6 eliminates the most important resource restriction by allowing 340 *trillion, trillion, trillion* unique IP addresses, therefore providing an adequate supply for the foreseeable future. With IP addresses not a restricted commodity anymore this will allow the true “Internet of things” to occur—where literally all of human possessions (now, and for the foreseeable future) could potentially be “tagged” and be accessible over the Internet. The new Internet is therefore just beginning.

Increasingly, this definition is being expanded upon to include not only “computers” but in effect all devices connected to the Internet.

for instance, *Supervisory Control and Data Acquisition* systems (SCADA) increasingly monitor and control industrial production or infrastructure over IP-based LAN-WAN connections.

¹¹ Naughton, John, *A brief History of the Future. The Origins of the Internet*, London, Phoenix, 1999, p. 314.

¹² Shannon, Victoria, ‘What’s in an ‘I’? Internet governance’, *New York Times*, 3 December 2006
<http://www.nytimes.com/2006/12/03/technology/03iht-btitu.3755510.html?pagewanted=1>.

¹³ See Kurbalija, Jovan, *An Introduction to Internet Governance*, Genève, DiploFoundation, 2010, p. 6,
<http://www.diplomacy.edu/poolbin.asp?IDPool=1060>.

¹⁴ Sometimes also written TCP/IP.

¹⁵ By using a technique called NAT it is in fact possible for some devices to share an IP number under certain circumstances.

¹⁶ Post, D.G., ‘Governing Cyberspace, or Where is James Madison When we Need Him?’ *Plugging in*, June 1999
www.temple.edu/lawschool/dpost/icann/comment1.html.

¹⁷ See for instance the ‘The IPv4’ depletion website’ at: http://www.ipv4depletion.com/?page_id=147.

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 through a wealth of information was eventually released to the wider public in 1991.¹⁸ However, the Web only had its breakthrough in 1993, when Mosaic—the first major graphics supporting browser—entered the market.¹⁹

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 Mark-up 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 sub pages) with domain names and content on the Net.²⁰ Compared to just 18,000 in August 1995,²¹ 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.²²

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 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%.²³

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, in fact, can be visualized by looking at the layered network architecture model called the *Internet Protocol Suite*.²⁴ 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*).²⁵ All this means that Web services can only be used properly if the underlying services (e.g., TCP/IP) work cor-

¹⁸ CERN, *The website of the world's first-ever web server*, 2008, <http://info.cern.ch/>.

¹⁹ W3C, *A Little History of the World Wide Web*, 2000, <http://www.w3.org/History.html>.

²⁰ Netcraft, *August 2011 Web Server Survey*, 2011, <http://news.netcraft.com/archives/2011/08/05/august-2011-web-server-survey-3.html>.

²¹ Walton, Marsha, ‘Web reaches new milestone: 100 million sites’, *CNN*, 1 November 2006. <http://edition.cnn.com/2006/TECH/internet/11/01/100millionwebsites/>

²² Netcraft, *August 2011 Web Server Survey*, 2011, <http://news.netcraft.com/archives/2011/08/05/august-2011-web-server-survey-3.html>.

²³ Ibid.

²⁴ IETF, ‘Requirements for Internet Hosts—Communication Layers’, *RFC 1122*, <http://tools.ietf.org/html/rfc1122>.

²⁵ ISO/IEC, Standard 7498-1:1994.

rectly.

In this context, the Net's overall idea is to *interconnect computers* in a global network of computer networks. Building upon this interconnection, the Web's essential aim is to *manage information*; traditionally, in a global Web of human-readable documents that can be defined as "content supplied in response to a request".²⁶

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."²⁷ Elsewhere, the Web was also referred to as a "hypermedia system linking text, graphics, sound and video on computers distributed all over the world."²⁸

Cyberspace—a four layer model

In the introduction to this chapter, cyberspace has been referred to as the *world behind your screen*. Since the 1960s, this world's horizons have widened considerably. This is, in no small part, due to Net 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 sections 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 quite some attention. Science fiction author William Gibson is credited with first mentioning it in his short story *Burning Chrome* (1982).²⁹ Two years later, in his famous 1984 cyberpunk novel called *Neuromancer*, the author described Cyberspace as a "consensual hallucination."³⁰

Years later Gibson labeled the term an "effective buzzword" that seemed "evocative and essentially meaningless" when it first emerged on his pages.³¹ However, today *cyberspace* is not only popular among different strands of computer enthusiast but has become a "common use" definition.

In contrast to land, sea, air and space, cyberspace is a human construct whose components can change over time. Today one can find a broad variety of different definitions of cyberspace.³² One of which was first used in the aftermath of 9/11, when the 2003 *US National Strategy to Secure Cyberspace* described

²⁶ W3C, *Glossary*, 2004, <http://www.w3.org/2003/glossary/alpha/D/80>.

²⁷ W3C, *World Wide Web*, 1992, <http://www.w3.org/History/19921103-hypertext/hypertext/WWW/TheProject.html>.

²⁸ Naughton, John, *A brief History of the Future. The Origins of the Internet*, London, Phoenix, 1999, p. 319.

²⁹ Gibson, William, *Burning Chrome*, New York, Arbor House, 1986.

³⁰ Gibson, William, *Neuromancer*, New York, Ace Books, 1984, p. 67.

³¹ Thill, Scott, 'March 17, 1948: William Gibson, Father of Cyberspace', *Wired*, 17 March 2009, http://www.wired.com/science/discoveries/news/2009/03/dayintech_0317.

³² For a first overview see Kuehl, Daniel T., 'From Cyberspace to Cyberpower: Defining the Problem,' in Kramer, Franklin D. et al., eds., *Cyberpower and National Security*, Washington, D.C., National Defense UP, 2009, pp. 26-7.

cyberspace as a national “nervous system” that controls the country’s critical infrastructure. While highlighting the role of public-private engagement, the strategy stated:

“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.”³³

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).³⁴ This document established the Comprehensive National Cybersecurity Initiative (CNCI);³⁵ a still partially classified³⁶ USD 17 billion program designed to protect Federal Government systems against intrusion attempts.³⁷ 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.”³⁸

Under the Obama administration, this definition has equally been adopted by the 2009 *60-Day Cyberspace Policy Review*.³⁹ Nevertheless, there is still no standard, universally accepted definition for cyberspace. In this context, 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. In the literature one finds different numbers and names of layers.⁴⁰ However, this paper argues in favor of the following four layer model of cyberspace:⁴¹

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 in-

³³ White House, *The National Strategy to Secure Cyberspace*, 2003, <http://georgewbush-whitehouse.archives.gov/pqipb/>.

³⁴ FAS, *National Security Presidential Directives (NSPD) George W. Bush Administration, 2001-2009*, <http://www.fas.org/irp/offdocs/nspd/>.

³⁵ White House, *The Comprehensive National Cybersecurity Initiative*, 2 March 2011, <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>

³⁶ United States District Court for the District of Columbia, *Complaint for Injunctive release*, 2009, http://epic.org/foia/NSPD54_complaint.pdf.

³⁷ Samson, Victoria, ‘The Murky Waters of the White House’s Cybersecurity Plan’, *CDI*, 23 July 2008, http://www.cdi.org/program/document.cfm?DocumentID=4345&from_page=../index.cfm.

³⁸ FCC, *Tech Topic 20: Cyber Security and Communications*, <http://transition.fcc.gov/pshs/techttopics/techttopics20.html>.

³⁹ White House, *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

⁴⁰ See, for instance, Libicki, Martin C., *Conquest in Cyberspace, National Security and Information Warfare*, Cambridge et al., Cambridge University Press, 2007, chapter 10; and Kramer, Franklin D. et al., eds., *Cyberpower and National Security*, Washington, D.C., National Defense UP, 2009, chapter 2.

⁴¹ See Clark, David, ‘Characterizing cyberspace: past, present and future’, *Working Paper MIT/Harvard*, <http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf>.

frastructure can be located geographically⁴² in “real space” and is thus subject to different national jurisdictions. If it were removed, the overlying layers would disappear as well, as happened earlier this year 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.⁴³

- 2. The logical layer** generally refers to the “code”, which includes both the software as well as the protocols that can be incorporated within that software.⁴⁴ Generally speaking, a protocol defines the rules or conventions that are necessary to obtain a certain goal (e.g. communication). The formalization of a protocol makes it a standard. Software, by 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. 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 segmentation, known as the OSI Model, basic every-day 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 eventually can themselves be combined and applied by other applications on even higher levels. This flexibility opens inexhaustible 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 has also a dark side: *malware*. Essentially, *malware* (also *malicious logic*) includes a variety of different *Trojans*, *viruses* and *worms*.⁴⁵ Similar to “benign” services, more complex malware often combines certain aspects of already existing logic – i.e. represent a combination of different abilities.⁴⁶ In the past, one of the first major “logical” incidents occurred in 1982 when the CIA purportedly corrupted the software of a Soviet gas pipeline computer control system, which subsequently was said to result in “the most monumental non-nuclear explosion and fire ever seen from space.”⁴⁷ Other threats include attacks on the basic infrastructure of the Net itself, for instance the Domain Name System. In April 2010, for example, a Chinese ISP introduced the wrong information into their routing tables. This caused around 10% of the Internet traffic to be (theoretically) routed

⁴² See, for instance, TeleGeography, *Map Gallery*, 2010, <http://www.telegeography.com/telecom-resources/map-gallery/index.html>.

⁴³ CBCNews, *Elderly “spade hacker” severs Armenian internet*, 6 April 2011,

<http://www.cbc.ca/news/world/story/2011/04/06/georgia-armenia-internet-cut.html>.

⁴⁴ See, for instance, Lessig, Lawrence, *The Future of Ideas. The Fate of the Commons in a Connected World*, New York, Random House, p. 23, http://www.the-future-of-ideas.com/download/lessig_FOI.pdf; and Lessig, Lawrence, *Code v2*, New York, Basic Books, 2006, <http://codev2.cc/download+remix/Lessig-Codev2.pdf>.

⁴⁵ Beal, Vangie, ‘The Difference Between a Computer Virus, Worm and Trojan Horse’, *Webopedia*, 29 June 2011, <http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp>.

⁴⁶ Klimburg, Alexander, Tiirmaa-Klaar, Heli, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*, Brussels, European Parliament, 2011, pp. 48,

http://www.oii.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/EP_Study_FINAL.pdf.

⁴⁷ Reed, Thomas C., *At the Abyss: An Insider’s History of the Cold War*, New York, Presidio Press, 2004, p. 269.

through China.⁴⁸ 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.”⁴⁹

3. **The content layer** describes all the *information* that is created, captured, stored and processed within cyberspace. Information is defined as “knowledge concerning objects, such as facts, events, things, processes, or ideas”.⁵⁰ It contains all human-readable messages delivered by social media Websites or email; the content of articles and books that are kept on memory sticks and virtual databases; the news that are broadcasted via blogs and Websites as well as the music, movies and pictures that are consumed online. However, access to information can also be systematically limited. Blocking or removing online content from the Web happens for different reasons such as protecting intellectual property rights, securing national order or social identity. In fact, in the last couple of years, online censorship and content restrictions have risen rapidly as is demonstrated by the OpenNet Initiative.⁵¹ Moreover, information may take a more abstract form. If computers, for instance, inform their connected printers how to print a certain document, they do so by using printer control strings. These can be considered to be informational in form but logical in purpose.⁵² 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* who are 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, they all share a specific characteristic: While in “real” life (*extra cyberspace*) people can ultimately be identified by their unique DNA code, attribution is a much more difficult on the Net (*intra cyberspace*). In contrast to the “meat” world, individuals in cyberspace have an easier time establishing multiple identities. One single virtual identity can have multiple human users (e.g., the same New York Times (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 the recent revolutions in Tunisia and Egypt, for instance, it has been argued that the exchange via Facebook played an important

⁴⁸ The difference here is between theoretical and actual route propagation—in fact while 10% of the Internet traffic could have gone through China, only a small fraction of it actually did. 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.

⁴⁹ See McMillan, Robert, ‘A Chinese ISP Momentarily Hijacks the Internet’, *PCWorld*, 8 April 2010, http://www.pcworld.com/article/193849/a_chinese_isp_momentarily_hijacks_the_internet.html.

⁵⁰ ISO/IEC, Standard 2382-1:1993.

⁵¹ <http://opennet.net/>

⁵² Libicki, Martin C., *Cyberdeterrence and Cyberwar*, RAND, 2009, p. 12, http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf.

role in giving birth to “a pan-Arab youth movement dedicated to spreading democracy in a region without it.”⁵³ The protests in Tunisia, Egypt, Libya, Yemen, and Syria have even been characterized as a “‘global political awakening’—a movement for change that is enabled and accelerated by modern technology’.”⁵⁴

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. Cyber threats, 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 seek to ultimately influence the “social layer”.

The Five Mandates of National Cybersecurity

Within the general context of discussing “national cybersecurity” it is very important to keep in mind that it is not one single subject matter. 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. This is not an ideal state. Unfortunately, there is normally always 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 overlap to a large extent, 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 of these mandates has developed its own emphasis and even own language, despite the fact that they are all simply different facets of the same problem.

1. **Cyberwarfare:** 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.⁵⁵ Many governments are building capabilities to wage cyberwar,⁵⁶ while some NATO reports have claimed that up to 120 countries are developing a military cyber-capability.⁵⁷ 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

⁵³ Kirkpatrick, David D., Sanker, David E., ‘A Tunisian-Egyptian Link That Shook Arab History’, *New York Times*, 13 February 2011,

http://www.nytimes.com/2011/02/14/world/middleeast/14egypt-tunisia-protests.html?_r=1.

⁵⁴ Ignatius, David, ‘What happens when the Arab spring turns into summer?’, *Foreign Policy*, 22 April 2011, http://www.foreignpolicy.com/articles/2011/04/22/what_happens_when_the_arab_spring_turns_to_summer.

⁵⁵ See Zeenews, *US, China, Russia have ‘Cyber weapons’: McAfee*, 18 November 2009, <http://www.zeenews.com/news579965.html>.

⁵⁶ See, Cheek, Michael W., ‘What is Cyber War Anyway? A Conversation with Jeff Carr, Author of ‘Inside Cyber Warfare’’, *The new new Internet – The Cyber Frontier*, 2 March 2010, <http://www.thenewnewinternet.com/2010/03/02/what-is-cyberwar-anyway-a-conversation-with-jeff-carr-author-of-inside-cyber-warfare/>.

⁵⁷ See Hale, Julian, ‘NATO Official: Cyber Attack Systems Proliferating’, *DefenceNews*, 23 March 2010, <http://www.defencenews.com/story.php?i=4550692>.

shutting down an air-defence system. 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: firstly, that the Laws of Armed Conflict apply also in cyberspace and, secondly, that a “cyberwar attack” is said to have occurred if “the level of damage is approximate to a physical attack.”⁵⁸ This has not prevent the term cyberwar being used in a number of inappropriate or misleading contexts (for instance when referring to cyber-espionage), and therefore it is true to say that “cyberwarfare is a loaded term.”⁵⁹

- 2. Cybercrime and -terrorism:** Cybercrime is increasingly considered to be 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 2009,⁶⁰ and it has long since overtaken the drug trade in terms of business volume.⁶¹ 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,⁶² and even the provision of entire hacking tools and root-kits to enable large-scale cyber-campaigns.⁶³ There are strong indications that Russian cybercrime syndicates played a role in the cyberattacks on Georgia and Estonia,⁶⁴ to name but two examples. This is also where cybercrime interacts not only with cyberwarfare, but also with cyberterrorism. Cyberterrorism is a highly contentious term—there is a strong concern that the term could be used to severely criminalize not only “minor acts of cybercrime” (often called *hacktivism*) but also any types of online expression that is simply 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—minor nuisance is certainly not an act of terrorism.

⁵⁸ This was agreed at the ‘Cyber 15’ deliberations conducted at the UN in the summer of 2010 (

⁵⁹ See Jackson, William, ‘How can we be at cyberwar if we don’t know what it is?’, *Washington Technology*, 22 March 2010, <http://washingtontechnology.com/articles/2010/03/22/cybereye-cyberwar-debate.aspx>.

⁶⁰ See Mills, Elinor, ‘Study: Cybercrime Cost Firms \$1 Trillion Globally’, *cnet news*, 28 January 2009, http://news.cnet.com/8301-1009_3-10152246-83.html.

⁶¹ See Leyden, John, ‘Cybercrime ‘More Lucrative’ than Drugs. At least phishing fraudsters don’t have Uzis’, *The Register*, 29 November 2005, <http://www.theregister.co.uk/2005/11/29/cybercrime/>.

⁶² See Kirk, Jeremy, ‘5 Indicted in Long-running Cybercrime Operation’, *csoonline*, 2 September 2009, http://www.csoonline.com/article/501180/5_Indicted_in_Long_running_Cybercrime_Operation.

⁶³ For an early mention of this see BBC, *Cyber crime tool kits go on sale*, 4 September 2009, <http://news.bbc.co.uk/2/hi/technology/6976308.stm>.

⁶⁴ See Project Grey Goose, *Phase I Report: Russia/Georgia Cyber War – Findings and Analysis*, 17 October 2008, <http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report>; Idem, *Phase II Report: The evolving state of cyber warfare*, 20 March 2009, <http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report>; and US Cyber Consequences Unit (US-CCU), *Overview by the US-CCU of the Cyber Campaign Against Georgia in August 2008*, August 2009, <http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf>.

- 3. Cyberespionage:** Differing cyberespionage from cybercrime and cyberwar 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 really a nation-state, or a criminal-group operating on behalf of a nation-state—or indeed 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 US economy USD 100-200 billion a year, according to a recent CSIS study. Cyberespionage, when directed towards states, also makes it necessary to develop specific foreign policy response mechanisms that also can deal with the inherent ambiguity of actors in cyberspace.
- 4. Critical Infrastructure Protection (CIP) and Information Assurance (IA):** CIP and IA are two diametrically different views of a rather complex field. 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. Information Assurance (IA) is often the tool of choice to manage cyber-risks. IA, itself a descendent of risk management methodology, is a collection of operational practices that seek to reduce the risk of any particular organization to suffering a breach of Confidentiality, Integrity or Availability of the information it manages. IA methodologies, for instance represented in the ISO2700 series, represent an important tool to increase the overall level of safety within a nation state.
- 5. Internet Governance:** While CIP has a national view, Internet Governance is probably the most international of all mandates. Internet Governance 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 the Internet. As one of the most understated and least understood aspects of national cybersecurity it is described at more length below.

As said in the introduction, the actual 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 thing—all of these mandates need to be engaged upon to be able to develop a comprehensive national cybersecurity perspective. However, this type of comprehensive view is a luxury most practitioners of cybersecurity can simply not leverage due to resource constraints.

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 “bot-

tom-up” in a process that is often referred to as the self-regulation of the Internet.⁶⁵ 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 programs that shape the evolution and use of the Internet.”⁶⁶

The Internet is a relatively new environment for human activities, and 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. 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. 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 late-comers 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.

Technical Internet Governance: ad hoc

Internet governance can be subdivided into two domains: the *technical* and the *policy domain*. The technical domain is widely dominated by volunteers and the civil society and 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 that 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.”⁶⁷ Meeting (usually) three times a year, the 300 to 1,300 software engineers do not vote on proposals. Instead, they hum. Whichever group is perceived to have “hummed louder” carries the (non) vote.⁶⁸ 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.

⁶⁵ See, for example, Ang, Peng Hwa, ‘Self Regulation after WGIG’, in Drake, William J. (ed.), *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance*, New York, UNICTTF, 2005, pp. 129-34, <http://www.wgig.org/docs/book/toc2.html>; for a shorter and older bibliography that provides a good overview of uses of the term, see Internet Law and Policy Forum, ‘A Bibliography of Internet Self-Regulation’, undated, http://www.ilpf.org/events/selfreg/bib4_18.htm.

⁶⁶ WGIG, ‘Report of the Working Group on Internet Governance’, *Château de Bossey*, June 2005, p. 4, <http://www.wgig.org/docs/WGIGREPORT.pdf>.

⁶⁷ Attributed to Dave Clark: see, for instance, in Borsook, 1995.

⁶⁸ The IETF is in its very existence ‘unofficial’ – it does not legally exist, and is officially part of the Internet Society (ISOC) – itself one of the ‘founding organisations’ of the Internet.

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 “non-profit 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.”⁶⁹ 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 structures⁷⁰ 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 that encompasses three of the most vital functions of the Internet: the allocation of Internet Protocol (IP) number resources for individual computers or machines; directly corresponding to these, Domain Name Service (DNS) “names”; and the allocation of the so-called Top Level Domains (TLDs)⁷¹ to registries that actually assign these identifiers to individual users and organizations across the globe. Taken together, these three functions represent a considerable segment of Internet functionality.

ICANN has grown with the Internet⁷²—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 that ICANN has increasingly positioned itself as a security actor. This is especially evident in the roll-out 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 shown great interest in assuming this role as well.

The ITU has often sought to challenge ICANN’s position as the principal body in Internet governance. As a 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 govern-

⁶⁹ See, for instance, ICANN, *Bylaws*, 25 January 2011, <http://www.icann.org/en/general/bylaws.htm>.

⁷⁰ See, for instance, Mueller, Milton, ‘Dancing the Quango: ICANN and the Privatization of International Governance’, *Conference on New Technologies and International Governance*, 11-12 February 2002, <http://faculty.ischool.syr.edu/mueller/quango.pdf>.

⁷¹ 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.

⁷² See Klimburg, Alexander, *Ruling the Domain – (Self) Regulation and the Security of the Internet*, 2011, www.oaip.at (unpublished).

ments, 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*⁷³ on “Non-discriminatory access and use of the Internet resources” effectively called for an “internationalization” of the Internet 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.⁷⁴ 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” ICANN⁷⁵ in 2009, and acknowledged that a significant step had been taken.⁷⁶ 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 which are trying to expand their relative importance in domain at the expense of the other stakeholders, according to some academics.⁷⁷ The GAC is also trying to upgrade its importance to a body that can influence decisions of the ICANN board. Interestingly, the present US proposal to this mirrors what European delegates made in 2005 that was blocked by the 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 that governments initially tried to reserve for themselves as their own prerogative. However, 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.

Alexander Klimburg is Fellow and Senior Adviser at the oiip and specialist on national cybersecurity.

Philipp Mirtl is Research Associate and Adviser at the oiip and researches issues on Internet Governance.

⁷³ See ITU, ‘Resolution 69 – Non-discriminatory access and use of Internet resources’, *World Telecommunication Standardization Assembly*, Johannesburg 21-30 October 2008, http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.69-2008-PDF-E.pdf.

⁷⁴ See New, William, ‘Controversy Over Internet governance: ITU Families And ICANN Cosmetics?’, *ITU*, http://www.itu.int/osg/csd/intgov/ituinpress/new_william.html.

⁷⁵ From the Joint Project Agreement (JPA) that effectively made ICANN subordinate to the Secretary of Commerce

⁷⁶ See Rapid Press Release, *European Commission welcomes US move to more independent, accountable, international Internet governance*, 30 September 2009, <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1397>.

⁷⁷ Including comments made by Victor Mayer-Schönberger of the Oxford Internet Institute at a recent conference in Vienna (see <http://www.domainpulse.de/de/programm>).