An Introduction to

INTERNET GOVERNANCE

Jovan Kurbalija

7th edition

DiPLO
www.diplomacy.edu

The history of this book is long, in Internet time. The original text and the overall approach, including the five-basket methodology, were developed in 1997 for a training course on information and communications technology (ICT) policy for government officials from Commonwealth countries. In 2004, Diplo published a print version of its Internet governance materials, in a booklet entitled *Internet Governance – Issues, Actors and Divides*. This booklet formed part of the Information Society Library, a Diplo initiative driven by Stefano Baldi, Eduardo Gelbstein, and Jovan Kurbalija. In 2008, a special, revised version of the book, entitled simply *An Introduction to Internet Governance*, was published in cooperation with NIXI India on the occasion of the 2008 Internet Governance Forum (IGF) held in Hyderabad, India. In 2009, a revised third edition was published in cooperation with the Ministry of Communication and Information Technology of Egypt. The fourth edition (2010) was produced in partnership with the Secretariat of the Africa-Caribbean-Pacific Group of Countries and the European Union. The fifth edition (2012) was published in cooperation with the Azerbaijan Diplomatic Academy (ADA). The sixth edition was published in September 2014. The late Eduardo Gelbstein made substantive contributions to the sections dealing with cybersecurity, spam, and privacy.

Thanks are due to the team of curators working on the *GIP Digital Watch* observatory, who contributed to updating various parts of the 2016 edition: Radek Bejdak, Stephanie Borg Psaila, Katharina Höne, Tereza Horejsova, Arvin Kamberi, Aida Mahmutović, Adriana Minović, Virginia Paque, Roxana Radu, Vladimir Radunović, Barbara Rosen Jacobson, and Sorina Teleanu. Stefano Baldi, Eduardo Gelbstein†, and Vladimir Radunović all contributed significantly to developing the concepts behind the illustrations in the book. Comments and suggestions from other colleagues are acknowledged in the text.

An Introduction to

INTERNET GOVERNANCE

Jovan Kurbalija

Published by DiploFoundation (2016)

Malta: DiploFoundation
Anutruf, Ground Floor
Hriereb Street
Msida, MSD 1675, Malta

Switzerland: DiploFoundation
7bis, Avenue de la Paix
CH-1211 Geneva, Switzerland

Serbia: DiploCentar
Braničevska 12a/12
11000 Belgrade, Serbia

E-mail: diplo@diplomacy.edu
Website: www.diplomacy.edu

Design and layout: Viktor Mijatović
Editing: Mary Murphy
Illustrations: Dr Vladimir Veljasević
Prepress : Aleksandar Nedeljkov

Except where otherwise noted, this work is licensed under **http://creativecommons.org/licences/by-nc-nd/3.0/**

The translation and publication of this book in other languages is encouraged.
For more information, please contact **diplo@diplomacy.edu**

Any reference to a particular product in this book serves merely as an example and should not be considered an endorsement or recommendation of the product itself.

The square icons and the links at the end of various sub-sections of the book indicate that there is more background material (ongoing developments, actors, events, instruments, and resources) available online, in the *GIP Digital Watch* observatory.

ISBN: 978-99932-53-30-3

DiPLO
www.diplomacy.edu

Contents

Foreword

In 2004, when I told my friends what I was doing as a member of WGIG – the Working Group on Internet Governance – they often called on me to fix their printers or install new software on their computers. As far as they were concerned, I was doing something related to computers. I remember taking a quick poll of my fellow WGIG members asking them how they explained to their friends, partners, and children what they were doing. Like me, they too were having difficulty. This is one of the reasons I started designing and preparing Diplo's first text and drawings related to Internet governance.

Today, 12 years later, the same people who asked me to install their printers are coming back to me with questions about how to keep ownership of their data on Facebook or how to ensure their children can navigate the Internet safely. Increasingly, they are concerned about a possible cyberwar and the online risks for water supply, power plants, and other critical infrastructure in their cities and countries. How far we all have come!

Internet governance is moving increasingly into the public eye. The more modern society depends on the Internet, the more relevant Internet governance will be. Far from being the remit of some select few, Internet governance concerns all of us to a lesser or greater extent, whether we are one of the 3.6 billion using the Internet or a non-user who depends on the facilities it services.

Internet governance is obviously more relevant for those who are deeply integrated in the e-world, whether through e-business or networking on Facebook. Yet it has a broad reach. Government officials, military personnel, lawyers, diplomats, and others who are involved in either providing public goods or preserving public stability are also concerned. Internet governance, and in particular the protection of privacy and other human rights, is a focal point for civil society activists and non-governmental organisations. For innovators worldwide, Internet governance must ensure that the Internet remains open for development and innovation. Creative inventors of tomorrow's Google, Skype, Facebook, and Twitter are out there, somewhere, browsing the Internet. Whether they will benefit from equal opportunities to develop new, more creative ways to use the Internet is currently debated in heated net neutrality discussions, but also in intellectual property forums. It is no longer easy to separate some of these discussions from their wide-ranging implications across sectors and stakeholders.

It is my hope that this book provides a clear and accessible introduction to Internet governance. For some of you, it will be your first encounter with the subject. For others, it may serve as a reminder that what you are already doing in your area of specialisation – be it e-health, e-commerce, e-governance, e-whatever – is part of the broader family of Internet governance issues.

The underlying objective of such a diverse approach is to modestly contribute to preserving the Internet as a great enabler for billions of people worldwide. At the very least, I hope it whets your appetite and encourages you to delve deeper into this remarkable and fluent subject. Stay current. Follow developments on http://www.diplomacy.edu/capacity/IG and http://www.diplomacy.edu/ig

Jovan Kurbalija
Director of DiploFoundation
Head of the Geneva Internet Platform
November 2016

Section 1

INTRODUCTION

Although Internet governance deals with the core of the digital world, governance cannot be handled with a digital-binary logic of true/false and good/bad. Instead, Internet governance demands many subtleties and shades of meaning and perception; it thus requires an analogue approach, covering a continuum of options, trade-offs, and compromises.

Therefore, this book does not attempt to provide definite statements on Internet governance issues. Rather, its aim is to propose a practical framework for analysis, discussion, and resolution of significant issues in the field.

Introduction

The controversy surrounding Internet governance starts with its definition. It is not merely linguistic pedantry. The way the Internet is defined reflects different perspectives, approaches, and policy interests. Typically, telecommunications specialists see Internet governance through the prism of the development of a technical infrastructure. Computer specialists focus on the development of different standards and applications, such as XML (eXtensible Markup Language) or Java. Communication specialists stress the facilitation of communication. Human rights activists view Internet governance from the perspective of freedom of expression, privacy, and other fundamental human rights. Lawyers concentrate on jurisdiction and dispute resolution. Politicians worldwide usually focus on issues that resonate with their electorates, such as techno-optimism (more computers = more education) and threats (cybersecurity, cybercrime, child protection). Diplomats are mainly concerned with the process and protection of national interests. The list of potentially conflicting professional perspectives of Internet governance goes on.

What does Internet governance mean?

The World Summit on the Information Society (WSIS)[1] came up with the following working definition of Internet governance:

> *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.*[2]

'I'nternet or 'i'nternet and diplomatic signalling

Back in 2003, *The Economist* magazine started writing Internet with a lowercase 'i'. The same approach was later followed by other magazines, such as *Associated Press* and *The New York Times*. This change in editorial policy was inspired by the fact that the Internet had become an everyday item, no longer unique and special enough to warrant an initial capital. The word 'Internet' followed the linguistic destiny of (t)elegraph, (t)elephone, (r)adio, and (t)elevison, and other such inventions.

The question of writing Internet/internet with an upper or lowercase 'i' was discussed at the International Telecommunication Union (ITU) Conference in Antalya (November 2006), where a political dimension was introduced when the term 'Internet' appeared in the ITU resolution on Internet governance with a lowercase 'i' instead of the usual, uppercase 'I'. David Gross, US Ambassador and Coordinator for International Communications and Information Policy, expressed concern that the ITU lowercase spelling might signal an intention to treat the Internet like other telecommunications systems internationally governed by the ITU. Some interpreted this as a diplomatic signal of the ITU's intention to play a more prominent role in Internet governance.[3]

This rather broad working definition does not resolve the question of different interpretations of two key terms: 'Internet' and 'governance'.

Internet

The term 'Internet' does not cover all of the existing aspects of global digital developments. Two other terms – information society and information and communication technology (ICT) – are usually put forward as more comprehensive. They include areas that are beyond the Internet domain, such as mobile telephony. The argument for the use of the term 'Internet', however, is enhanced by the rapid transition of global communication towards the use of Internet protocol (IP) as the main communications technical standard. The already ubiquitous Internet continues to expand at a rapid rate, not only in terms of the number of users but also in terms of the services that it offers; the so-called over-the-top (OTT) services, such as voice-over Internet protocol (VoIP) or Internet protocol television (IPTV), are now more and more widespread, and are increasingly seen as competitors to conventional services like telephony and television.

Governance

In the Internet governance debate, controversy arose over the term 'governance' and its various interpretations. According to one interpretation, governance is synonymous with government. In the early WSIS process, many national delegations had this initial understanding, leading to the interpretation that Internet governance should be the business of governments and consequently addressed at intergovernmental level with the limited participation of other, mainly non-state actors.

There is further confusion if we look at how the term 'governance' is used by some international organisations. For example, the term 'good governance' has been used by the World Bank to promote the reform of states by introducing more transparency, reducing corruption, and increasing the efficiency of administration. In this context, the term 'governance' is directly related to core government functions.

These interpretations clashed with a broader meaning of the term 'governance', which includes the governance of affairs of any institution, including non-governmental ones. This was the meaning accepted by the Internet community, since it describes the way in which the Internet has been governed since its early days.

The terminological confusion is further complicated by the translation of the term 'governance' into other languages. In Spanish, the term refers primarily to public activities or government (*gestión pública, gestión del sector público,* and *función de gobierno*). The reference to public activities or government also appears in French (*gestion des affaires publiques, efficacité de l'administration, qualité de l'administration,* and *mode de gouvernement*). Portuguese follows a similar pattern when referring to the public sector and government (*gestão pública* and *administração pública*).

The evolution of Internet governance

Early Internet governance (1970s–1994)

The Internet started as a government project. In the late 1960s, the US government sponsored the development of the Advanced Research Projects Agency Network (ARPANet), a network aimed to facilitate the sharing of digital resources among computers. By the mid-1970s, with the invention of TCP/IP (Transmission Control Protocol/Internet Protocol), this network evolved into what is known today as the Internet.

One of the key principles of the Internet is its distributed nature: data packets can take different paths through the network, avoiding traditional barriers and control mechanisms. This technological principle was matched by a similar approach to regulating the Internet at its early stages. The Internet Engineering Task Force (IETF), established in 1986, managed the further development of the Internet through a cooperative, consensus-based, decision-making process, involving a wide variety of individuals. There was no central government, no central planning, no grand design.

This led many people to think that the Internet was somehow unique and that it could bring an alternative to the politics of the modern world. In his famous Declaration of the Independence of Cyberspace, American cyberlibertarian political activist John Perry Barlow states:

> *[the Internet] is inherently extra-national, inherently anti-sovereign and your [states'] sovereignty cannot apply to us. We've got to figure things out ourselves.*[4]

The DNS war (1994–1998)

This decentralised approach to Internet governance soon began to change as governments and the business sector realised the importance of the global network. In 1994, the US National Science Foundation, which managed the key infrastructure of the Internet, decided to subcontract the management of the Domain Name System (DNS) to a private US company called Network Solutions Inc. (NSI). This was not well received by the Internet community and led to the so-called DNS war.

This war brought new players into the picture: international organisations and nation states. It ended in 1998 with the establishment of a new organisation, the Internet Corporation for Assigned Names and Numbers (ICANN), which became the coordinator of the main Internet technical resources, on the basis of a contract with the US government. ICANN subsequently became the focus of many Internet governance debates.

World Summit on the Information Society (2003–2005)

WSIS, held in Geneva (2003) and Tunis (2005), officially placed the question of Internet governance on diplomatic agendas. The focus of the Geneva phase of the summit, preceded by a number of preparatory committees (PrepComs) and regional meetings, was rather broad, with a range of issues related to ICT put forward by participants. In fact, during the first preparatory and regional meetings, the term 'Internet governance' was not used.[5]

Internet governance was introduced to the WSIS process during the West Asia regional meeting in February 2003; after the Geneva summit, it became the key issue of the WSIS negotiations.

After prolonged negotiations and last-minute arrangements, the WSIS Geneva summit in 2003 agreed to establish the Working Group on Internet Governance (WGIG), which prepared a report[6] used as the basis for negotiations at the second WSIS meeting held in Tunis (November 2005). The WSIS Tunis Agenda for the Information Society elaborated on the question of Internet governance, including adopting the definition proposed by WGIG, listing Internet governance issues, and establishing the Internet Governance Forum (IGF), a multistakeholder body convoked by the UN Secretary General to function as a space for discussions on public policy issues related to key elements of Internet governance.[7]

Developments in 2006

After the Tunis summit, three main developments and events marked the Internet governance debate in 2006. First was the expiration of the existing memorandum of understanding (MoU) and the establishment of a new one between ICANN and the US Department of Commerce. Some had hoped that this event would change the relationship between ICANN and the US government, and that the former would become a new type of international organisation. However, while the new MoU thinned the umbilical cord between ICANN and the US government, it maintained the possibility of the eventual internationalisation of ICANN's status.

The second event of 2006 was the IGF in Athens, Greece. It was the first such forum and, in many respects, it was an experiment in multilateral diplomacy. It was truly multistakeholder. All players – states, businesses, academic and technical communities, and civil society – participated on an equal footing. It also had an interesting organisational structure for its main events and workshops. Journalists moderated the discussions and the IGF therefore differed from the usual UN-style meeting format. However, some critics claimed that the IGF was only a talk show without any tangible results in the form of a final document or plan of action.

The third main development in 2006 was the ITU Plenipotentiary Conference held in Antalya, Turkey, in November. A new ITU Secretary-General, Dr Hamadoun Touré, was elected. He announced a stronger focus on cybersecurity and development assistance. It was also expected that he would introduce new modalities to the ITU's approach to Internet governance.

Developments in 2007

In 2007, the ICANN discussion focused on the .xxx domain (for adult materials), re-opening debates on numerous governance points, including whether ICANN should deal only with technical problems or also with issues relevant to public policy.[8] Interventions by the US and other governments in this context further raised the question of how national governments should become involved in ICANN deliberations.

At the second IGF, held in November in Rio de Janeiro, Brazil, the main development was the adding of critical Internet resources (CIR) (names and numbers) to the IGF agenda.

Developments in 2008

The major development of 2008, which will continue to influence Internet governance as well as other policy spheres, was the election of Barack Obama as US President. During his presidential election campaign, Obama used the Internet and Web 2.0 tools intensively. Some even argue that this was one of the reasons for his success. His advisors included many people from the Internet industry, including the CEO of Google. In addition to his techno-awareness, President Obama supported multilateralism which inevitably influenced discussions on the internationalisation of ICANN and the development of the Internet governance regime.

In 2008, net neutrality[9] emerged as one of the most important Internet governance issues. It was primarily discussed in the USA between two main opposing blocks. It even featured in the US presidential campaign, supported by President Obama. Net neutrality is mainly supported by the so-called Internet industry, including companies such as Google, Yahoo!, and Facebook. A change in the architecture of the Internet triggered by a breach in net neutrality might endanger their business. On the other side sit telecommunications companies, such as Verizon and AT&T, Internet service providers (ISPs), and the multimedia industry. For different reasons, these industries would like to see some sort of differentiation between packets travelling on the Internet.

Refer to Section 2 for further discussion on net neutrality.

Another major development was the fast growth of Facebook and social networking. When it comes to Internet governance, the increased use of Web 2.0 tools opened up the issue of privacy and data protection on social media platforms.

Developments in 2009

The first part of 2009 saw the Washington Belt trying to figure out the implications and future directions of President Obama's Internet-related policy. Obama's appointments to key Internet-related positions did not bring any major surprises. They followed his support for an open Internet. His team also pushed for the implementation of the principle of net neutrality in accordance with promises made during his election campaign.

The highlight of 2009 was the conclusion of the Affirmation of Commitments between ICANN and the US Department of Commerce, which was intended to make ICANN a more independent organisation. While this move represented a step forward in addressing one problem in Internet governance – the US supervisory role of ICANN – it opened many new issues, such as the international position of ICANN and the further supervision of ICANN's activities. The Affirmation of Commitments provided guidelines, but left many issues to be addressed in the forthcoming years.

In November 2009, the fourth IGF was held in Sharm el Sheikh, Egypt. The main theme was the IGF's future in view of the 2010 review of the IGF mandate. In their submissions, stakeholders took a wide range of views on the future of the IGF. While most of them supported the continuation of the IGF, there were major differences of opinion as to how the future IGF should be organised. China and many developing countries argued for the stronger anchoring of the IGF in the UN system, which would imply a more prominent role for governments. The USA, most developed countries, the business sector, and civil society argued for the preservation of the existing IGF model.

Developments in 2010

The main development in 2010 was the impact of fast-growing social media on the Internet governance debate, including the protection of privacy of users of social media platforms such as Facebook. In 2010, the main development in Internet geopolitics was US Secretary of State Hillary Clinton's speech on freedom of expression on the Internet, in particular in relation to China.[10] Google and Chinese authorities conflicted over the restricted access to Google-search in China. The conflict led to the closing of Google's search operations in the country.

There were two important developments in the ICANN world: (1) The introduction of the first non-ASCII top-level domains for Arabic and Chinese. By solving the problem of the availability of top-level domains in scripts other than Latin, ICANN reduced the risk of disintegration of the Internet DNS. (2) ICANN's approval of the .xxx domain (adult materials). With this decision ICANN formally crossed the Rubicon by officially adopting a decision of high relevance for public policy on the Internet. Previously, ICANN had tried to stay, at least formally, within the realm of technical decision-making only.

The IGF review process started in 2010 with the UN Commission on Science and Technology for Development (CSTD) adopting the resolution on the continuation of the IGF, which suggested continuation for the next five years, with only minor changes in its organisation and structure. In July 2010, the UN Economic and Social Council (ECOSOC) endorsed this resolution, and the final decision on the continuation of the IGF was taken by the UN General Assembly (UNGA) in the autumn.

Developments in 2011

In 2011, the main general development was the rise of Internet governance on the global politics agenda. The relevance of Internet governance moved closer to other diplomatic issues such as climate change, migration, and food security. Another consequence of the growing political relevance of the Internet is the gradual shift of national coverage of Internet governance issues from technology (IT, telecoms) to political ministries (diplomacy, prime ministerial cabinets). In addition, the main global media (e.g. *The Economist, IHT, Al Jazeera, BBC*) were now following Internet governance developments more closely than ever before.

Internet governance was affected by the Arab Spring. Although there are very different views on the impact of the Internet on the Arab Spring phenomenon (ranging from minimal to key), one outcome is certain: social media is now perceived as a tool that can be decisive in modern political life. In various ways, the Internet – and its governance – popped up on political radars worldwide this year.

On 27 January, Egyptian authorities cut the Internet in the vain hope of stopping political protests. This was the first example of a complete countrywide Internet blackout ordered by the government. Previously, even in the case of military conflicts (former Yugoslavia, Iraq), Internet communication had never been completely severed.

Hillary Clinton's initiative on freedom of expression on the Internet, initiated by her speech in February 2010, was accelerated in 2011. There were two major conferences on this subject: the Vienna Conference on Human Rights and the Internet, and The Hague Conference on Internet and Freedom.

In 2011, ICANN continued its soul-searching with the following main developments:

- Implementation of management reform.
- Final policy preparations for the introduction of new generic top-level domains (gTLDs).
- The search for a new CEO.

2011 was also marked by the avalanche of Internet governance principles which were proposed by the Organisation for Economic Co-operation and Development (OECD), the Council of Europe (CoE), the EU, Brazil, and other players. The numerous convergences of these principles were seen as a possible starting position of a future preamble of a global Internet declaration or a similar document that could serve as a framework for Internet governance development.

Developments in 2012

Two major events marked the 2012 agenda with important consequences for the years to come: the ICANN leadership change, and the revision of the ITU's International Telecommunication Regulations (ITRs).

ICANN had gone through significant developments over the previous year with the introduction of new gTLDs. Despite some problems with the registration process (software glitches, controversies over the policy process), over 1900 applications for new gTLDs were received and entered into an evaluation process that eventually decided which gTLDs would be introduced to the root starting in 2014. Moreover, the new CEO, Fadi Chehadé, brought a new approach to the steering of the ICANN multistakeholder policy processes. In his speech to civil society at the ICANN 45 meeting, he outlined some promising improvements at ICANN, including development of responsible multistakeholderism, frank recognition of problems, active listening, empathetic guidance, search for compromise, etc.

The World Conference on International Telecommunications (WCIT) converged in Dubai in December 2012 to amend the ITRs for the first time since 1988; it caught the spotlight throughout the year and raised concerns about and debate on the impact of a new regulation on the future of the Internet. At the end of an exhausting two-week conference, negotiations ended in a stalemate: participants had failed to reach a consensus on the amended text, leaving the debate open for upcoming meetings. The main contentious point was a non-binding resolution on fostering the role of the ITU in Internet governance, which polarised participating states into two blocks: western countries favouring the current multistakeholder model, with supporters of the resolution, including states like China, Russia, and Arab countries, leaning towards an intergovernmental model.

Other notable developments were registered in the intellectual property rights (IPR) area, where Internet users' mobilisation and protests managed to block national (Stop Online Piracy Act (SOPA) in the USA) and international (Anti-Counterfeiting Trade Agreement (ACTA)) regulations that would have affected users' legitimate rights through their implementation.

Developments in 2013

The main development in global digital policy was the Snowden revelations of the various surveillance programmes run by the US National Security Agency (NSA) and other agencies. The Snowden revelations made the global public interested in how the Internet is governed. The main focus was on the question of the right to privacy and data protection.

The question of protection of privacy was addressed by many leaders during the UNGA. The UNGA resolution initiated a new policy process on online privacy. The issue would be further discussed in 2014 at the UN Human Rights Council (UNHRC).

In October 2013, Brazilian president Dilma Rousseff and ICANN's President Fadi Chehadé initiated the NETmundial process. Internet governance came into focus at numerous academic conferences and in research activities of think-tanks worldwide.

Developments in 2014

The year 2014 started with US President Obama's speech on NSA surveillance. He repeatedly used the term 'cyber-attacks', placing cybersecurity at the forefront of the security agenda (higher than terrorism).

On 14 March, the National Telecommunications and Information Administration (NTIA) of the US Department of Commerce announced that it intended to transition its stewardship role over key domain name functions to the global multistakeholder community. At that point, the NTIA oversaw the performance of the Internet Assigned Numbers Authority (IANA) functions, which includes maintaining the registries of global IP addresses and domain names, among other critical parameters. The NTIA also authorised changes in the root zone file (a global Internet address book), thereby holding a safety-stop mechanism. The announcement triggered a long process of consultation and consolidation of proposals, originally to be completed by September 2015 but subsequently extended by one year. At the same time, a process aimed at consolidating the accountability mechanisms within ICANN was also launched.

Three discussion forums emerged, two of which were related to ICANN:

- An ICANN-initiated /1net (online) platform to connect various constituencies and feed discussion summaries into other forums, in particular for the NETmundial process. The NETmundial conference (jointly organised by /1net and the Brazilian Internet Steering Committee (CGI.br)) took place on 23 and 24 April in São Paulo. It resulted in the NETmundial Multistakeholder Statement, containing a set of Internet governance principles, as well as a roadmap for the future evolution of the Internet governance ecosystem.

- The High-Level Panel on Global Internet Cooperation and Governance Mechanisms (GICGM), was formed through a partnership between ICANN and the World Economic Forum (WEF), with assistance from The Annenberg Retreat at Sunnylands. The panel produced a report titled Towards a Collaborative, Decentralized Internet Governance Ecosystem, which outlines a set of recommendations for the advancements of a collaborative and decentralised Internet governance ecosystem.

- The Global Commission on Internet Governance, which was launched by the Canadian Centre for International Governance Innovation and UK-based think-thank Chatham House with the aim of advancing a strategic vision for the future of Internet governance.

The 'right to be forgotten' was introduced on 3 May by the Court of Justice of the European Union (CJEU), which ruled that Google must remove links to 'outdated', 'excessive', and 'irrelevant' personal data when a request is made by an individual related to the search results displayed under their name.

Developments in 2015

Throughout the year, the IANA stewardship transition and ICANN accountability stayed in focus as the process was extended to September 2016. Cybersecurity remained high on the agenda, for both security breaches and policy responses. After concluding earlier in 2013 that existing international law applies to the use of ICT by states, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) agreed on several norms, including no attacking of critical infrastructure or Computer Emergency Response Teams (CERTs), and assisting other nations in investigating cyber-attacks and cybercrime in their territories.

In July, as part of the sustainable development goals (SDGs) process, the UN established a new Technology Facilitation Mechanism,[11] which included a UN inter-agency task team on science, technology, and innovation; a multistakeholder forum; and a new online 'mapping' platform. Following UNHRC discussions, a special mechanism for the right to privacy was agreed on and the first Special Rapporteur on Privacy (Professor Joseph Cannataci) was appointed on 3 July.

Summer also marked the start of the WSIS+10 review process, culminating in December with the High-Level Meeting of the General Assembly on the overall review of the implementation of the WSIS outcomes. The outcome document adopted there renewed the mandate of the IGF for another ten years and highlighted the direction of development for the next decade, reiterating the 2005 Tunis Agenda roles and responsibilities of stakeholders.

Within the ICANN community, work continued on the development of the IANA stewardship transition proposal, and the ICANN accountability proposal.

Developments in 2016

The year 2016 started with two reports that raised one fundamental question: How do we maximise the opportunities and minimise the risks that the Internet brings about? The World Bank's World Development Report 2016: Digital Dividends[12] argued that the Internet does not automatically bring about benefits for society. Policy, education, and much more are needed in order to ensure that the Internet has a positive impact on society. WEF issued a more cautionary report on Internet fragmentation, outlining risks that exist for the global Internet (in the form of technical, governmental, and commercial fragmentation).[13]

A controversy between Apple and the US Federal Bureau of Investigation (FBI) stayed in the headlines for several months throughout 2016, as a court order was issued asking Apple to assist the FBI in breaking into an iPhone belonging to one of the terrorists who killed 14 people in San Bernardino, California, in December 2015. The debate brought back into the digital realm the old question of balancing security and human rights. Although the case was dropped in the end (as the US government argued it had benefitted from the assistance of a third party to break into the phone), issues related to encryption, privacy, and security continued to remain in focus over the year.

In June 2016, the Global Commission on Internet Governance published the One Internet report, which outlines a series of recommendations to policymakers, private industry, the technical community, and other stakeholders on modalities for maintaining a healthy Internet. It tackles aspects such as promoting a safe, open and secure Internet; securing human rights for digital citizens; identifying the responsibilities of the private sector; safeguarding the stability and resiliency of the Internet's core infrastructure; and improving multistakeholder Internet governance.[14]

On the ICANN side, the first half of the year was marked by the submission, to the US government, of the IANA stewardship transition proposal and the ICANN accountability proposal. After reviewing the two proposals, the NTIA acknowledged, in August 2016, that they met the criteria announced in March 2014. As such, ICANN moved forward with implementing the provisions of the two proposals, notably the creation of Public Technical Identifiers (PTI), as a subsidiary of ICANN, tasked to take over the performance of the IANA functions, and the empowerment of the ICANN community through the inclusion, in ICANN's bylaws, of a number of provisions giving the community more powers to hold ICANN (staff and Board) accountable for its actions. On 1 October, the IANA functions contract between the US government and ICANN expired, allowing the stewardship of the IANA functions to transition to the global Internet community.

Prefixes: *e- / virtual / cyber / digital / net*

The prefixes *e- / virtual / cyber / digital / net* are used to describe various ICT/Internet developments. Typically, they are used interchangeably. Each prefix describes the Internet phenomenon.

Yet, we tend to use e- for commerce, cyber for crime and security, digital for development divides, and virtual for currencies, such as Bitcoin. Usage patterns have started to emerge. While in our everyday language, the choice of prefixes *e-/virtual/cyber/digital/net* is casual, in Internet policy the use of prefixes has started to attract more meaning and relevance.

Let's have a quick look at the etymology of these terms and the way they are used in Internet policy.

The etymology of 'cyber' goes back to the Ancient Greek meaning of 'governing'. Cyber came to our time via Norbert Weiner's book *Cybernetics*, dealing with information-driven governance.[15] In 1984, William Gibson coined the word cyberspace in the science-fiction novel *Neuromancer*.[16] The growth in the use of the prefix 'cyber' followed the growth of the Internet. In the late 1990s, almost anything related

to the Internet was 'cyber': cybercommunity, cyberlaw, cybersex, cybercrime, cyberculture, cyber… If you named anything on the Internet and you had 'cyber'. In the early 2000s, cyber gradually disappeared from wider use, only remaining alive in security terminology.

Cyber was used to name the 2001 Council of Europe Cybercrime Convention. It is still the only international treaty in the field of Internet security. Today there is the USA's Cyberspace Strategy, the ITU's Global Cybersecurity Agenda, the North Atlantic Treaty Organization (NATO) Policy on Cyber Defence, Estonia's Cyber Defence Center of Excellence ...

Cyberpunk author and *Wired* columnist Bruce Sterling had this to say:

> *I think I know why the military calls it 'cyber' — it's because the metaphor of defending a 'battlespace' made of 'cyberspace' makes it easier for certain contractors to get Pentagon grants. If you call 'cyberspace' by the alternate paradigm of 'networks, wires, tubes and cables' then the NSA has already owned that for fifty years and the armed services can't get a word in.*[17]

'E' is the abbreviation for 'electronic'. It got its first and most important use through e-commerce, as a description of the early commercialisation of the Internet. In the EU's Lisbon Agenda (2000), e- was the most frequently used prefix. E- was also the main prefix in the WSIS declarations (Geneva 2003; Tunis 2005). The WSIS follow-up implementation is centred on action lines including e-government, e-business, e-learning, e-health, e-employment, e-agriculture, and e-science. Nonetheless, e- is not as present as it used to be. Even the EU has been distancing itself from using e- recently.

Today, the EU works on implementing a Digital Single Market Strategy.[18] Digital refers to '1' and '0' – two digits which are the basis of whole Internet world. Ultimately, all software programs start with them. In the past, digital was used mainly in development circles to represent the digital divide. During the last few years, digital has started conquering Internet linguistic space. It is likely to remain the main Internet prefix. Jean-Claude Juncker, President of the European Commission, used the 'digital' prefix 10 times in his initial speech at the European Parliament, presenting his policy plan for the five-year mandate. In addition to the EU, Great Britain now has digital diplomacy, and an increasing number of diplomatic missions have a dedicated person for digital issues, usually covering them transversally.

Virtual relates to the intangible nature of the Internet. Virtual introduces the ambiguity of being both intangible and, potentially, non-existent. Virtual reality could be both an intangible reality, (something that cannot be touched) and a reality that does not exist (a false reality). Academics and Internet pioneers used virtual to highlight the novelty of the Internet, and the emergence of 'a brave new world'. Virtual, because of its ambiguous meaning, rarely appears in policy language and international documents.

Today, there is truce in the war for prefix dominance. Each prefix has carved its own domain, without a catch-all domination which, for example, cyber had in the late 1990s. Today, cyber preserves its dominance in security matters. E- is still the preferred prefix for business. Digital has evolved from development issue use to wider use by the government sector. Virtual has been virtually abandoned.

The Internet Governance Cognitive Toolkit

Profound truths are recognised by the fact that the opposite is also a profound truth, in contrast to trivialities where opposites are obviously absurd.

Niels Bohr, Atomic Physicist (1885–1962)

The Internet Governance Cognitive Toolkit is a set of tools for developing and understanding policy argumentation. The core of the toolkit is a reference framework which includes perceptions of cause-and-effect relationships, modes of reasoning, values, terminology, and jargon. This reference framework shapes how particular issues are framed and what actions are taken.

In many cases, the common reference framework is influenced by the specific professional culture (the patterns of knowledge and behaviour shared by members of the same profession, e.g. diplomats, academics, software developers). The existence of such a framework usually helps in facilitating better communication and understanding. It can also be used to protect professional turf and prevent outside influence. To quote American linguist, Jeffrey Mirel: 'All professional language is turf language.'[19]

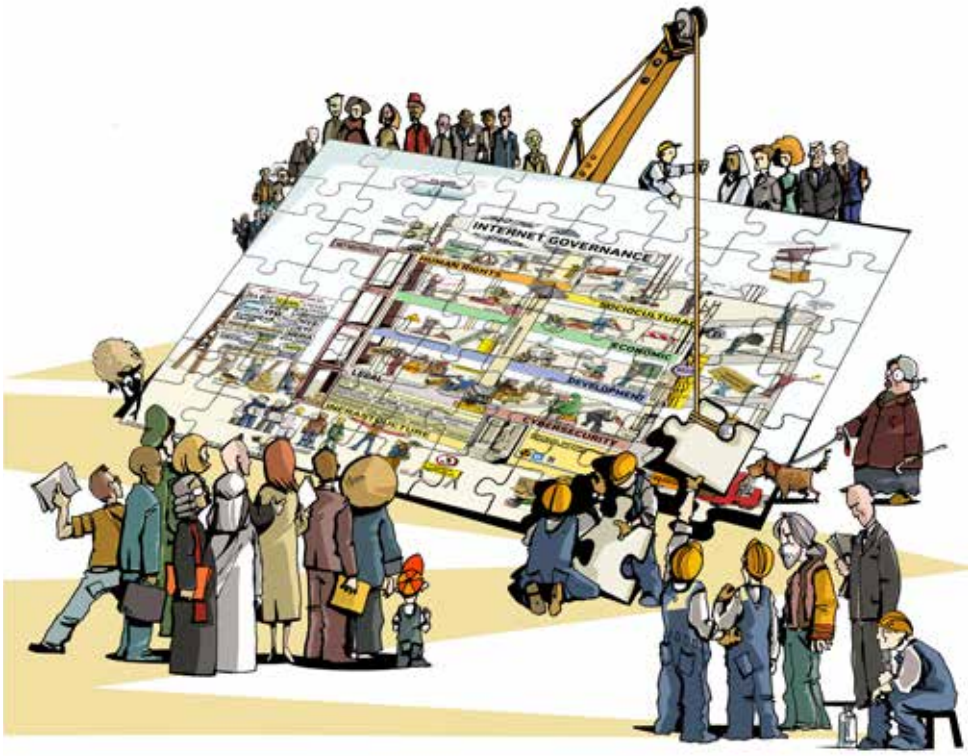

Figure 1. Internet governance puzzle

The Internet governance regime is complex as it involves many issues, actors, mechanisms, procedures, and instruments. Figure 1, inspired by Dutch artist MC Escher, demonstrates some of the paradoxical perspectives associated with Internet governance.

The toolkit reflects the nature of Internet governance, as a so-called wicked policy area, characterised by the difficulty encountered in assigning causation for policy development to one specific reason. In many cases, every problem is a symptom of another problem, sometimes creating vicious circles. Certain cognitive approaches, such as linear, mono-causal, and either/or thinking, have a very limited utility in the field of Internet governance. Internet governance is too complex to be strapped inside a corset of coherence, non-contradiction, and consistency. Flexibility, and being open and prepared for the unexpected, might be the better part of Internet.[20]

Like the Internet governance process, the toolkit is also in flux. Approaches, patterns, and analogies emerge and disappear depending on their current relevance in the policy process. They support specific policy narratives in the Internet governance debate.

Policy approaches

The first section of the Internet Governance Cognitive Toolkit describes a number of policy approaches that underpin the positions of the main Internet governance actors. These policy approaches also explain the framing of negotiation positions and policy debates.

Narrow vs broad approach

The narrow approach focuses on the Internet infrastructure (DNS, IP numbers, and root servers) and on ICANN's position as the key actor in this field. According to the broad approach, Internet governance negotiations should go beyond infrastructural issues and address legal, economic, developmental, and sociocultural issues. This latter approach is adopted in the WGIG report and the Tunis Agenda for the Information Society. It is also used as the underlying principle of IGF architecture.

However, there is a tendency to consider cybersecurity and e-commerce as separate policy fields from Internet governance. For example, the 2015 WSIS+10 review document[21] addressed Internet governance and cybersecurity in separate chapters. Framing of the digital policy debate is far beyond simple academic pedantry. If issues are addressed in policy silos (e.g. security, human rights, e-commerce), this may affect the effectiveness of addressing Internet policy issues which are by their nature multi-disciplinary. Many actors, from governments to international organisations and the business sector, face the problem of how to move beyond silos and address Internet policy issues in a broad and multidisciplinary way.

Technical and policy coherence

A significant challenge facing the Internet governance process has been to deal with technical and policy aspects, as it is difficult to draw a clear distinction between the two. Technical solutions are not neutral. Ultimately, each technical solution/option promotes certain interests, empowers certain groups, and, to a certain extent, impacts social, politi-

cal, and economic life. In the case of the Internet, for a long time both the technical and the policy aspects were governed by just one social group – the early Internet technical community.

With the growth of the Internet and the emergence of new Internet governance actors – mainly the business sector and governments – it was difficult for the Internet technical community to maintain an integrated coverage of technical and policy issues under one roof. Subsequent reforms, including the creation of ICANN, tried to re-establish coherence between technical and policy aspects. This issue remains open, and as expected, has shown to be one of the controversial topics in the debate on the future of Internet governance.

'Old-real' vs 'new-cyber' approach

There are two approaches to almost every Internet governance issue (Figure 2). The 'old-real' approach argues that the Internet has not introduced anything new to the field of governance. The Internet is just another new device, from the governance perspective, no different from its predecessors: the telegraph, the telephone, and the radio.

For example, in legal discussions, this approach argues that existing laws can be applied to the Internet with only minor adjustments. In the economic field, this approach argues that there is no difference between regular commerce and e-commerce. Consequently, there is no need for special legal treatment of e-commerce.

The 'new-cyber' approach argues that the Internet is a fundamentally different communication system from all previous ones. The main premise of the cyber approach is that the

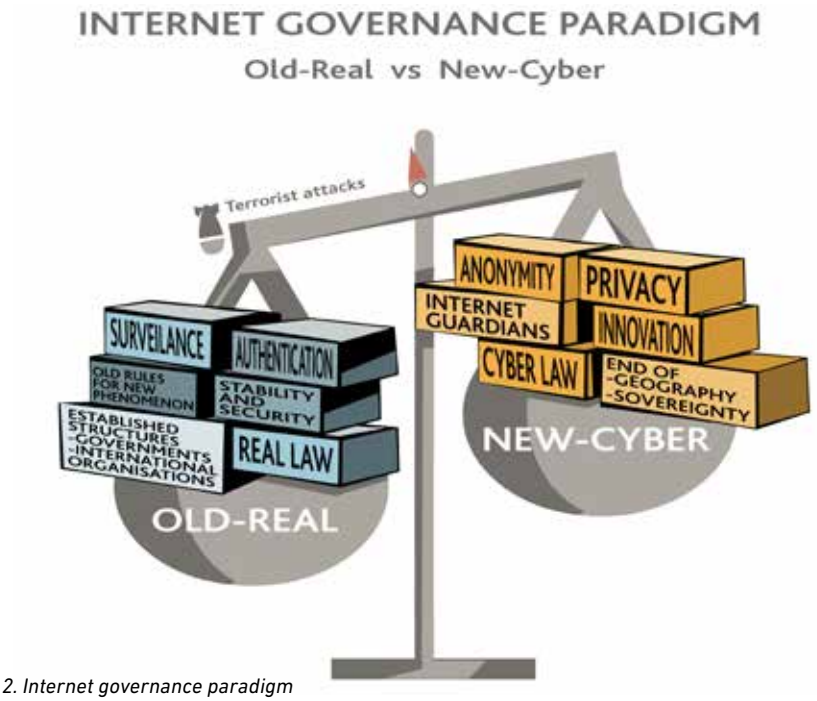

Figure 2. Internet governance paradigm

Internet has managed to de-link our social and political reality from the physical world defined by geographically separated sovereign states territories. Cyberspace is different from real space and requires a different form of governance. A view that cyberspace is a new and different space is supported by the decision taken by NATO at its 2016 Warsaw Summit to declare cyberspace as the fourth military operational domain, in addition to land, water, and air.[22]

In the legal field, the cyber school of thought argues that existing laws on jurisdiction, crime, and contracts cannot be applied to the Internet and that new laws must be created. Increasingly, the old-real approach is becoming more prominent in both regulatory work and the policy field. The UN GGE reaffirmed the view that existing international law applies to the use of ICT by states. In addition, numerous UN human rights conventions have accepted the principle that human rights offline apply online.

Decentralised vs centralised structure of Internet governance

According to the decentralised view, Internet governance should reflect the very nature of the Internet: a network of networks. This view underlines that the Internet is so complex it cannot be placed under a single governance umbrella, such as an intergovernmental organisation, and that decentralised governance is one of the major factors allowing fast Internet growth. This view is mainly supported by the Internet technical community and by developed countries.

The centralised approach argues for a one-stop shop to address Internet governance issues, preferably within the framework of an international organisation. One of the main motivations for a more centralised approach is the difficulty of countries with limited human and financial resources to follow Internet governance discussions in a highly decentralised and multi-institutional setting. Such countries find it difficult to attend meetings in the main diplomatic centres (Geneva, New York), let alone follow the activities of other institutions, such as ICANN, the World Wide Web Consortium (W3C), and the IETF.

Protection of public interests on the Internet

One of the main strengths of the Internet is its open and public nature, which has enabled its rapid growth and also fosters creativity and inclusiveness. How to protect the public nature of the Internet will remain one of the core issues of the Internet governance debate. This problem is especially complicated given that a substantial part of the core Internet infrastructure – from transcontinental backbones to local area networks – is privately owned. Whether or not private owners can be requested to manage this property in the public interest and which parts of the Internet can be considered a global public good are some of the difficult questions that need to be addressed. For example, the view that the core Internet infrastructure should be considered as a global public resource has been advanced by Dutch researcher Dennis Broeders[23] and Maltese ambassador Dr Alex Sceberras Trigona.[24] The question of the public nature of the Internet has been re-opened through the debate on net neutrality.

Refer to Section 7 for further discussion on global public goods.

Geography and the Internet

One of the early assumptions regarding the Internet was that it overcame national borders and eroded the principle of sovereignty. With Internet communication easily transcending national borders and user anonymity embedded in the very design of the Internet, it seemed to many, to quote the famous Declaration of the Independence of Cyberspace, that governments had 'no moral right to rule us [users]' nor 'any methods of enforcement we have true reason to fear'.

Technological developments of the recent past, however, including more sophisticated geo-location software, increasingly challenge the view of the end of geography in the Internet era. In fact, they mark the return of geography. Internet users are more anchored in geography than in the pre-Internet era. Consequently, the more the Internet is anchored in geography, the less unique its governance is. For example, with the possibility of geographically locating Internet users and transactions, the complex question of jurisdiction on the Internet can be solved through existing laws.

Digital technology and policy uncertainty

Digital technology develops very quickly. New services are introduced almost on a daily basis. This creates additional difficulties in organising the Internet governance debate. For example, in November 2005, when the current Internet governance arrangement was negotiated at WSIS in Tunisia,[25] Twitter did not exist. Today, the use of Twitter has triggered some of the core Internet governance issues, such as protection of privacy and freedom of expression.

The fight against spam is another example of how technology impacts Internet governance. Back in 2005, spam was one of the key governance issues. Today, thanks to highly sophisticated technological filters, spam is a less prominent Internet governance issue.

Thus, some of the current policy problems could be solved in the wake of technological developments.

Policy balancing acts

Balance is probably the most appropriate visualisation of Internet governance and policy debates. On many Internet governance issues, balance has to be established between various interests and approaches. Establishing this balance is very often the basis for compromise. Areas of policy balancing include:

- Freedom of expression vs protection of public order: The well-known debate between Article 19 (freedom of expression) and Article 29 (protection of public order) of the Universal Declaration of Human Rights (UDHR) has been extended to the Internet. It is very often discussed in the context of content control and censorship on the Internet.

- Cybersecurity vs privacy: Like security in real life, cybersecurity may endanger some human rights, such as the right to privacy. The balance between cybersecurity and privacy is in constant flux, depending on the overall global political situation. With ter-

Refer to Section 3 for further discussion on cybersecurity.

rorist attacks leading to the securitisation of the global agenda, the balance has shifted towards cybersecurity.

- Intellectual property: The protection of authors' rights vs fair use of materials is another 'real' law dilemma which has taken a new perspective in the online world.

Refer to Section 4 for further discussion on intellectual property.

Many criticise these balancing pairs, considering them false dilemmas. For example, there are strong arguments that more cybersecurity does not necessarily mean less privacy. There are approaches to enhancing both cybersecurity and privacy. While these views are strongly held, the reality of Internet governance policy is that it is shaped by the search for balancing solutions, through identifying trade-offs among various policy options.

Don't re-invent the wheel

Any initiative in the field of Internet governance should start from existing regulations and/or policies, which can be divided into two broad groups:

- Those invented for the Internet (e.g. ICANN policies regarding the management of Internet names and numbers, net neutrality regulations, policies in the field of the Internet of Things - IoT).

- Existing policies and regulations that require adjustment in order to address Internet--related specificities. The level of adjustment varies from limited adjustments, such as in the field of human rights, to more profound ones in regulating, for example, cyber-currencies and e-taxation.

The use of existing rules would significantly increase legal stability and reduce the complexity of the development of future digital policy regimes.

If it ain't broke, don't fix it

Internet governance must maintain the current functionality and robustness of the Internet and yet remain flexible enough to adopt changes leading to increased functionality and higher legitimacy. General consensus recognises that the stability and functionality of the Internet should be one of the guiding principles of Internet governance.

The stability of the Internet has been preserved through the use of the early Internet approach of 'running code', which involves the gradual introduction of well-tested changes in the technical infrastructure. However, some actors are concerned that the use of the slogan 'if it ain't broke, don't fix it' will provide blanket immunity from any changes in the current Internet governance, including changes not necessarily related to technical infrastructure. One solution is to use this principle as a criterion for the evaluation of specific Internet-governance-related decisions (e g. the introduction of new protocols and changes in decision-making mechanisms).

Promote a holistic approach and prioritisation

A holistic approach should facilitate addressing not only the technical aspects of the Internet, but also its legal, social, economic, developmental, security, and human rights related dimensions. This approach should also take into consideration the increasing convergence of digital technology, with Internet companies moving into telecommunications market (e.g. Google and Facebook deploying submarine cables), and telecom companies providing digital content-related services.

While maintaining a holistic approach to Internet governance negotiations, stakeholders should identify priority issues depending on their particular interests, as branches on the 'tree' of their choice, but without losing sight of the forest of Internet governance issues (Figure 3).

Neither developing nor developed countries are homogenous groups. Among developing countries there are considerable differences in priorities, level of development, and IT-readiness (e.g. between ICT-advanced countries, such as India, China, and Brazil, and some least-developed countries (LDCs) in sub-Saharan Africa).

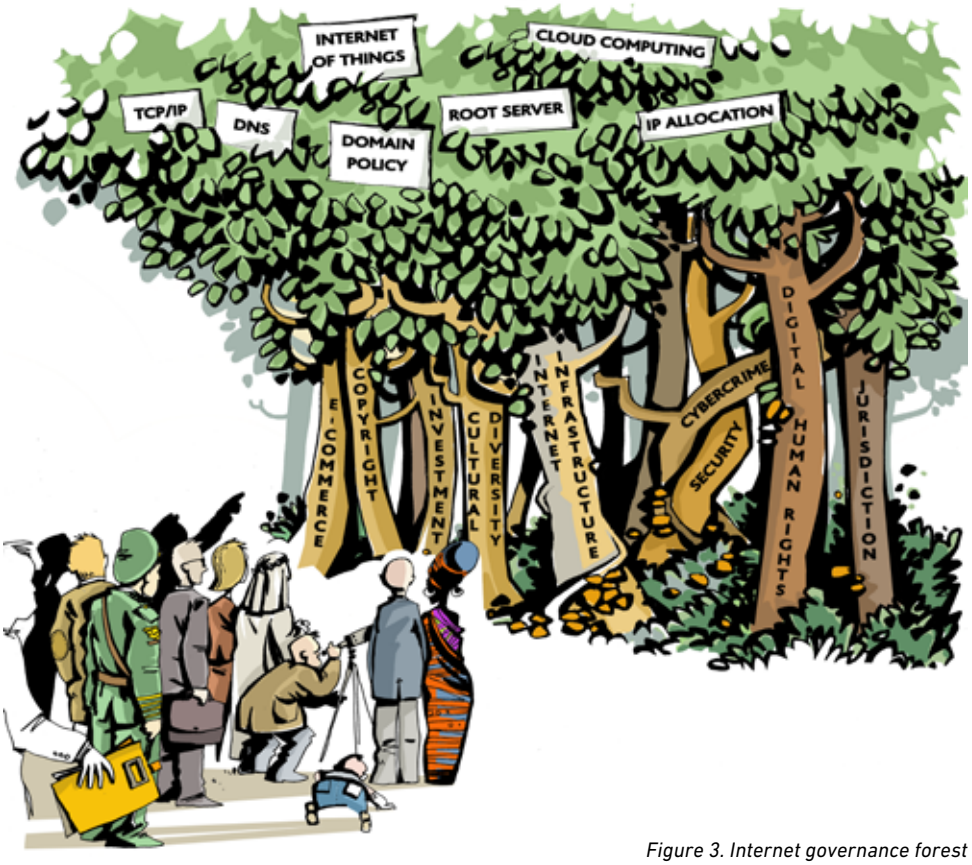

Figure 3. Internet governance forest

A holistic approach and prioritisation of the Internet governance agenda should help stakeholders from both developed and developing countries to focus on a particular set of issues. This should lead towards more substantive and possibly less politicised negotiations. Stakeholders would group around issues rather than around the traditional highly politicised division-lines (e.g. developed–developing countries, governments–civil society).

Technological neutrality

According to the principle of technological neutrality, policy should not be designed for specific technologies or devices. For example, regulations for the protection of privacy should specify what should be protected (e.g. personal data, health records), not how it should be protected (e.g. access to databases, crypto-protection).

Technological neutrality provides many governance advantages. It ensures the continuing relevance of governance regardless of future technological developments and likely convergence of the main technologies (telecommunication, media, the Internet, etc.). Technological neutrality is different from net neutrality: the former indicates that particular policy is independent of the technology which it regulates; the latter focuses mainly on the neutrality of Internet traffic.

Technological solutions as tacit policy

It is a view commonly held within the Internet community that certain social values, such as free communication, are facilitated by the way in which the Internet is technologically designed. For instance, the principle of net neutrality, which says that the network should merely transmit data between two end points without any discrimination of traffic, is often acclaimed as one of the technical safeguards of the freedom of communication on the Internet. This view could lead to the erroneous conclusion that technological solutions are sufficient for promoting and protecting social values. Some other solutions, such as the use of firewall technologies for restricting the flow of information, prove that technology can be used in many, seemingly contradictory, ways. Whenever possible, principles such as free communication should be clearly stated at policy level, not tacitly presumed at the technical level. Technological solutions should strengthen policy principles, but should not be the only way to promote them.

Running society through algorithms

One key aspect of the relationship between technology and policy was identified by American academic Lawrence Lessig, who observed that with its growing reliance on the Internet, modern society may end up being regulated by software code instead of legal rules. Ultimately, some functions of parliament, government, and courts could de facto be taken over by computer companies and software developers. Through a combination of software and technical solutions, they would be able to influence life in increasingly Internet-driven societies. A new set of technologies based on artificial intelligence (AI) are expected to transfer some human decisions to machines. One of the most vivid debates currently is about the future regulation of driverless cars. Modern society will have to identify and deal with the borderline between machines replacing humans in daily activities, and machines moving into the realm of making decisions concerning the political and legal organisation of our society.

Analogies

Though analogy is often misleading, it is the least misleading thing we have.

Samuel Butler, British Poet (1835–1902)

Analogy helps us to understand new developments by referring to what is already known. Drawing parallels between past and current examples, despite its risks, is one of the key cognitive processes in law and politics. Most legal cases concerning the Internet are solved through analogies, especially in the Anglo-Saxon precedent legal system. The use of analogies in Internet governance has a few important limitations.

First, 'Internet' is a broad term, which encompasses a variety of services, including e-mail (analogous to telephony), web services (analogous to broadcasting services – television), databases (analogous to libraries), and social media platforms (analogous to cafés or bazaars). An analogy based on any particular aspect of the Internet may reduce the understanding of the Internet to limited aspects.

Second, with the increasing convergence of different telecommunications and media services, the traditional differences between the various services are blurring. For example, with the introduction of VoIP, it is increasingly difficult to make a clear distinction between the Internet and telephony. In spite of these limiting factors, analogies are still powerful; they are still the main cognitive tool for solving legal cases and developing an Internet governance regime.

Thirdly, analogies were highly important in the early days of the Internet, when it was a new tool and phenomenon. For example, in the first edition of this book (2004), analogies were crucial to explain the Internet. With the growth of the Internet, analogies have become less relevant. Young generations are growing with the Internet. For them, some analogies in this survey (such as videocassette recorders – VCRs) could sound archaic. Analogies, however, remain important as the basis of many Internet court decisions and policies which have been shaping Internet governance. Thus, the following summary of analogies is aimed to serve both as a historical record of the use of analogies in Internet governance, and as a tool for interpreting the roots of current developments in digital policies.

Internet – telephony

Similarities: In the early Internet days, this analogy was influenced by the fact that the telephone was used for dial-up access to the Internet. In addition, a functional analogy holds between the telephone and the Internet (e-mail and chat), both being means for direct and personal communication.

Differences: Analogue telephony used circuits, while the Internet uses packets. Unlike telephony, the Internet cannot guarantee services; it can only guarantee a 'best effort'. The analogy highlights only one aspect of the Internet: communication via e-mail or chat.

Other major Internet applications, such as the World Wide Web, interactive services, etc., do not share common elements with telephony.

Used by: This analogy is used by those who oppose the regulation of Internet content. If the Internet is analogous to the telephone, the content of Internet communications cannot be legally controlled, unlike – for example – broadcasting. It is also used by those who argue that the Internet should be governed like other communications systems (e.g. telephony, post), by national authorities, with a coordinating role of international organisations, such as the ITU. According to this analogy, the Internet DNS should be organised and managed like the telephony numbering system.[26]

A new twist in the complex analogy was created by VoIP services (e.g. Skype) which perform the function of the telephone while using Internet protocol numbers. This dichotomy triggered a policy controversy at WCIT-12 in Dubai. The current view that VoIP is an Internet service is challenged by those who argue that it should be regulated like telephone service on both national and international levels, including a more prominent role for the ITU.

Internet – mail/post

Similarities: This analogy is based on a common function, namely the delivery of messages. The name itself, e-mail, highlights this similarity.

Differences: This analogy covers only one Internet service: e-mail. Moreover, the postal service has a much more elaborate intermediary structure between the sender and the recipient than the e-mail system, where the active intermediary function is performed by ISPs or an e-mail service provider like Yahoo! or Hotmail.

Used by: The Universal Postal Convention describes e-mail as: 'a postal service involving the electronic transmission of "messages"'. This analogy can have consequences concerning the delivery of official documents. For instance, receiving a court decision via e-mail would be considered an official delivery.

The families of US soldiers who died in Iraq have also attempted to make use of the analogy between mail (letters) and e-mail in order to gain access to their loved ones' private e-mail and blogs, arguing that they should be allowed to inherit e-mail and blogs as they would letters and diaries. ISPs have found it difficult to deal with this highly emotional problem. Instead of going along with the analogy between letters and e-mail, most ISPs have denied access based on the privacy agreement they signed with their users.

The postal system and ICANN

Paul Twomy, former CEO of ICANN, used the following analogy between the postal system and ICANN's function: 'If you think of the Internet as a post office or a postal system, domain name and IP addressing are essentially ensuring that the addresses on the front of an envelope work. They are not about what you put inside the envelope, who sends the envelope, who's allowed to read the envelope, how long it takes for the envelope to get there, what the price of the envelope is. None of those issues are important for ICANN's functions. The function is focusing on just ensuring that the address works.'

Internet – television

Similarities: The initial analogy related to the physical similarity between computers and television screens. A more sophisticated analogy draws on the use of both media – web and TV – for broadcasting.

Differences: The Internet is a broader medium than television. Aside from the similarity between a computer screen and a TV screen, there are major structural differences between them. Television is a one-to-many medium for broadcasting to viewers, while the Internet facilitates many different types of communication (one-to-one, one-to-many, many-to-many).

Used by: This analogy is used by those who want to introduce stricter content control to the Internet. In their view, due to its power as a mass media tool similar to television, the Internet should be strictly controlled. The US government attempted to use this analogy in the seminal Reno vs American Civil Liberty Union case.[27] This case was prompted by the Communication Decency Act passed by Congress, which stipulates strict content control in order to prevent children from being exposed to pornographic materials via the Internet. The court refused to recognise the television analogy.

Internet – library

Similarities: The Internet is sometimes seen as a vast repository of information and the term 'library' is often used to describe it: for example, 'a huge digital library', 'a cyber-library', 'the Alexandrian Library of the twenty-first century', etc.

Differences: The storage of information and data is only one aspect of the Internet, and there are considerable differences between libraries and the Internet:

- Traditional libraries aim to serve individuals living in a particular place (city, country, etc.), whereas the Internet is global.
- Books, articles, and journals are published using procedures to ensure quality (editors). Typically, the Internet does not always have editors.
- Libraries are organised according to specific classification schemes, allowing users to locate the books in their collections. There is no such overall classification scheme for information on the Internet.
- Apart from keyword descriptions, the contents of a library (text in books and articles) are not accessible until the user borrows a particular book or journal. The content of the Internet is immediately accessible via search engines.

Used by: This analogy is used by various projects that aim to create a comprehensive system of information and knowledge on particular issues (portals, databases, etc.). The library analogy has been used in the context of a Google book project with the objective of digitalising all printed books.

Internet – VCR, photocopier

Similarities: This analogy focuses on the reproduction and dissemination of content (e.g. texts and books). Computers have simplified reproduction through the process of 'copy and paste'. This, in turn, has made the dissemination of information via the Internet much simpler.

Differences: The computer has a much broader function than the copying of materials, although copying itself is much simpler on the Internet than with a VCR or photocopier.

Used by: This analogy was used in the context of the US Digital Millennium Copyright Act (DMCA), which penalises institutions that contribute to the infringement of copyright (developing software for breaking copyright protection, etc.). The counterargument in such cases was that software developers, like VCR and photocopier manufacturers, cannot predict whether their products will be used illegally.

This analogy was used in cases against the developers of Napster-style software for peer-to-peer (P2P) sharing of files, such as Grokster and StreamCast.

Internet – highway

Similarities: What the highway is for transportation in the real world, the Internet is for communication in a virtual space.

Differences: Aside from the data transportation aspect of the Internet, there are no other similarities between the Internet and highways. The Internet moves intangible materials (data), while highways facilitate the transportation of goods and people.

Used by: The highway analogy was used extensively in the mid-1990s, after Al Gore allegedly coined the term 'information superhighway'. The term 'highway' was also used by the German government in order to justify the introduction of a stricter Internet content control law in June 1997:

> *It's a liberal law that has nothing to do with censorship but clearly sets the conditions for what a provider can and cannot do. The Internet is a means of transporting and distributing knowledge... just as with highways, there needs to be guidelines for both kinds of traffic.*[28]

Highways and the Internet

Hamadoun Touré, former ITU Secretary General, used an analogy between highways and the Internet by relating highways to telecommunications and the Internet traffic to trucks or cars: 'I was giving a simple example, comparing Internet and telecommunications to trucks or cars and highways. It is not because you own the highways that you are going to own all the trucks or cars running on them, and certainly not the goods that they are transporting, or vice versa. It's a simple analogy. But in order to run your traffic smoothly, you need to know, when you are building your roads, the weight, the height and the speed of the trucks, so that you build the bridges accordingly. Otherwise, the system will not flow. For me, that's the relationship between the Internet and the telecommunication world. They are condemned to work together.'[29]

Internet – high seas

Similarities: Initially, an analogy was made between high seas waters and Internet traffic, which seemed to be beyond any national jurisdiction.

Differences: There is no matching aspect between the Internet and high seas waters. First, Internet data is always within the realm of some national jurisdiction. Telecommunications seabed cables may be laid on the beds of the high seas in the Pacific and Atlantic oceans, but they are owned by, predominantly, private companies, which are subject to the national jurisdiction where they are legally incorporated. If Microsoft locates data-centres in high seas (something the company has been considering), it will be still subject to US jurisdiction, as Microsoft is incorporated in the USA. Any device, cable, or ship operating on the high seas must be under some national jurisdiction.

Used by: The high seas analogy is used to support a variety of views. Sometimes, it is used to justify a need for international regulation of the Internet. Concretely speaking, this analogy suggests the use of the old Roman law concept of res communis omnium (i.e., a space which is part of the common heritage of humankind, to be regulated and garnered by all nations) on the Internet as it is used for regulating the high seas. In other cases, the high seas analogy is used as an argument against national regulation of the Internet, with the Internet being seen as a space beyond the jurisdiction of any single country, like it is the case with the Antarctic and outer space, in addition to high seas.

Classification of Internet governance issues

Internet governance is a complex field requiring an initial conceptual mapping and classification. Its complexity is related to its multidisciplinary nature, encompassing a variety of aspects, including technology, socioeconomics, development, law, and politics.

The practical need for classification was clearly demonstrated during the WSIS process. In the first phase, during the lead-up to the Geneva summit (2003), many players, including nation states, had difficulty grasping the complexity of Internet governance. A conceptual mapping, provided by various academic inputs and the WGIG report, contributed to more efficient negotiations within the context of the WSIS process. The WGIG report (2005) identified four main areas:

- Issues related to infrastructure and the management of CIR.
- Issues related to the use of the Internet, including spam, network security, and cybercrime.
- Issues relevant to the Internet but that have an impact much wider than the Internet and for which existing organisations are responsible, such as IPR or international trade.
- Issues related to the developmental aspects of Internet governance, in particular capacity building in developing countries.

The agenda for the first IGF, held in Athens in 2006, was built around the following thematic areas: access, security, diversity, and openness. At the second IGF in Rio de Janeiro

in 2007, a fifth thematic area was added to the agenda: managing CIR. These five thematic areas have influenced the agendas of all subsequent IGF meetings.

Although the classification changes, Internet governance addresses more or less the same set of 40–50 specific issues, with the relevance of particular issues changing. For example, while spam featured prominently in the WGIG classification in 2004, its policy relevance diminished at the IGF meetings, where it became one of the less prominent themes within the security thematic area.

Diplo's classification of Internet governance groups the main 40–50 issues into the following seven baskets:[30]

- Infrastructure
- Security
- Legal
- Economic
- Development
- Sociocultural
- Human rights

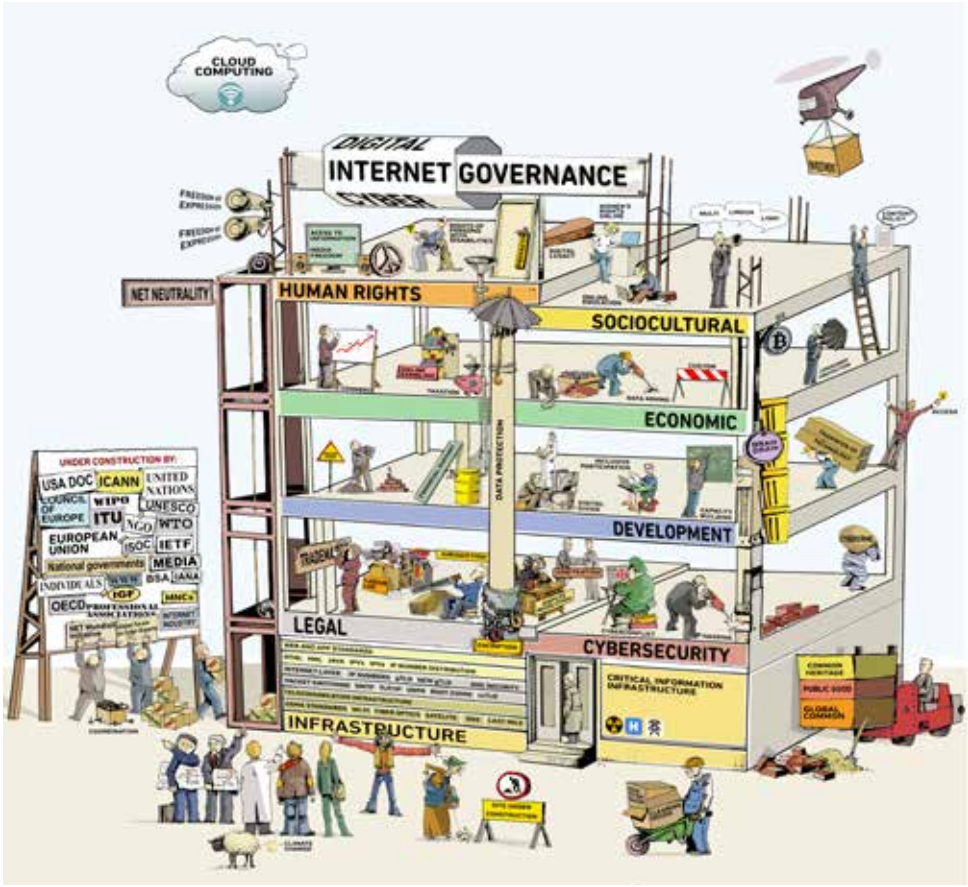

Figure 4. Internet governance building under construction

This classification (Figure 4) reflects both the aforementioned (WGIG, IGF) policy approaches as well as academic research in this field. The classification was developed in 1997 and has been regularly adjusted based on feedback from course participants (an alumnus of more than 3000 people at the end of 2015), research results, insights from the policy process, and data-mining. A similar classification, based on seven clusters, is used in the report Mapping of international Internet public policy issues prepared by the secretariat of the CSTD, for the November 2014 Inter-sessional Panel of the Commission.[31]

Naming, defining, and framing Internet governance

In the previous pages, we have discussed alternative ways of defining and framing the concept of Internet governance. The concept remains open, and prone to different interpretations, as is vividly illustrated in the Internet governance building (Figure 4). At the top of the building there is a banner with the name 'Internet governance'; the banner has a rotating section, which allows us to easily change *Internet* governance to *cyber* governance or *digital* governance. In the public policy debate, other terms are used as well, such as Internet policy, digital policy, and cyber diplomacy.

The discussion is further complicated when we include the question of the scope of Internet governance, i.e., which issues fall within its remit. Some argue, for example, that cybersecurity is part of Internet governance. Others argue that cybersecurity is a separate field. Some say that Internet governance is only about ICANN-related issues (management of domain names, IP addresses, etc.). Others extend the coverage of Internet governance to a wide set of Internet-related public policy issues.

This debate is not only of theoretical relevance. It also impacts practical aspects related to where, how, and by whom Internet policy issues are discussed and addressed. There is no simple resolution to this debate on terms and definitions. Differences will persist and, ultimately, it is not likely that we will all agree on the 'right' term and definition.

In this book, Internet governance is used as an umbrella concept, covering over 40 Internet public policy issues grouped into 7 baskets. This approach is inspired by the WGIG definition of Internet governance, and the way in which the term has been used in WSIS processes, in publications, and in academic research. The use of different terms and definitions is inspired by other policy and research justifications.

While the debate on the 'right' term or definition is not likely to be particularly effective or useful, it is of utmost importance to have a clear understanding of the exact issue coverage of each term. For example, what issues are discussed under the concepts of Internet governance, digital policy, or cyber governance? Do they include cybersecurity, e-commerce, or online privacy, to name only few of the Internet public policy issues? Understanding the scope of each term is the first step towards reducing confusion and increasing clarity in policy processes.

Ultimately, with the seamless integration of digital tools in modern society, the discussion about terminology will become less relevant. E-commerce will take its place as an indispensable part of commerce. Cybersecurity will continue to align with, and support overarching security priorities. The more digital advancements become an intrinsic part of our daily lives, the more likely it is that Internet governance will coalesce into the underlying governance of society.

Endnotes

1 The UN General Assembly Resolution 56/183 (21 December 2001) endorsed the holding of the World Summit on the Information Society (WSIS) in two phases. The first phase took place in Geneva from 10 to 12 December 2003 and the second phase took place in Tunis, from 16 to 18 November 2005. The objective of the first phase was to develop and foster a clear statement of political will and to take concrete steps to establish the foundations for an information society for all, reflecting all the different interests at stake. More than 19 000 participants from 174 countries attended the summit and related events. Source: http://www.itu.int/wsis/basic/about.html [accessed 28 September 2016].

2 The WGIG definition follows the pattern of frequently used definitions in the regime theory. The founder of regime theory, Stephen D. Krasner, notes: 'Regimes can be defined as sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations. Principles are beliefs of fact, causation, and rectitude. Norms are standards of behaviour defined in terms of rights and obligations. Rules are specific prescriptions or proscriptions for action. Decision-making procedures are prevailing practices for making and implementing collective choice.' Krasner S (1983) *Introduction, in International Regimes.* Krasner SD (ed.), Cornell University Press: Ithaca, NY, USA.

3 Shannon V (2006) What's in an 'i'? *International Herald Tribune,* 3 December 2006. Available at http://www.nytimes.com/2006/12/03/technology/03iht-btitu.3755510.html [accessed 28 September 2016].

4 Barlow JP (1996) A declaration of the independence of cyberspace. Available at https://www.eff.org/cyberspace-independence [accessed 28 September 2016].

5 For the evolution of the use of the word 'Internet' in the preparation for the WSIS Summit, refer to DiploFoundation (2003) The Emerging Language of ICT Diplomacy – Key Words. Available at https://www.diplomacy.edu/IGFlanguage/2004research [accessed 3 August 2014].

6 Working Group on Internet Governance (2005) Report. Available at http://www.wgig.org/docs/WGIGREPORT.pdf [accessed 10 October 2016].

7 World Summit on the Information Society (2005) Tunis Agenda for the Information Society. Available at http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html [accessed 10 October 2016].

8 In June 2010, ICANN approved the .xxx top level domain for adult material.

9 For more on network neutrality, watch our explanatory video at https://www.youtube.com/watch?v=R-uMbZFfJVU [accessed 3 October 2016].

10 Clinton H (2010) Remarks on Internet freedom. Available at http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm [accessed 3 October 2016].

11 Refer to paragraph 123 of the Addis Ababa Action Agenda, adopted at the Third International Conference on Financing for Development, held between 13 and 16 July 2015. Available at http://www.un.org/esa/ffd/wp-content/uploads/2015/08/AAAA_Outcome.pdf [accessed 10 October 2016].

12 World Bank (2016) World Development Report 2016: Digital Dividends. Available at http://www.worldbank.org/en/publication/wdr2016 [accessed 3 October 2016].

13 Drake W *et al.* (2016) Internet Fragmentation: An Overview. Available at http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf [accessed 3 October 2016].

14 Global Commission on Internet Governance (2016) One Internet. Available at https://www.ourinternet.org/report [accessed 3 October 2016].

15 Wiener N (1948) *Cybernetics: Or Control and Communication in the Animal and the Machine.* Paris: Hermann & Cie, Cambridge, MA: Technology Press, and New York: John Wiley & Son.

16 Gibson W (1984) *Neuromancer.* New York: Ace Books.

17 Newitz A (2013) The bizarre evolution of the word 'cyber'. Available at http://io9.gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487 [accessed 3 October 2016].

[18] European Commission (2015) A Digital Single Market Strategy for Europe. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0192 [accessed 11 October 2016].

[19] Cited in Helfand D (2001) Edpseak is in a class by itself. *Los Angeles Times*, 16 August. Available at http://articles.latimes.com/2001/aug/16/news/mn-34814 [accessed 3 October 2016].

[20] This section could not have been completed without discussion with Aldo Matteucci, Diplo's senior fellow, whose contrarian views on modern governance issues are a constant reality check in Diplo's teaching and research activities.

[21] United Nations General Assembly (2015) Resolution A/70/125. Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society. Available at http://workspace.unpan.org/sites/Internet/Documents/UNPAN95735.pdf [accessed 10 October 2016].

[22] NATO (2016) Warsaw Summit Communiqué. Available at http://www.nato.int/cps/en/natohq/official_texts_133169.htm [accessed 10 October 2016].

[23] Broeders D (2015) The public core of the Internet. Amsterdam: Amsterdam University Press. Available at http://www.wrr.nl/fileadmin/en/publicaties/PDF-Rapporten/The_public_core_of_the_internet_Web.pdf [accessed 3 October 2016].

[24] Ambassador Trigona's statement delivered at the UN General Assembly meeting dedicated to the World Summit on Information Society Review Process, on 15 December 2015, in New York: https://www.gov.mt/en/Government/Press%20Releases/Documents/pr152897a.pdf [accessed 3 October 2016].

[25] The WSIS process started with the first preparatory meeting held in July 2002 in Geneva. The first summit was held in Geneva (December, 2003) and the second summit in Tunisia (November, 2005).

[26] Volker Kitz provided an argument for the analogy between administration of telephony systems and Internet names and numbers. Kitz V (2004) ICANN may be the only game in town, but Marina del Rey isn't the only town on Earth: Some thoughts on the so-called uniqueness of the Internet. Available at http://studentorgs.law.smu.edu/Science-and-Technology-Law-Review/Articles/Fall-2005/Kitz.aspx [accessed 3 October 2016].

[27] US Supreme Court (1997) Decision in Reno vs American Civil Liberty Union. Available at https://supreme.justia.com/cases/federal/us/521/844/case.html [accessed 10 October 2016]

[28] Quoted in Mock K and Armony L (1998) Hate on the Internet. Available at http://archive.is/M70XS [accessed 3 October 2016].

[29] Excerpts from the ITU Secretary General's speech delivered at the ICANN meeting in Cairo (6 November 2008). Available at http://archive.icann.org/en/meetings/cairo2008/files/meetings/cairo2008/toure-speech-06nov08.txt [accessed 3 October 2016].

[30] The term 'basket' was introduced into diplomatic practice during the Organization for Security and Co-operation in Europe (OSCE) negotiations.

[31] CSTD (2015) Mapping of international Internet public policy issues. Available at http://unctad.org/meetings/en/SessionalDocuments/ecn162015crp2_en.pdf [accessed 19 October 2016].

Section 2

THE INFRASTRUCTURE BASKET

The infrastructure basket

The infrastructure basket includes the basic, mainly technical, issues related to the running of the Internet. The main criterion for putting an issue in this basket is its relevance to the basic functionality of the Internet. This basket includes the essential elements without which the Internet and the World Wide Web (www)[1] could not exist. These issues are grouped into three main areas, which to some extent, follow the three-layer Internet model shown in Figure 5.

1. The telecommunications infrastructure, through which all Internet traffic flows.

2. Technical issues related to standards (technical and web standards) and critical Internet resources (IP numbers, the DNS, and the root zone).

3. Cross-cutting issues including net neutrality, cloud computing, the IoT, and convergence.

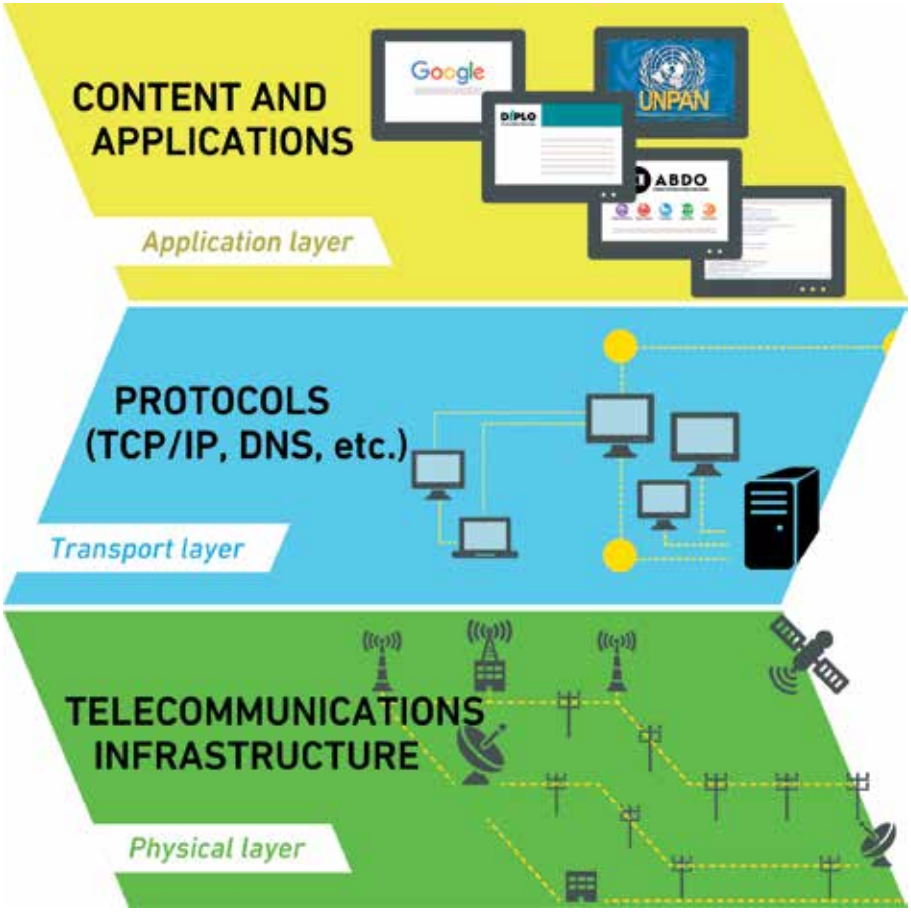

Figure 5. Internet layers

The telecommunications infrastructure[2]

The current situation

The Internet relies on the telecommunications infrastructure as the medium through which the traffic flows: cables such as copper wires or optical fibres; electromagnetic waves such as satellite, wireless links, and mobile networks. In many cases, the existing telecommunications infrastructure – such as the telephone lines and mobile connectivity, power grid,[3] undersea cables, or satellite links – is utilised to carry Internet packages. Increasingly, an innovative telecommunications infrastructure is being deployed to carry data – such as high-bandwidth submarine fibre optic cables, fifth-generation (5G) mobile networks, and innovative wireless solutions like Google balloons[4] or Television White Spaces,[5] as well as technologies enabling greater deployment of the IoT.

Most commonly used Internet connectivity technologies

Wired telecommunications infrastructure

- Digital subscriber lines (DSLs): use existing copper phone wires to transmit data and voice traffic.
- Television cable networks: cable broadband services provide access to the Internet over the cable television infrastructure.
- Fibre optics: optical fibre networks are the preferred backbone infrastructure of the Internet, because a single fibre can carry significant amounts of data over vast distances, without significant signal deterioration by distance.
- Internet over power lines: allows users to plug a device into any electrical outlet and instantly get high-speed Internet service.

Wireless telecommunications infrastructure

- Satellite Internet: used to bring Internet connectivity to communities in locations where terrestrial Internet access is not available, and to communities that move frequently.
- Wi-Fi: allows devices to connect to wireless local area networks (WLANs) via radio frequencies.
- WiMAX (Worldwide Interoperability for Microwave Access): facilitates the delivery of wireless broadband access over long distances, as an alternative to cable and DSL, using licensed and unlicensed frequencies.
- Mobile broadband: one of the widest used technology is the Global System for Mobile Communications (GSM), which emerged in Europe and is becoming globally dominant with its third- and fourth-generation (3G and 4G), and, eventually, 5G.

The way in which telecommunications are regulated impacts Internet governance directly. The telecommunications infrastructure is regulated at both national and international level. The key international organisations involved in the regulation of telecommunications

include the ITU, which has developed rules for coordination among national telecommunications systems, the allocation of the radio spectrum, and the management of satellite positioning; and the World Trade Organization (WTO), which has played a key role in the liberalisation of telecommunications markets worldwide.[6]

Two International Telecommunication Regulations

The 1988 ITU's ITRs facilitated the international liberalisation of pricing and services and allowed a more innovative use of basic services, such as international leased lines, in the Internet field. They provided one of the infrastructural bases for the rapid growth of the Internet in the 1990s. The ITRs were amended in December 2012 during WCIT-12 in Dubai; 89 states – mostly developing countries – have signed the amended ITRs, while 55 states, including the USA and many European states, have not.[7] Thus, starting from 1 January 2015, when the 2012 ITRs entered into force, two international telecommunications regimes (1988 and 2012) have been operating. Fortunately, since the 2012 amendments are not major, they do not affect the integrated functionality of the global telecommunications system. Yet, this 'governance duality' is something that needs to be resolved.

The roles of the ITU and the WTO are quite different. The ITU sets detailed voluntary technical standards and telecommunication-specific international regulations, and provides assistance to developing countries.[8] Most policy controversies are related to the ITU dealing with policy issues which are on the border between the telecommunications infrastructure and the Internet, such as VoIP, cybersecurity, and digital object identifiers (Digital Object Architecture – DOA).[9] The WTO provides a framework for general market rules.[10] Its role in the telecommunications field has not raised any major controversies up to now. However, the WTO's more active involvement in e-commerce may trigger more debate on aspects related to addressing the border zones between e-commerce and related fields such as cybersecurity and data protection.

The issues

Internet backbone cables[11]

Ever since the first telegraph cable reached India via the Mediterranean Sea, the Red Sea, and the Indian Ocean, in 1870, most international electronic communications traffic has been carried via seabed cables. Currently, more than 90% of all global Internet traffic flows through submarine fibre optics cables, which largely follow the old geographical routes used by the telegraph.

Submarine Internet cables reach land in a few Internet traffic hubs. Most Latin American cables reach land in Miami. In Asia, the key Internet traffic hubs are Singapore and Hong Kong SAR. Other key points for Internet traffic include Amsterdam, New York, and San Francisco. The most vulnerable points for Internet cables and traffic continue to be traditionally strategic hotspots, including the Straits of Luzon, Hormuz, and Malacca, as well as the Suez Canal.

In digital connectivity between Asia and Europe, geography matters as well. For example, 95% of Internet traffic between Asia and Europe passes via Egypt, similar to maritime transport that uses the Suez Canal as a shortcut.

Since most Internet traffic currently flows through submarine cables, the installation of new terrestrial Internet cables is often seen as an important step towards diversifying Internet traffic, in particular between Asia and Europe.

The United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP) and the Asian Development Bank have been promoting a digital component of the Asian Highway, a transcontinental transport infrastructure project that spans 141,000 km.[12] Furthermore, the Trans-Eurasian Information Super Highway (TASIM) is planning to connect Eastern Europe and Central Asia, further diversifying the data flow between the two continents. The project aims to 'enhance the speed of the connection with the Eastern Asian partners and to improve the resiliency of the Internet', and, in the process, improve regional cooperation in Central Asia.[13]

Digital aspects also feature prominently in the One Belt, One Road initiative, which includes a digital component referred to as the Digital Silk Road.[14] Digital connection could benefit from transportation and energy infrastructural projects, which will include laying fibre-optic cables along railroads and energy pipelines.

All planned terrestrial cable projects, and the Digital Silk Road in particular, might, for the first time in history, shift a considerable volume of telecommunications traffic from seabed to terrestrial cables.

The local loop – last mile

The 'local loop' (or 'last mile') is the name given to the connection between ISPs and their individual customers. Problems with the local loop (such as cable lines in poor condition, power outages, etc.) are an obstacle to the more widespread use of the Internet in many, mainly developing countries. Wireless communication is one possible, low-cost solution to the local loop problem. In recent years, Google has been experimenting in providing wireless mobile access from balloons (Project Loon), while Facebook has been working on providing Internet access using a fleet of drones. Apart from increasingly available technological options, the solution to the problem of the local loop also depends on the liberalisation of this segment of the telecommunications market, including allowing multiple operators to use the last mile of the telephone network (known as local loop unbundling process).

The liberalisation of telecommunications markets

Historically, telecommunications infrastructure and services were provided by state-owned operators on a monopoly basis. Over the last two decades, many countries have liberalised their telecommunications sectors and introduced market competition by allowing new operators to enter the market and to provide competing electronic communications network and services. Liberalisation also meant that new service providers were allowed to access the existing (state-owned) infrastructure. Privatisation of the state-owned telecom operators has accompanied liberalisation policies. Yet, this process has been slower among developing countries. They often face a dilemma between, on the one hand, liberalising the telecommunications market, reducing communication costs, and boosting economic development, and, on the other hand, preserving telecommunications monopolies as sources of important budgetary income (something they enjoyed thanks to, in particular, the inter-carrier international settlement system of traditional telephony). Such financial considerations have led to a question of redistribution of income from Internet communications services, which was raised by some developing countries at WCIT-12 and at other international meetings.

Electromagnetic spectrum management

While wireless communication is often seen as a more convenient alternative to the deployment of a wired infrastructure, one of the inconvenient features of the spectrum, however, is that it is scarce. Theoretically one could split each frequency segment into endless smaller pieces, yet in practice the equipment we use – even though it is continuously improved to utilise the spectrum more efficiently – has limits to the narrowness of the frequency bands it can use and still avoid interference by other equipment with similar frequencies. This suggests that there should be an authority to allocate specific frequency bands for use by one or more types of radio communications services, as well as to assign specific segments of the spectrum to specific wireless operators – which includes TV stations, radio emitters, mobile network operators, and Internet service providers, among others.

The frequency management in each country – i.e., decisions on which technologies and which providers can use which sub-segment of the allocated spectrum and with what licences – is usually in the hands of the national telecommunications regulatory authorities, which further harmonise their national allocations with neighbouring and other countries bilaterally or through regional initiatives (such as the EU's Radio Spectrum Committee (RSC) and the Radio Spectrum Policy Group (RSPG)) or international institutions (such as the ITU).

In the USA, as well as in most EU member states, for example, the granting of rights to use radio frequencies is done through submitting the frequencies to public auction processes. The EU has also developed a comprehensive regulatory approach for radio spectrum management, with the objective of introducing some level of harmonisation in the use of radio frequencies across member states.[15] Licensing the use of certain parts of the spectrum and allocating them to those who can pay the most for it – such as mobile network operators – ensures that the spectrum will be used according to certain needs, but also brings good revenue for states.

The development of new communications services using radio spectrum, most notably wireless broadband and mobile communications, has increased the demand for radio frequencies, urging governments around the world to find solutions to accommodate an optimal spectrum use. One way to extend the usable spectrum band for digital communications is to release large portions of the spectrum occupied by analogue TV broadcasters: by motivating broadcasting companies to turn from the analogue signal to a digital signal (which requires significant investment in new broadcasting equipment as well as additional devices for each household, but brings better quality of service and opportunity for offering other services), important parts of the spectrum would be freed to be allocated to other services – the so-called digital dividend.

The volume and limits of the use of spectrum are influenced by technological developments. This has led to the argument, by some groups, that current government regulation should be replaced with an 'open spectrum', i.e., open access for all, which would follow the unlicensed approach used for regular Wi-Fi (there is no licence needed to set up a home or another Wi-Fi network). However, there are two potential problems with this view. One is related to the huge investment that telecommunications companies, especially in Europe, made in acquiring the rights to operate 3G and 4G mobile-phone networks. An open spectrum policy would be unfair to these companies. It could trigger their bankruptcies and instability in the telecommunications sector. The other is that if the spectrum becomes a free-for-all resource, this does not necessarily mean that it will be used as a

public good, for the benefit of many. Rather, it may primarily be used by actors who have technical capacities to take advantage of the 'free' spectrum for their own purposes, including for profit.

Internet access providers

The Internet access architecture consists of three tiers. ISPs who connect end-users constitute Tier 3. Tiers 1 and 2 consist of the Internet bandwidth providers (IBPs). Tier 1 carriers are the major IBPs. They usually have peering[16] arrangements with other Tier 1 IBPs. The main difference between Tier 1 and Tier 2 IBPs is that Tier 1 IBPs exchange traffic through peering, while Tier 2 IBPs have to pay transit fees to Tier 1 providers.[17] Tier 1 is usually run by large companies, such as AT&T, Verizon, Level 3 Communications, Vodafone, and NTT Communications.

The issues

Telecommunications monopolies and ISPs

It is common in countries with telecommunications monopolies for those monopolies to also provide Internet access. Monopolies preclude other ISPs from entering this market and inhibit competition. This results in higher prices and often a lower quality of service (QoS), and fails to reduce the digital divide. In some cases, telecommunications monopolies tolerate the existence of other ISPs, but interfere at operational level (e.g. by providing lower bandwidths or causing disruptions in services).

Telecommunications liberalisation and the role of ISPs and IBPs

There are opposing views about the extent to which ISPs and IBPs should be subject to existing international instruments. One view, shared mainly by developed countries, argues that the liberalised rules granted by the WTO to telecommunications operators can also be extended to ISPs. Others, mainly developing countries, argue that the WTO telecommunications regime applies only to the telecommunications market. In this view, the regulation of the ISP market requires new WTO rules.

The role of ISPs in enforcing legal rules

Since ISPs connect end-users to the Internet, they are seen as being able to provide the most direct and straightforward enforcement of legal rules on the Internet. This is why many states have started concentrating their law enforcement efforts on ISPs, in areas such as copyright infringement, child online protection, and other content policy fields.

Refer to Section 4 for further discussion on the role of intermediaries.

Should the Internet infrastructure be considered a public service?

Internet data can flow over any telecommunications medium. In practice, facilities such as Tier 1 backbones (i.e., principal data routes between large, strategically interconnected

networks and core routers in the Internet), commonly having optical cables or satellite links, have become critical to the operation of the Internet. Their pivotal position within the Internet network grants their owners the market power to impose prices and conditions for providing their services.[18] Ultimately, the functioning of the Internet could depend on the decisions taken by the owners of central backbones. The trend of increasing data volume flows has brought in some new players who were originally not connected directly with the telecommunications sector. For example, Google, Facebook, and Microsoft have been financing the deployment of their own undersea cables in recent years.[19]

Can reliability of the Internet be guaranteed?

Is it possible for the global Internet community to request assurances and guarantees for the reliable functioning of the critical Internet infrastructure from major Internet companies and telecommunications operators?

Currently, there are no such provisions. However, the trend in discussion seems to be on imposing certain public requirements on private Internet infrastructure operators.

IBPs and critical infrastructure

In early 2008, a disruption occurred when one of the main Internet cables was cut in the Mediterranean Sea near Egypt. This incident endangered access to the Internet in a broad region extending to India. Two similar incidents with Internet cables near Taiwan and Pakistan have clearly shown that the Internet infrastructure is part of a national and global critical infrastructure. Disruption of Internet services can affect the overall economy and the social life of a region. The possibility of such a disruption leads to a number of questions:

- Are the main Internet cables properly protected?
- What are the respective roles of national governments, international organisations, and private companies in the protection of Internet cables?
- How can we manage the risks associated with potential disruption of the main Internet cables?

www.igbook.info/infrastructure

Transmission Control Protocol/Internet Protocol

The current situation

TCP/IP is the main Internet technical standard. It is based on three principles:

- Packet-switching: Messages are split into small chunks – called packets – and sent separately through different routes over the Internet, to be assembled again into the original message at the receiving end.

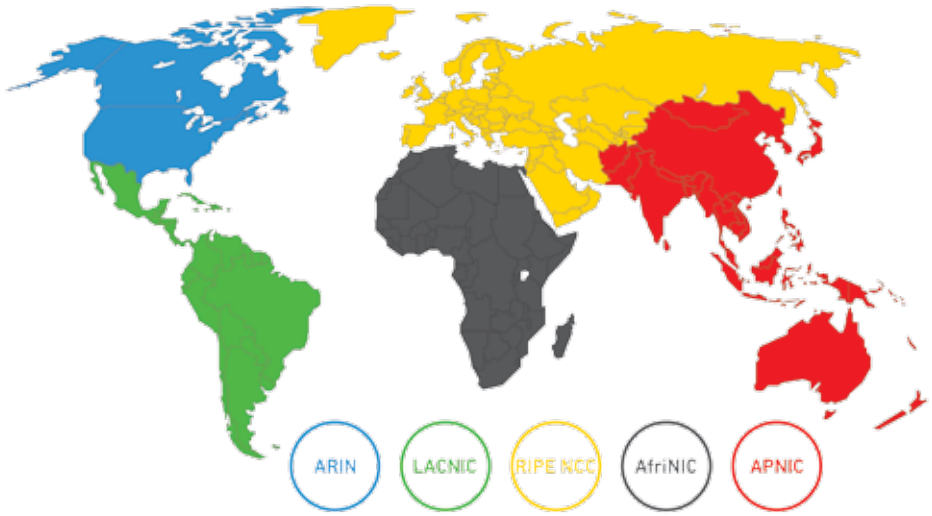

Figure 6. Regional Internet Registries

- End-to-end networking: This is one of the core design principles which states that communications operations and services should take place at the originating and receiving ends, while the network itself should be as neutral or 'dumb' as possible.

- Robustness: Sending data should conform to the specifications, while receiving data should be more flexible, to be able to accept information that is non-conforming.

With respect to the TCP/IP, the two main Internet governance related aspects are:

- The introduction of new standards.

- The distribution of IP numbers.

TCP/IP standards are set by the IETF. Given the core relevance of these standards to the Internet, they are carefully and constantly reviewed by the IETF. Any changes to TCP/IP require extensive prior discussion and proof that they are an effective solution (i.e., the 'running code' principle).

An IP address (or number) is a unique numeric address that each device connected to the Internet must have; each address specifies how to reach a network location via the Internet routing system. Generally speaking, two devices connected to the Internet cannot have the same IP address.

The system for the distribution of IP numbers is hierarchically organised. At the top is IANA, whose functions are currently performed by the PTI, an affiliate of ICANN.[20] PTI distributes blocks of IP numbers to the five regional Internet registries (RIRs) (Figure 6).[21] RIRs distribute IP numbers to the local Internet registries (LIRs) and national Internet registries (NIRs), which in turn distribute IP numbers to smaller ISPs, companies, and individuals further down the ladder.

The issues

The limitation of IP numbers and the transition to IPv6

The pool of IP numbers under IP version 4 (IPv4), which was introduced in 1983, contains some four billion numbers, which were initially thought to be sufficient to satisfy the demand for addresses. However, in February 2011, IANA announced that it no longer had blocks of IPv4 available to allocate to RIRs.

The depletion of IPv4 numbers has been accelerated in recent years, with the introduction of Internet-enabled devices (such as mobile phones, smart devices, game consoles, and home appliances) and the rise of worldwide Internet connectivity. Developments in the area of the IoT have also led to an increase in the demand for IP addresses, with IoT devices requiring IP addresses to connect to the Internet. The concern that IP numbers might run out and eventually inhibit the further development of the Internet led the technical community to take three major actions.

- Rationalise the use of the existing pool of IP numbers through the introduction of Network Address Translation (NAT): a technique that allows computers in a private network (such as those used in companies and organisations) to share one single IP address when connecting to the Internet.

- Address the wasteful address allocation algorithms previously used by the RIRs by introducing Classless Inter-Domain Routing (CIDR): an IP addressing scheme which, in very simple terms, allows a single IP address to designate many unique IP addresses (thus making the allocation of IP addresses more efficient).

- Introduce a new version of the IP – IP version 6 (IPv6) – which provides a much bigger pool of IP numbers (over 340,000,000,000,000,000,000).

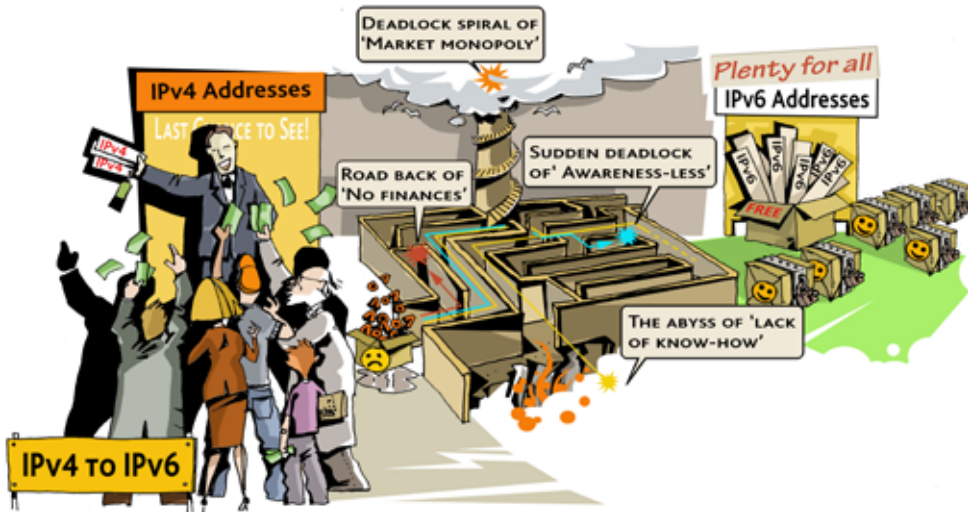

Figure 7. IPv4 to IPv6

The Internet technical community responded proactively to the problem of a potential shortage of IP numbers. While NAT and CIDR provided a quick fix for the problem, a proper long-term solution was the transition to IPv6.

However, although IPv6 was introduced back in 1996, its deployment has been slow, due to insufficient awareness about the need for transition, as well as limited funds for investment in new equipment in developing countries (Figure 7). Experts have warned that a slow transition to IPv6 risks leading to the so-called technical fragmentation of the Internet, where two parallel internets – one IPv4 enabled, and the other one IPv6 enabled – will not be able to interact with one another. This was underlined, for example, in a report published in early 2016 by WEF,[22] according to which only about 4% of the Internet was at that time servicing IPv6 usage.

The technology of the Internet allows the coexistence of IPv4 and IPv6; most networks that use IPv6 support both IPv4 and IPv6 addresses. Nevertheless, for smooth transition between the two protocols, a set of techniques is needed to implement mechanisms for true Internet working, coexistence, easy address mapping, and name service migration. The IETF specifications for IPv6 contain pertinent transition strategies, tools, and mechanisms.[23]

Apart from the problem of transition, the policy framework for IPv6 distribution will require a proper distribution of IP numbers, demanding the introduction of open and competitive mechanisms to address the needs of end-users in the most optimal way. Even with the introduction of IPv6, an 'artificial' scarcity of IP numbers could still arise, if those responsible for allocating them at local level, such as ISPs, choose to abuse their power and link such allocation to, for example, the purchase of other services, thus affecting the availability and price of IP numbers.

The transition from IPv4 to IPv6 requires the involvement of a wide range of stakeholders. Technical organisations such as IANA/PTI, the RIRs, and the IETF need to ensure an efficient and effective administration of IPv6 resources, and to develop the necessary standards and specifications for the use of IPv6. ISPs have to implement techniques that ensure communication between IPv4 and IPv6, and introduce IPv6 in their networks and services. Manufacturers of equipment (operating systems, network equipment, etc.) and applications developers (business software, smart cards, etc.) need to ensure that their products and applications are compatible with IPv6. And providers of information society services have to implement IPv6 within their servers.[24]

Changes in TCP/IP and cybersecurity

Security was not a major issue for the original developers of the Internet (in 1970-1980), as, at that time, the Internet consisted of a closed network of research institutions. With the expansion of the Internet to three billion users worldwide and its growing importance as a commercial and societal infrastructure, the question of security is high up on the list of Internet governance issues.

Although IPv4 offers IP security support (called IPSec), this feature is optional. In IPv6, security is required and IPSec is an integral part which allows authentication, encryption, and compression of Internet traffic without having to adjust any applications.[25]

IPv6 addresses the known security vulnerabilities affecting IPv4 networks, including device authentication, data integrity, and confidentiality. Although IPv6 offers better se-

curity in these cases, the protocol also raises some new security problems due to poor implementation and misconfiguration, which is more likely than with the simpler IPv4.[26] Many of these concerns can be alleviated by careful transition procedures, but fear of these concerns, lack of awareness, and low priority are causing many businesses, for example, to delay transition.[27]

In addition, there are concerns that the IPv6 addresses could hinder privacy, since every connected device will be assigned a unique identifier. This identifier, however, does not need to remain static but could be assigned dynamically and changed occasionally; therefore, the way IPv6 is implemented will be important in this regard.

Changes in TCP/IP and the problem of limited bandwidth

To facilitate the delivery of multimedia content (e.g. Internet telephony, or video on demand), it is necessary to provide a QoS capable of guaranteeing a minimum level of performance. QoS is particularly important in delay-sensitive applications, such as live event broadcasting, and is often difficult to achieve due to bandwidth constraints. The introduction of QoS may require changes in the TCP/IP, including a potential challenge for the principle of net neutrality.

Given the continuous evolution of network technologies, and the challenges underlined herein, organisations in the technical community have started looking into the possibility of developing a next generation of Internet protocols that would be better suited to the realities of the evolving technical landscape. As an example, in early 2016, the European Telecommunications Standard Institute (ETSI) established a working group tasked with 'identifying the requirements for next generation protocols and network architectures'; the group is expected to analyse issues such as: addressing, security and authentication, requirements of the IoT, requirements of video and content distribution, and requirements of e-commerce.[28]

www.igbook.info/protocols

The Domain Name System

The current situation

The DNS translates Internet domain names (like google.com) – easier to remember and use by individuals – into IP addresses, used by computers and other devices to identify a certain Internet resource (a simplified scheme of this process is presented in Figure 8).

From an infrastructure point of view, the DNS consists of root servers, top-level domain (TLD) servers, and a large number of DNS servers located around the world.[29]

A TLD is the highest level in the hierarchical DNS of the Internet. The DNS includes two main types of top-level domains: generic top-level domains and country code top-level domains (ccTLDs). gTLDs include traditional TLDs such as com, .info, .net, and .org, as well as relatively new gTLDs (introduced starting 2014) such as .pub, .بازار (bazaar), .rentals, .ngo, or .游戏 (game). While most gTLDs have an open registration policy, allowing the registration of domain names by any interested individual or entity, there are also gTLDs that are restricted or reserved to specific groups/sectors/communities. For example, .aero

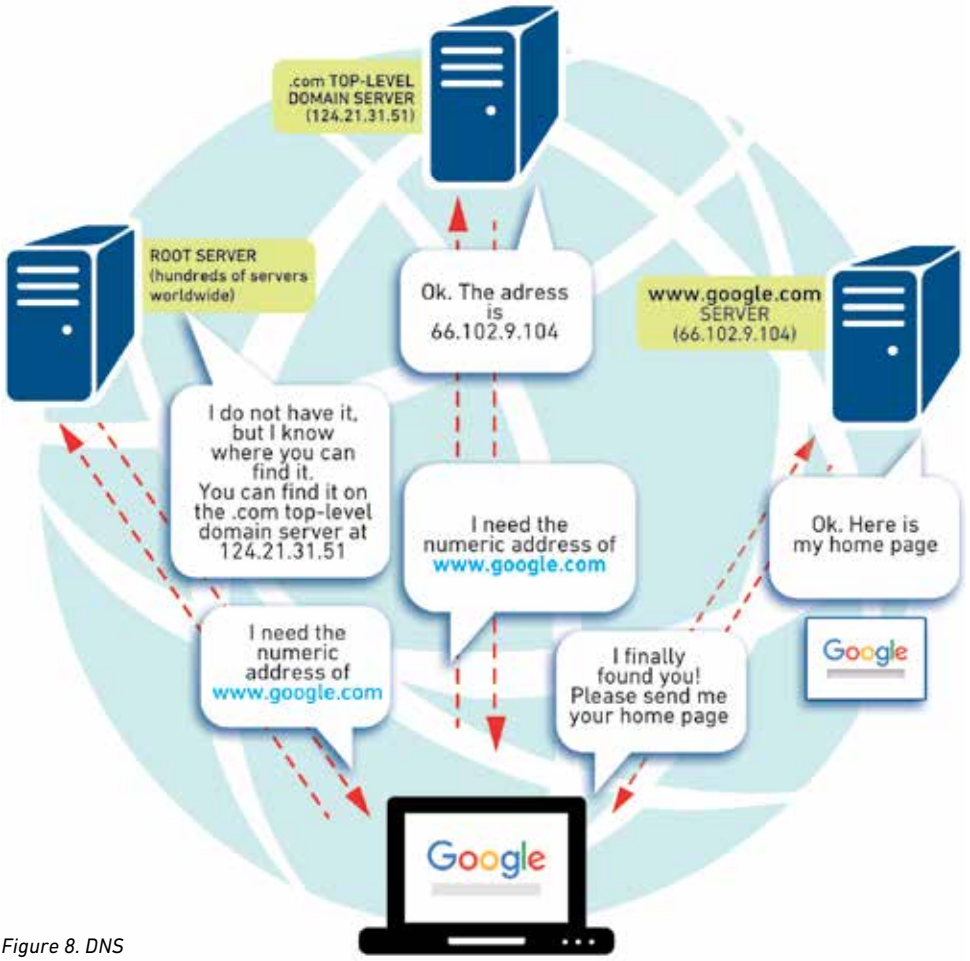

Figure 8. DNS

is open for registration only for the air-transport industry, while .bank can only be used by authorised banking institutions. ccTLDs are two-letter TLDs that designate specific countries or territories (such as .uk for the United Kingdom, .cn for China, and .br from Brazil).

Each gTLD and ccTLD is managed by a registry (also called a registry operator), whose main responsibility is to maintain and administer a database with all domain names registered in the respective TLD. For example, the .com gTLD is managed by VeriSign, while .uk is managed by Nominet. The actual registration of domain names, by end-users (called registrants) is performed through registrars. While in most cases the registry and registrar functions are clearly separated, there are also exceptions; for some ccTLDs, for example, the registry operator can also perform the registrar function.

ICANN ensures the overall coordination of the DNS by:

- Coordinating the allocation and assignment of names in the DNS root zone.
- Coordinating the development and implementation of policies concerning the registration of second-level domain names in gTLDs.

- Facilitating the coordination of the operation and evolution of the DNS root name server system.[30]

Refer to Section 9 for further discussion on ICANN.

For gTLDs, ICANN concludes agreements with registries (for the administration of each gTLD)[31] and accredits registrars.[32] ccTLDs have a special status in that ICANN does not set the rules for how they are administered and managed. There are, however, several ccTLD registries that have concluded some type of agreement with ICANN (such as accountability frameworks, memoranda of understanding, and exchange of letters), mainly for the purpose of setting up some high level principles for the relation between the two parties.

The operational coordination of the DNS is performed through ICANN's affiliate PTI.

The issues

Trademarks

A sensitive aspect related to domain names concerns the protection of trademarks and the related dispute resolution mechanisms. The first-come-first-served principle of domain name allocation used in the early days of the Internet triggered the phenomenon known as cybersquatting, the practice of bad faith registration of domain names representing registered trademarks, generally for the purpose of reselling them later, to entities that have trademark rights over the names. The Uniform Dispute Resolution Policy (UDRP) developed by ICANN and the World Intellectual Property Organization (WIPO) provides mechanisms that have significantly reduced cybersquatting.

Refer to Section 4 for further discussion on intellectual property.

Privacy and data protection

Another important element is related to privacy and data protection in the context of domain names. Currently, registries maintain so-called WHOIS databases containing information about the registered domain names, including data about the registrants. With such information (name, e-mail addresses, postal addresses, etc.) being publicly available, concerns have been raised, mainly by civil rights advocates, who have asked for a redesign of the WHOIS policy. Discussions on this matter have been held within ICANN for the past several years, and a process aimed at redesigning the WHOIS policy is undergoing.

The creation of new generic top level domains

In 2012, after six years of consultations and development of a new policy, ICANN launched the New gTLD Program, opening up the DNS beyond the 22 gTLDs existing at that moment. Under the new programme, any organisation in the world could apply to run a new gTLD registry, including in non-Latin language scripts, as long as it complied with a series of criteria established in the New gTLD Applicant Guidebook. The introduction of new gTLDs was received with enthusiasm by some stakeholders, who saw the programme as an opportunity to enhance competition and consumer choice in the domain name market. Other expressed concerns, especially in relation to the protection of trademarks in the

context of the increasing number of gTLDs, and the potential need for trademark holders to undertake defensive registrations of domain names in multiple gTLDs, for the purpose of avoiding cybersquatting. Although the debate on the introduction of new gTLDs continues, the programme is up and running; at the end of September 2016, there were 1186 delegated new gTLDs (introduced into the DNS).[33]

Intellectual property was not the only concern related to new gTLDs. Governments represented in ICANN's Governmental Advisory Committee (GAC) have drawn attention to the need to implement measures that would ensure the protection of end-users and would preserve market competition in the context of the delegation of new gTLDs. As an example, in the case of gTLDs representing regulated sectors (such as .bank and .pharm), governments have proposed measures aimed at ensuring that only entities having the appropriate authorisations to operate in the respective sectors could register domain names in such gTLDs.

The protection of geographical names and indicators appears to be another area of concern: ICANN stopped the delegation process for .amazon to Amazon (the online retailer) after Latin American countries raised a strong opposition within the GAC. Delegation of .wine/.vin has been intensively debated within the GAC, with countries such as Switzerland and France asking for measures that would prevent the 'abusive registration' of domain names representing names of wines for which geographical indications exist (in certain jurisdictions). When ICANN assigned. Africa to a consortium whose application had been endorsed by countries members of the African Union (AU), this decision was contested by a private company.

The management of country domains

The management of ccTLDs involves three important issues. The first concerns the often politically controversial decision as to exactly which country codes should be registered when dealing with countries and entities with unclear or contested international status (e.g. newly independent countries, resistance movements). One controversial issue was the allocation of a Palestinian Authority domain name.[34] In justifying its decision to assign the .ps TLD, IANA reiterated the principle of allocating domain names in accordance with the ISO 3166 standard for country codes, as was proposed by Jon Postel, one of the founding fathers of the Internet.

The second issue concerns who should manage ccTLDs. Currently, there are several registry models in place for ccTLDs.[35] In some cases, the registry functions are performed by a public entity (a national telecom regulatory authority, a research institute within the government, a public university, etc.). There are also countries where the government sets the rules for the management of the ccTLD, but leaves the actual administration in the hands of the private sector. In yet other instances, private companies manage the ccTLDs, with no involvement from the governmental side. In addition, there are several multistakeholder ccTLD registries, whose management structures include representatives of various stakeholder groups.[36]

If, in the early days of the Internet, governments did not seem to be very interested in ccTLDs, things have changed over the years, with some governments trying to gain control over their country domains, which they consider to be national resources. National governments have chosen a wide variety of policy approaches.[37] Transition (re-delegation) to a new institution managing the ccTLD (delegee) within each country is approved by ICANN only if there is no opposition from any of the interested stakeholders within the country.

The third issue relates to the fact that, unlike the case of gTLDs, ICANN imposes no rules as to who should manage ccTLDs, and how these should be managed. ICANN goes only as

far as delegating or redelegating ccTLDs on the basis of some high-level guidelines aimed at ensuring that the ccTLD registry is technically competent to manage it, and that it has the support of the local community to do so.[38]

In 2005, ICANN's GAC adopted a set of Principles and Guidelines for the delegation and administration of country code top level domains,[39] intended to serve as a guide to the relationship between governments, ccTLDs, and ICANN. One of the key principles outlined in this document, which does not have a legally binding status, is subsidiarity, according to which 'ccTLD policy should be set locally, unless it can be shown that the issue has global impact and needs to be resolved in an international framework.'

As mentioned before, there are several ccTLD registries (such as those in Brazil, Chile, Netherlands, Sweden, and the United Kingdom, among others) that have concluded some type of agreement with ICANN, setting up high-level principles for the relation between them. There are also many registries represented in ICANN's Country Code Names Supporting Organization (ccNSO), which develops and recommend global policies to the ICANN Board for a limited set of ccTLD-related issues (such as the introduction of Internationalised Domain Names (IDNs)). However, at the same time, some ccTLD registries have shown reluctance to become part of the ICANN system (in September 2016, ccNSO had 161 members, while there were more than 240 ccTLDs in existence at that time).

Country domain operators are organised at regional level: Europe – Council of European National Top Level Domain Registries (CENTR), Africa – Africa Top Level Domains Organization (AFTLD), Asia – Asia Pacific Top Level Domain Association (APTLD), and Latin America and the Caribbean – Latin American and Caribbean ccTLDs Organization (LACTLD).

Internationalised domain names

The Internet was originally a predominantly English-language medium. Through rapid growth, it has become a global communication facility with an increasing number of non-English-speaking users. For a long time, the lack of multilingual features in the Internet infrastructure was one of the main limits of its future development.

In May 2010, after a long testing period and political uncertainties, ICANN started approving TLDs in a wide variety of scripts, such as Chinese, Arabic, and Cyrillic. IDNs have been introduced in several countries and territories as equivalent to their Latin ccTLDs. For example, in China, 中国 has been introduced in addition to .cn, while in Russia, рф has been introduced in addition to .ru. IDNs are also part of ICANN's New gTLD Program, allowing for the registration of new gTLDs in scripts other than Latin; for example, .сайт (website) and .онлайн (online) are among the new TLDs available to the public.

The introduction of IDNs is considered to be one of the main successes of the Internet governance regime. There are, however, remaining technical obstacles, particularly related to enabling the entire e-mail address being used in any script: while the TLD in e-mail addresses can already be an IDN, the initial part of the e-mail (i.e., the one before the @ sign) still needs to be written in Latin script. Recognition of IDNs by search engines also remains an issue that needs to be tackled. Besides this technical issue, with which dedicated ICANN groups are dealing, there remains a challenge to actually make IDNs widely used; this requires raising awareness about this option in countries using a non-Latin script. Creation of services and content should also be a high priority.

www.igbook.info/dns

Root zone and root servers

At the top of the DNS hierarchical structure, the root zone and root servers have attracted a lot of attention, especially in policy and academic discussion on Internet governance issues.

The current situation

The function and robustness of the DNS can be illustrated by analysing the concern that the Internet would collapse if the root servers were ever disabled.

The root zone is the highest level in the DNS technical structure. The root zone file contains the lists of names and IP addresses of all TLDs (both gTLDs and ccTLDs) in the DNS.[40] The management of the root zone is carried out by PTI, ICANN's subsidiary entrusted with the operation of the IANA functions. In performing this role, PTI assigns the operators of TLDs and maintains a database with their technical and administrative details. The maintenance (update) of the root zone file itself is performed by VeriSign. This root zone maintainer function was initially performed on the basis of a cooperative agreement between VeriSign and the US government, which, in the context of the IANA stewardship transition, was replaced with an agreement between ICANN and VeriSign.

The DNS root zone is served by root servers – also known as authoritative servers, which keep the public copy of the root zone file. There is a misconception that the total number of root servers is 13. The fact is that there are hundreds of root servers[41] scattered at various locations around the world. The number 13 comes from the 13 different hostnames,[42] due to a technical limitation in the design of the DNS. Twelve entities – academic/public institutions (6), commercial companies (3), and governmental institutions (3) – manage these primary instances and ensure that all root servers within the same instance have the updated copy of the root zone file.

If one of the 13 hostnames crashes, the remaining 12 would continue to function. Even if all 13 went down simultaneously, the resolution of domain names into IP addresses (the main function of root servers) would continue on other domain name servers, distributed hierarchically throughout the Internet.

The system of root servers is considerably strengthened by the Anycast scheme,[43] which replicates root servers throughout the world. This provides many advantages, including an increased robustness of the DNS and the faster resolution of Internet addresses (with the Anycast scheme, the resolving servers are closer to the end-users).

Therefore, hundreds of domain name servers contain copies of the root zone file and an immediate and catastrophic collapse of the Internet could not occur. It would take some time before any serious functional consequences would be noticed, during which time it would be possible to reactivate the original servers or to create new ones.

As mentioned before, the root zone file is maintained and updated by VeriSign. When, for example, a new gTLD is approved by ICANN, this information is passed on to VeriSign, which makes the necessary changes into the root zone (introducing the new gTLD into the root) and distributes the revised root zone file to the root name servers.

The issues

Alternative roots – feasibility and risks

One might ask why ICANN would have the exclusive right to dictate the list of TLDs and the way those resolve into IP addresses – could there be no alternative options to the current DNS system? While ICANN – via PTI, as the IANA functions operator – operates and administers the official DNS root that most users of the public Internet use in order to resolve domain names into IP addresses, several organisations operate active alternative DNS roots (Alt Roots). While such organisations offer their own array of TLDs – usually quite different from the ICANN TLD list – end-users wanting to use such a service have to reconfigure their network settings to deviate from the universal root to the alternative root. One of the first Alt roots is the AlterNIC which was founded in 1995, and remained functional until the formation of ICANN in 1998.

Several other attempts to create an alternative DNS have been made by Open NIC, New.net, and Name.space. Most of them were unsuccessful, accounting for only a few per cent of Internet users.

Currently, there are several alternative DNS servers up and running, including Google DNS, Open DNS, Advantage DNS, and ScrubIT.[44]

Another relatively recent and more ambitious project – the Yeti DNS Project, launched in 2015 – plans to 'build a parallel experimental live IPv6 DNS root system to discover the limits of DNS root name service'.[45]

Creating an alternative root name server system is technically straightforward. The main question is how many followers an alternative system would have, or, more precisely, how many computers on the Internet would point to the alternative servers, when it comes to resolving domain names. Without users, any alternative DNS would be useless.

Conceptual discussion: single vs alternative root server system

For a long time, the principle of the single root name server system was considered one of the main Internet mantras, which were not supposed to be touched or even discussed. Various arguments have been put forward to prevent any discussions about alternatives to the single system. One argument is that the current system prevents the risk of the DNS being used by some governments for censorship. However, the censorship argument against changes in DNS policy is losing ground on a functional basis. Governments do not need control over the DNS system or the root zone file in order to introduce censorship. They could rely on more effective tools, based on the filtering of web traffic.

A more solid argument is that any alternative root systems could lead towards the fragmentation and even, maybe, the ultimate disintegration of the Internet. Even though all the root systems use the same system of IP numbers, they use different naming approaches and resolution techniques. It may happen that several root systems have the same domain name, but each resolves it to a different IP address. Since most of the alternative DNS roots, however, are not interoperable – with the ICANN's DNS root or among themselves – their co-existence breaks the principle of universal resolvability, which ensures that there is a single way to resolve a TLD to an IP address – unless the alternative roots are used for a strictly private purpose, not publicly. From a DNS perspective, it prevents some parts of

the Internet from reaching other parts. The fragmentation of the Internet could endanger one of the core functions of the Internet – a unified global communication system. How realistic is this danger.[46]

www.igbook.info/root

Network neutrality

The Internet's success lies in its design, which is based on the principle of net neutrality. From the outset, the flow of all the content on the Internet, whether coming from start-ups or from big companies, was treated without discrimination. New companies and innovators did not need permission or market power to innovate on the Internet. With the growth in use and the development of new digital services, especially the ones consuming high bandwidth such as high-quality video streaming, some Internet operators (telecom companies and ISPs) started prioritising certain traffic – such as their own services or the services of their business partners – based on business needs and plans, justifying such an approach with a need to raise funds to further invest in the network. Net neutrality proponents, on the other hand, strongly fight back such plans arguing this could limit open access to information and online freedoms, and stifle online innovations.

The importance of net neutrality to the success of the Internet is key. The debate on maintaining the principles of net neutrality has attracted a wide range of actors, from US President Obama to human rights grassroots activists. The way in which net neutrality is treated can influence the future development of the Internet.

The current situation

One has to make a distinction between network neutrality and network traffic management. Since the early days of dial-up modem connection to the Internet, network traffic management has been used to deal with a gap between available bandwidth and the users' bandwidth needs. In order to address this challenge and provide quality service, Internet operators (telecom companies and ISPs) – also commonly referred to as carriers – have used various traffic management techniques to prioritise certain traffic. For example, Internet traffic carrying voice conversation over VoIP services (e.g. Skype) should have priority over traffic carrying a simple e-mail: while we can hear delays in Skype voice chat, we won't notice minor delays in an e-mail exchange.

The need for traffic management is especially important today with the extended demands for high bandwidth: a growing number of users regularly use Internet voice and video calls (Skype, Google Hangout, teleconferencing), play online games, or watch TV shows and movies in high definition (HD) quality (e.g. services like Hulu or Netflix). Traffic management is important for wireless communication due to, on one hand, expansion of use of mobile devices and, on the other hand, the technical limits of the wireless spectrum.[47] Traffic management is becoming increasingly sophisticated in routing Internet traffic in the most optimal way for providing quality service, preventing congestion, and eliminating latency and jitter.

The first discord in the interpretation of the principle of net neutrality focused on whether any traffic management at all should be allowed. Net neutrality purists argued that 'all bits are created equal' and that all Internet traffic must be treated equally. Telecoms and ISPs challenged this view arguing that it is users who should have equal access to Internet services and if this is to happen, Internet traffic cannot be treated equally. For example, if both video and e-mail traffic are treated equally, users will not have good video-stream reception, yet they would not notice a few seconds delay in receiving an e-mail. Even net neutrality purists have ceased to question this rationale.

The issues

In the net neutrality debate, there is an emerging consensus around the need for appropriate traffic management. The main question is how to determine what is appropriate. Apart from technical concerns, there are two areas where the debate on traffic management and net neutrality is particularly heated: the economic aspect and human rights issues.

The economic aspect

During the past few decades, many significant network operators – including telecoms and ISPs – have started to change their business models: besides providing Internet access to households and businesses, they have introduced their own VoIP or IPTV services, video on demand, music or video download portals, etc. They are now competing not only with their counterparts for providing cheaper, faster, and better quality connections, but also with the OTT service providers – content and service providers like Google, Facebook, Netflix, and Skype.

Traffic management may be an important tool when competing in service and content provision by prioritising packages according to business-driven preferences. For instance, an operator may decide to slow down or fully ban the flow of data packages from a competing company (such as Skype or Google Voice) to end-users through its network, while giving priority to data packages of its own in-house service (such as the IP telephony or Internet television it offers to its customers).[48]

At the same time, operators argue that the demand for more bandwidth – spurred mostly by OTT services – requires increased investments in basic infrastructure. They argue that, since OTT service providers are the ones contributing the most to the expanded demand and benefiting the most from the improved infrastructure, a multi-tiered network policy model requiring these providers to contribute financially would guarantee the required quality of service for OTT services customers. Once again, such cases demonstrate how traffic management is used for economic rather than technical reasons.

In an attempt to increase revenues, the telecom industry has designed new business models or arrangements.

Zero-rating services, offered to customers by mobile telecom providers, allow unlimited (free) use of specific applications or services. In some cases, access to such applications or services does not count towards a subscriber's data threshold, while in other arrangements, users are allowed access even without a data plan. Although it is increasingly present throughout the world, zero-rating has become a controversial subject. On the one hand, it is seen by some as particularly important in developing and least developed countries, where access to mobile data services is more expensive than the average income. One of the

main arguments in favour of zero-rating is that it lowers the cost of access to online information (when offered as part of a data plan), and gives access to (some) online information to users who cannot afford a data plan (when access is free of charge). Supporters argue that access to some information is preferable to no access at all; in addition, offering users free access to certain types of applications could generate demand for general Internet access, thus encouraging operators to invest in building and deploying infrastructures.

On the other hand, opponents argue that zero-rating prioritises certain services over others, and, as such, challenges the net neutrality principle while harming market competition and innovation. Some have also expressed concerns over the implications that zero-rating could have on users' human rights, in that such services can conflict with a user's right to information (seen as part of the broader right to freedom of expression).

Debates on zero-rating have become more intensive following the introduction of the Free Basics service in 2014. Offered by Facebook in several developing and less developed countries, the service allows users of mobile communications to access applications such as Wikipedia and AccuWeather (in addition to Facebook) without incurring data charges. These debates have led to the service being suspended in some of the countries where it had been previously introduced (such as India and Egypt).

At the same time, besides zero-rating services, telecoms also refer to 'specialised services' – such as HD video streaming offers that require high bandwidth, or future e-health solutions – that may be offered in future and would require high quality and therefore special treatments.

Proposals for a multi-tier Internet have been at the heart of discussions on net neutrality for years. One such proposal was the Legislative Framework Proposal for an Open Internet,[49] put forward by Verizon and Google in 2010, in which the business tier was proposed in the form of 'additional online services'. Proponents of such models argue this would bring more choice of services for users and would encourage investment in the infrastructure; opposers fear that this would be detrimental to the best effort network, since both economic and business tiers would effectively use same 'pipes' (i.e., wireless spectrum and cables).

In the meantime, the market has brought changes in the way the Internet works: in order to reduce transit costs and time, content providers have come closer to users by setting up

Multi-tier Internet

Internet traffic is currently delivered with 'best effort': this implies no guarantees of a particular QoS, effective speed, or delivery time of data packages. Instead, users share the available bandwidth and obtain variable bit rates (speed) depending on the traffic load at the time.[50] Traffic management therefore plays an important role in the effective quality of service for end-users.

The multi-tier Internet concept refers to introducing a 'business tier' to the Internet, i.e., special services with a guaranteed QoS beyond best effort. Proponents explain that the business tier would run in parallel with the economic tier (the Internet as we know it now), which would remain based on best effort. OTT service providers would have the choice to run their services, at cost through the business tier, or without cost through the best effort network.

Content Delivery Networks (CDNs) – caching servers placed close to regional Internet Exchange Point (IXP) hubs or within big regional telecoms. This has improved network performance and costs. While initially it was mainly the big content providers that could afford (and needed) a CDN, the emergence of a market for data centres and cloud providers allows the service of a CDN to be available on the open market, which enables anyone with a cloud service that needs to serve users around the globe to rent the services of a CDN.

Human rights issues

The consequences of violating net neutrality principles are not only economic. The Internet has become one of the key pillars of modern society linked to basic human rights, including access to information, freedom of expression, health, and education. Endangering Internet openness could thereby impact fundamental rights.

In addition, the ability to manage network traffic based on origin or destination, on service or content, could give authorities the opportunity to filter Internet traffic with objectionable or sensitive content in relation to the country's political, ideological, religious, cultural, or other values. This opens possibilities for political censorship through Internet traffic management.

Users or customers?

The net neutrality debate triggers linguistic debates. Proponents of net neutrality focus on Internet 'users', while the others – mainly commercial players – describe them as 'customers'. Internet users are more than simply customers; the term 'user' implies active participation in the development of the Internet through social networks, blogging, and other tools and the important role they have in deciding the future of the Internet. Internet services customers, on the other hand, like any other customers, can decide whether or not to purchase the services on offer. Their status on the Internet is based on a contract with the ISP and customer protection rules. Beyond that, customers are not supposed to have any role in deciding how the Internet is run.

Who are the main players and what are their arguments?

The position of the main players in the net neutrality debate is in a state of constant flux. Some of the main proponents of net neutrality include consumer advocates, online companies, some technology companies, many major Internet application companies including Google, Yahoo!, Vonage, eBay, Amazon, EarthLink, and software companies like Microsoft.

Opposers of net neutrality include the main telecom companies, ISPs, producers of networking equipment and hardware, and producers of video and multimedia materials. Their arguments against regulations to network traffic management are market-centred, starting from the need to offer what consumers want. Contrary to the common tendency for telecom operators to oppose any regulation on net neutrality, the European Telecommunications Network Operators (ETNO) proposal to WCIT-12 requested international regulation to prevent further national regulations protecting net neutrality. Their US counterparts – like Verizon – however, oppose the ETNO initiative.[51]

The four main arguments in the net neutrality debate are summarised in Table 1.

Table 1. Main arguments in the net neutrality debate

Argument	Proponents of net neutrality	Opponents of net neutrality
Past/future argument	New Internet companies developed thanks to the Internet's open architecture, and end users are benefiting from innovation and diversity of services thanks to net neutrality. Net neutrality will preserve the Internet architecture that has enabled the fast and innovative development of the Internet so far.	Traffic management is inevitable, and neutrality has never existed. Besides, there are already non-neutral leased services like VPNs (virtual private networks). Without net neutrality restrictions, Internet companies can develop new services for customers, with guaranteed QoS.
Economic argument	Without net neutrality, the Internet will look like cable TV: a handful of big companies will control access and distribution of content, deciding what users get to see and how much it costs them to see it. New entrants and small businesses will not have a chance to develop, especially those in developing countries. OTT service providers already pay a lot to telecoms for their Internet connections, and invest in infrastructure like caching servers.	Without net neutrality restrictions in commercial agreements with content and service providers, telecom operators will be able to raise funds which would make them more interested in investing in better infrastructure. Better infrastructure will encourage new services and innovations, more tailored to customers' needs, bringing more revenue to all. OTT service providers will also find value in possible innovative services with QoS, enabled by the operators if not restricted by net neutrality provisions.
Ethical argument	The Internet is the result of developments by many volunteers over decades. They invested time and creativity into everything from technical protocols to content. The Internet is more than a business – it has become a global heritage of mankind. It is not justifiable to have such a huge investment of time and creativity harvested by only a few companies who will lock the Internet in constrained business models by breaching net neutrality, and turn the creativity of many into the profit of a few.	Net neutrality is ethically questionable because operators have to invest in maintaining and expanding the Internet's infrastructure to support new services, while most benefits are reaped by Internet 'content' companies such as Google, Facebook, and Amazon.
Regulation argument	Net neutrality must be imposed by government to preserve the public interest. Any form of self-regulation will leave it open for operators to breach the principle of net neutrality. The open market is not a sufficient mechanism since major global telecoms are at the core of the Internet infrastructure. Even if there is a possibility to choose, this is not always realised since users need technical and legal literacy and awareness of the consequences of the various choices available.	The Internet has developed because of very light or no regulation. Heavy government regulation could stifle creativity and the future development of the Internet. The open market is based on choice, and users can always change their Internet provider if not satisfied with the offer. The users' choice and the market will kill bad offers and sustain good ones.

The basic principles

In recent years, policy debates and regulations have crystallised a few key principles for net neutrality:[52]

- Transparency: Operators must provide complete and accurate information on their network management practices, capacity, and the quality of their service to customers, in a form understandable by an average user.

- Access: Users should have [unrestricted] access to any [legal] content, service or application [with minimum QoS guaranteed for meaningful use, as prescribed by the regulator] or to connect any hardware that does not harm the network.

- (Non)discrimination: Operators should make no discrimination [or only reasonable discrimination] of traffic based on:
  - Origin of sender or receiver.
  - Type of content, type of application and service [with fair competition – no discrimination against undesired competitors or OTT service providers' services].
  - Where 'reasonable' could be any practice for public benefit (assuring QoS, security and resilience of network, innovations and further investments, lowering costs, etc.) but not for business advantage only.

Other principles most frequently debated in international forums such as the global IGF and the European Dialogue on Internet Governance (EuroDIG) include:

- Preserving freedom of expression, access to information, and choice.

- Assuring minimal QoS and security and resilience of the network.

- Preserving incentives for investments.

- Stimulating innovations [including opportunities for new business models and innovative businesses, i.e., new entrants].

- Defining rights, roles, and accountability of all parties involved (providers, regulators, users) including the right to appeal and redress.

- Preventing anti-competitive practices.

- Creating a market environment that would allow users to easily choose and change their network operator.

- Protecting the interests of the disadvantaged, such as people with disabilities and users and businesses in the developing world.

- Maintaining diversity of content and services.

Policy approaches

With the net neutrality debate, another question has come to the fore: what is the role of the legislators and regulators in broadband policy and operator practices? One of the major challenges regulators face is whether to act pre-emptively (ex-ante), in order to prevent possible breaches of the net neutrality principle, or to respond based on precedents (ex-post) once (and if) the breach occurs. Another challenge that legislators and policymakers face is whether the problem should be dealt with, with 'hard law' – encoding the principles into legislation – or if 'soft law' (guidelines and policies) would be sufficient.[53]

Developed countries

In the USA, the Federal Communications Commission (FCC) adopted a set of rules in favour of net neutrality. Entered into force in June 2015, the rules allow the FCC to regulate

broadband services as a utility and to prohibit wired and wireless broadband providers to introduce unreasonable practices that the FCC considers to harm the open Internet: blocking of lawful content, applications, services or devices; impairing or degrading lawful Internet traffic on the basis of content, application, or service (throttling); and paid prioritisation of certain content, applications, or services.[54] Telecom providers have challenged the rules in court, arguing that they would negatively impact innovation and investments in infrastructure, but their claims were denied by a federal appeals court in June 2016.[55] However, it is expected that the providers will continue their 'battle' against the FCC rules.

At EU level, the Regulation on open Internet access, adopted in November 2015, sets out the obligation for providers of Internet access services to treat all traffic equally, when providing internet access services, without discrimination, restriction, or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used.[56] The regulation also deals with the concept of 'specialised services', allowing operators to offer 'services other than internet access services which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality'. [57] In August 2016, the Body of European Regulators for Electronic Communications (BEREC) published a set of guidelines for national regulatory authorities on how the EU regulation should be implemented, including by closely monitoring and ensuring 'compliance with the rules to safeguard equal and non-discriminatory treatment of traffic in the provision of Internet access services and related end-user rights'.[58]

Brazil,[59] Chile,[60] Slovenia,[61] and the Netherlands[62] protect net neutrality by national legislation. Norway, on the other hand, has chosen a soft-law approach, with the national regulatory authority issuing a set of guidelines for net neutrality (drafted in collaboration with various industry players, such as ISPs, industry organisations, content providers, and consumer protection agencies).[63]

Developing countries

Due to limited infrastructure and bandwidth, regulators of developing countries put more focus on fair usage policy – affordable prices and fair access for all. Some raise concerns over cross-border non-discrimination, saying that the traffic from all countries should be treated the same way with no preferences based on termination costs. Also, certain countries have more sensitivity to internal cultural, political, or ethical aspects, thereby understanding '(in)appropriate use' and management differently than others.

Concerns have been raised that the innovative models of the developed world might hamper developing markets: by prioritising the services of big Internet companies, emerging business and competition would be additionally downsized, threatening innovation, local content and services, and media diversity. As mentioned earlier, some countries have already taken strong positions in favour of net neutrality by banning zero-rating practices. Other positions may include allowing national telecoms to charge global OTTs for priority, thereby adding to the income of incumbent telecoms; or, on the contrary, enforcing net neutrality on a national level in order to attract the OTTs to operate outside the USA.

International organisations and NGOs

Many international organisations and user groups have also developed policy positions with regard to net neutrality. The CoE, within its 2010 Declaration of the Committee of

Ministers on network neutrality and the 2016 Recommendation of the Committee of Ministers on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality emphasise the fundamental rights to freedom of expression and information.[64] The Internet Society approaches net neutrality from a user-centric perspective, focusing mostly on the following issues: allowing freedom of expression, supporting user choice, and preventing discrimination.[65] The Trans Atlantic Consumer Dialogue (TACD), a forum of US and EU consumer organisations, additionally emphasises requests for carrier non-discriminatory behaviour, calling on the USA and the EU to defend the principles of openness and neutrality of the Internet.[66] Net neutrality and a multi-tiered Internet were heavily discussed within the WCIT-12 process. The final NETmundial document[67] in 2014 did not include net neutrality among the agreed principles, but has invited further discussions on the topic, especially within the IGF.

Many NGOs are especially concerned about the future of non-commercial and non-competing online content and services, requesting these to be broadcast through any carrier network equal to commercial ones. They also emphasise the rights of marginalised groups – especially people with disabilities – to use content, services, and applications (including those that demand high-bandwidth) for their needs without any limits whatsoever.

Open issues

There are a number of open issues on the net neutrality debate agenda:

- Where should the balance be between public good effects of the Internet and user (and human) rights, on the one hand, and the rights of the providers to innovate within the networks they own, on the other?
- Would an unregulated market with open competition, as advocated by the carriers, provide unlimited (or sufficient) choice for users? And would the users be able to make meaningful decisions?[68] Or should the regulators inevitably be empowered as safeguards, and if so, with what authority?
- How would different legal and regulatory approaches impact the broadband market and further investment and innovation?
- What are the implications of net (non)neutrality for the developing world?
- What are the implications of a tiered Internet for competition, innovation, investment, and human rights?
- Should zero-rating tariffs or the development of CDNs be considered a 'tiered Internet'?
- Will the dominant OTT – both content and service providers – find a tiered Internet and possible new services a lucrative business model as well? In such case, will they be able to adapt it to include the users of developing countries, or will those be left out?
- Can telecom operators innovate their business models to grow their revenues without violating net neutrality (following successful examples of iTunes, Google, and other OTT service providers, and the potential for partnerships between OTT service providers and operators)?

- Will the need for traffic management for technical (quality) reasons be outdated in future, due to advancements in carrier technology?
- How will the growing dependence on clouds and the IoT influence the debate on net neutrality, and vice versa?
- Should the debate be extended from traffic management on a carrier level to content and application management on content and application provider level, such as Google, Apple, or Facebook?
- Will consumer protection continue to be intrinsically linked to net neutrality?
- If net neutrality is 'defeated', what principles will support consumer protection in the future?

www.igbook.info/netneutrality

Technical and web standards

Technical standards

The Internet technical standards ensure that hardware and software developed or manufactured by various entities can not only connect to the Internet, but also work together as seamlessly as possible. Standards therefore guide the technical community, including manufacturers, to develop interoperable hardware and software. As explained previously, TCP/IP is the main Internet technical standard.

The establishment of technical infrastructure standards

The process of standardisation can be very long in any industry. Given that ICT companies implement new technologies at a fast pace, the ITU had to adapt to real-time conditions and so streamlined its standardisation workflow into few months. Still, some important standards may take years to be adopted. For example, the ITU expects the so-called 5G networks to be standardised by 2020.[69]

Besides the ITU, technical standards are increasingly being set by private and professional institutions. The Internet Architecture Board (IAB) oversees the technical and engineering development of the Internet, while most standards are set by the IETF as Request for Comments (RFC). Both the IAB and the IETF have their institutional home within the Internet Society.

Other institutions include the Institute of Electrical and Electronic Engineers (IEEE), which develops standards such as the WiFi standard (IEEE 802.11b); the WiFi Alliance, which is the certification body for WiFi-compatible equipment; and the Groupe Speciale Mobile Association (GSMA), which develops standards for mobile networks.

The very function of setting or implementing standards in such a fast developing market affords these institutions considerable influence.

Standards that are open (open Internet standards) allow developers to set up new services without requiring permission. Examples include the www and a range of Internet protocols. The open approach to standards development has been affirmed by a number of institutions. The Open Stand initiative, for example, encourages the development of open and global market-driven standards, and is endorsed by bodies such as the IEEE, the IETF, the IAB, and the Internet Society.

Technology, standards, and policy

The relevance of setting of implementing standards in such a fast developing market gives standard-setting bodies a considerable amount of influence.

Technical standards could have far-reaching economic and social consequences, promoting specific interests and altering the balance of power between competing businesses and/or national interests. Standards are essential for the Internet. Through standards and software design, Internet developers can, for example, shape how human rights are used and protected (e.g. freedom of information, privacy, and data protection).

Efforts to create formal standards bring private technical decisions made by system builders into the public realm; in this way, standards battles can bring to light unspoken assumptions and conflicts of interest. The very passion with which stakeholders contest standards decisions should alert us to the deeper meaning beneath the nuts and bolts.

Web standards

Web standards are a set of formal standards and technical specifications for the www. They ensure that content is accessible across devices and configurations, and therefore provide the core rules for developing websites and Internet applications. The main content and applications standards include HyperText Markup Language (HTML) (HTML5 is the fifth and current version of the HTML standard), a plain text language which makes use of tags to define the structure of the document; XML, another type of language used for sharing structured information; Cascading Style Sheets (CSS), a language used in conjunction with HTML to control the presentation of web pages; and eXtensible HTML (XHTML), an extended version of HTML which uses stricter rules.

The evolution of web standards

By the late 1980s, the battle of network standards was over. TCP/IP gradually became the main network protocol, marginalising other standards, such as the ITU-supported X-25 (part of the Open Systems Interconnection architecture) and many proprietary standards, such as IBM's systems network architecture (SNA). While the Internet facilitated normal communication between a variety of networks via TCP/IP, the system still lacked common applications standards.

A solution was developed by Tim Berners-Lee and his colleagues at the European Organization for Nuclear Research (CERN) in Geneva, consisting of a new standard for sharing information over the Internet, called HTML (really just a simplification of an existing standard from the International Organization for Standardization (ISO), called SGML – Standard Generalized Markup Language). Content displayed on the Internet first had to be organised according to HTML standards. HTML, as the basis of the www, paved the way for the Internet's exponential growth.

Since its first version, HTML has been constantly upgraded with new features. The growing relevance of the Internet has brought the question of the standardisation of HTML into focus. This was particularly relevant during the Browser Wars between Netscape and Microsoft, when each company tried to strengthen its market position by influencing HTML standards. While basic HTML only handled text and photos, newer Internet applications required more sophisticated technologies for managing databases, video, and animation. Such a variety of applications required considerable standardisation efforts in order to ensure that Internet content could be properly viewed by the majority of Internet browsers.

Application standardisation entered a new phase with the emergence of XML, which provided greater flexibility in the setting of standards for Internet content. New sets of XML standards have also been introduced. For example, the standard for the distribution of wireless content is called Wireless Markup Language (WML).

Setting web standards

The main web standard-setting institution is the W3C, headed by Tim Berners-Lee. Standards are developed through an elaborate process which aims to promote consensus, fairness, public accountability, and quality. After extensive consensus-building, standards are published in the form of Recommendations.[70]

W3C standards define an open platform for the development of applications, which enables developers to build rich interactive experiences. W3C states that 'although the boundaries of the platform continue to evolve, industry leaders speak nearly in unison about how HTML5 will be the cornerstone for this platform.'[71]

It is interesting to note that in spite of its high relevance to the Internet, so far, the W3C has not attracted much attention in the debate on Internet governance.

www.igbook.info/standards

Cloud computing

What cloud computing is and how it works

Cloud computing (Figure 9) could be described as the shift from storing data on hard disks on our computers to storing them in servers in the clouds (i.e., big server farms). Cloud computing offers ubiquitous access to our data and services from any device anywhere around the world (where there is an Internet connection). At the same time, the fact that our data are stored with a third party – often in pieces and copies scattered across several jurisdictions – raises concerns for privacy and data protection. Security of the cloud is likely to be on a much higher level than of our own computers, as security breaches at the level of cloud systems could provide access to vast amounts of data.

The first wave of cloud computing started with the use of online mail servers (Gmail, Yahoo!), social media applications (Facebook, Twitter) and online applications (Wikis, blogs, Google Docs). Apart from everyday applications, cloud computing is extensively used for business software. More and more of our digital assets are moving from our hard

disks to the cloud. The main players in cloud computing are Google, Microsoft, Apple, Amazon, and Facebook, who either already have or plan to develop big server farms.

In a way, cloud computing closed a circle in the development of computer technology. In the early days of computers, there were powerful mainframe computers and 'dumb' workstations. The power was in the centre, at the powerful servers. The shift of power from powerful servers to end-users' terminals took place when companies such as IBM, Apple, and Microsoft started to produce personal computers. Computer power shifted to computers worldwide. We started storing data on floppy disks and hard disks and executing applications (from text processors to games) on our computers. Then network technologies started connecting these individual computers first within companies and organisations (via Local Area Networks, LANs) and later on globally, via, in particular, the Internet. In the early phase of the public growth of the Internet (until 2005), the Internet was mainly used for the exchange of data, while data were stored on our computers, which also executed core software applications such as word processing.

Another shift started with the growth of social media and the emergence of smartphones and tablets in the last 10 years. In parallel, software and data started moving from our computers to powerful servers in the cloud. This process started with e-mail services such as Gmail, and continued with storing our photos, text files, and other digital resources in the cloud, and increasingly operating software from the cloud as well (such as Google Docs or Microsoft Office 365). Today, most of our digital assets are stored in centralised servers in the cloud. In a way, we closed the circle from an early centralised network architecture, via decentralised personal computers, to centralised storage in the cloud.

Figure 9. Cloud computing

A cloud set-up consists of three layers: hardware, middleware or platform, and application software. Based on what is rented by the user, there are three types of cloud services:

- Software as a Service (or SaaS), in which a cloud provider provides the user with access to software applications, thus allowing the user to access such applications (as well as the data produced through them) from any device connected to the Internet. Here, the user has no control over any of the cloud resources, but can only use the application available. This is the most dominant type of service where the end-user application is an entry point for use – such as in the case of Twitter or an application for the central database in the local organisation.

- Platform as a Service (or PaaS), where the user themself can develop an application that would run on the rented cloud platform. This way, the user can decide on particular hardware resources they want to use; yet they still won't have the possibility of adjusting the server or storage setting. Standardisation is important especially with regard to the platform, because it enables developers to address a wide range of potential customers and gives users choice.

- Infrastructure as a Service (or IaaS) is the least used cloud service among wider population, since it requires advanced IT skills, though it allows for the greatest freedom in choosing how to use the resources. In IaaS, the provider only provides hardware resources (computing power or storage), while the user needs to set up the services, including the operating system.

Legal and policy aspects related to cloud computing

Cloud servers as critical information infrastructure

Most Internet applications run from cloud servers. In the pre-cloud era, when the Internet went down, damage was limited to the lack of availability of service – we were not able to send e-mails or browse the web. In the era of cloud computing, we may not even be able to write text or do calculations, as these tasks are performed through cloud-based applications. The high relevance of cloud services for millions of Internet users and companies makes cloud servers part of critical infrastructures at global level and in most societies worldwide.

Security and encryption

The mere fact that a single cloud operator provides service to thousands or millions of people is sufficient to attract the attention of various perpetrators – criminals, terrorists, cyber-spies, or others – to exploit vulnerabilities.

Possible security breaches of the cloud can be categorised according to the well-known information security triad – confidentiality, integrity, and availability (CIA) of the data and the system. To that end, securing the cloud would involve the consideration of a set of measures such as: deciding on access rights to specific segments of data and service, encrypting the entire set of data in the cloud, securing each segment of the ICT system and the network between the cloud and the users, encrypting the data transfer between the cloud and the end-users, and backing up all data stored in the cloud (Figure 10).

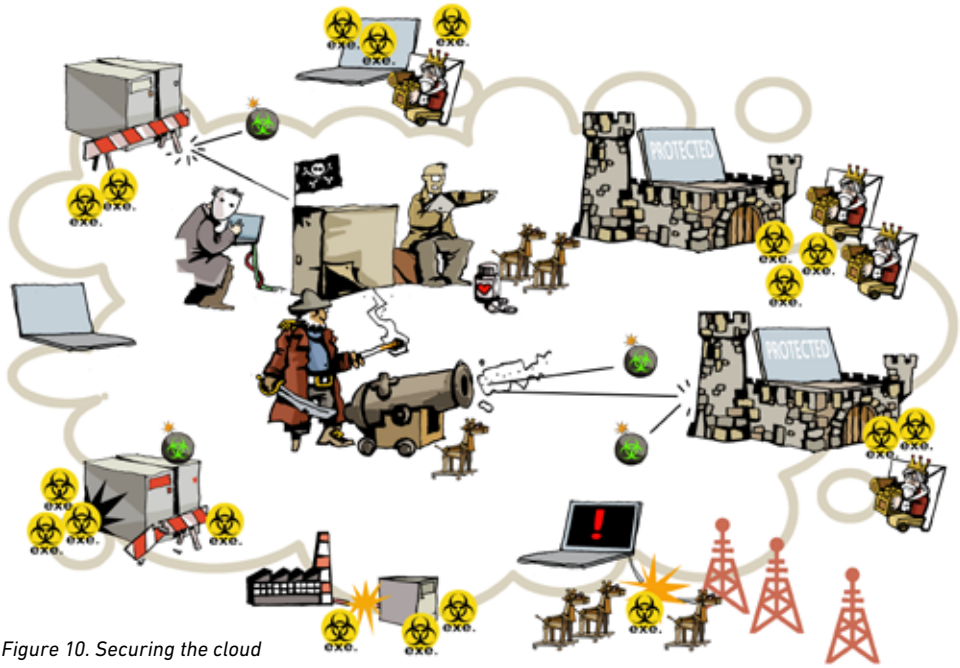

Figure 10. Securing the cloud

Privacy and data protection

With more of our personal data stored on clouds, the questions of privacy and data protection will become central. Will we have control of our text files, e-mails, and other data? Could cloud operators use these data without our permission? Who will have access to our data?

The EU is particularly concerned with privacy and data protection issues in the context of cloud computing. With more and more digital data crossing the Atlantic Ocean, the EU and the USA have tried to address the problem of different privacy regimes, while ensuring that US cloud computing operators comply with EU regulations regarding the protection of EU citizens' personal data and privacy. The replacement of the Safe Harbour agreement (which was declared invalid by the CJEU in October 2015) with the Privacy Shield (formally adopted in July 2016), is supposed to solve the problem, but it remains to be seen how effective the new agreement will be.

Big data

Most of the big data phenomenon is related to cloud computing. While there is a lot of hype about big data, it is a highly important phenomenon in modern digital developments. In particular, big data will gain new relevance with the fast growth of the Internet of things where cars, home appliances, and even our clothes will start collecting data. Big data will trigger a new type of economic models. It will trigger new demand for cloud resources.

For example, fog computing is being developed as an addition to cloud computing, with the aim of reducing the amount of data that is transferred to the cloud for processing and analysis. As explained by Cisco, fog computing extends the cloud closer to the 'things' that

produce and act on data; this allows data to be analysed closer to where it is collected or produced, thus minimising latency,[72] offloading gigabytes of network traffic from the core network, and keeping sensitive data inside the network.[73]

Data localisation

With a growing volume of information assets going digital, countries are becoming uncomfortable with having national data assets outside national borders. Some of them are adopting, or exploring the possibility of adopting, policies imposing data localisation rules (requiring cloud service providers and/or the data they store to be located within national borders).

The motivations for data localisation are different, ranging from economic to political. Economic data localisation is often based on a protectionist economic policy. If data are the key resource of the Internet economy, countries are trying to preserve this resource on their territories and foster the development of a local economy based on data processing and management. Data protection and security considerations can also make governments require that certain data are only processed and stored within the country, thus making national legislation directly applicable to service providers. Moreover, countries have also started exploring the idea of setting up governmental clouds, designed specifically for the processing and storing of governmental/official data. Political reasons for data localisation policies are linked to some countries' interests in controlling political activism, which can arguably be easier to attain when the country has jurisdiction over data servers.

Cloud service providers are trying to find solutions, including technical ones, to overcome localisation policies, while offering their clients the possibility to take advantage of cloud services. As an example, in March 2016, Oracle launched a new cloud computing service that would allow companies to place Oracle cloud servers within their own data centres. According to Oracle, the new service is intended to respond to the needs of organisations that have not adopted cloud computing so far because of legislative or regulatory requirements related to the location of cloud servers.[74]

Standards and interoperability

With diverse operators of cloud computing, the question of standards is becoming very important. Standards are particularly important for interoperability and the transfer of data among different clouds (e.g. from Google to Apple). One possibility which is being discussed is the adoption of open standards by the main players in cloud computing. This is not easy to achieve, though, since major cloud computing companies see their proprietary standards as part of their competitive advantage. Yet, there are several initiatives aimed at achieving interoperability. For example, in 2013, the Open Group (with members such as Fujitsu, IBM, and Oracle) published a Guide to Cloud Computing Portability and Interoperability, containing recommendations to users on how to achieve portability and interoperability when working with cloud products and services, as well as recommendations to suppliers and standards bodies on how standards and best practices should evolve to enable greater portability and interoperability.[75] The IEEE has set up the IEEE Cloud Computing Initiative, which works, among others, on developing standards for intercloud interoperability.

www.igbook.info/cloud

Internet of Things

The IoT extends connection to the Internet mainly from information and communication devices (computers, mobile phones, tablets, and e-readers) towards other devices such as cars, home appliances, clothes, city infrastructure, medical, and healthcare devices.

Estimates for the number of IoT connected devices by 2020 vary between 20 and 100 billion. These devices will generate significant amounts of data particularly valuable for analysis. The International Data Corporation (IDC) has forecasted that, by 2020, the 'digital universe' will reach 44 ZB (zettabytes, i.e., trillion gigabytes), and 10% of this overall amount would come from IoT devices.[76]

Predictions of financial development of IoT industry are growing and plans from manufactures are skyrocketing. Verizon predicts that the worldwide IoT market will grow significantly over the next few years, from $591.7 billion in 2014 to $1.3 trillion in 2019, with a compound annual growth rate of 17%.[77]

A report published by the ITU and Cisco Systems in early 2016 concludes that IoT is a significant development opportunity that can improve living standards throughout the world and substantively contribute to achieving the sustainable development goals. The report outlines the increasing impact that IoT has in areas such as healthcare, education, water and sanitation, resiliency, climate change and pollution mitigation, natural resource management and energy.[78]

IoT devices are often connected in wide systems, typically described as 'smart houses' or 'smart cities'. Such devices both generate enormous amount of data and create new contexts in which data are used**.** IoT devices use the present Internet structure, not a separate/different Internet.

The most common sensors and parts currently used for IoT device communication are the following:

- Radio Frequency identifiers (RFIDs): electronic tags attached to items to enable tracking. Suitable for clothes, pets, box shipping/tracking.
- Universal Product Codes (UPCs): on nearly all products, UPCs are used in supermarket checkout scanning.
- Electronic Product Codes (EPCs): provide a unique identity for every physical object anywhere in the world, all the time. EPCs function like UPCs, but are electronic.

In addition to these, researchers continue to explore other modalities for connecting IoT devices. For example, in a paper published in June 2016,[79] a group of researchers proposes the use of Light Emitting Diode (LED) bulbs for connecting devices in the IoT. They argue that such a system could be a solution to communication challenges in the saturated radio spectrum (given that many IoT devices now rely on the use of radio frequencies).

Even if the size of a single piece of data generated by connected IoT devices could be quite small, the final sum is staggering due to the number of devices that can connect, and the fact that the data can be stored and processed in cloud. Therefore, the cloud computing industry will play a major role in future IoT developments.

IoT industries

Some of the most developed IoT industries include:

- Home automation: Providing access to home appliances from anywhere. There is no unified protocol, no industry web API standard.
- Health monitoring: Actively adjusting your health (insulin pumps remotely adjusted by doctors, pacemaker monitoring, etc.). Creating data on your cycles or habits, yet with many possible security issues and arbitrary data upload.
- Transportation: Using IoT systems to keep track of information such as fuel usage, location, time, distance, as well as to anticipate maintenance needs in vehicles and optimise the use of resources (including fleets). Going a few steps beyond, self-driving cars, currently explored by automakers (such as Tesla and Toyota), as well as companies like Google and Uber, also make use of IoT technologies.

Other industries in which IoT is playing an increasing role include energy, infrastructure, agriculture, manufacturing, and consumer applications. The overall concept of smart cities (where ICTs are integrated into urban services and infrastructures to improve their quality and performance and increase the overall standards of urban life) is also strongly related to IoT.

Private and public initiatives

The business sector is leading major IoT initiatives. While technology companies such as Cisco and Intel continue to develop their portfolios of IoT services, telecom providers have started to deploy IoT-dedicated networks on a larger scale, to encourage the use of IoT.[80] Moreover, companies from different sectors are joining forces in alliances aimed at further contributing to developments in the field of IoT. One example is the Open Connectivity Foundation, whose aim is to contribute to ensuring that IoT devices can communicate with one another regardless of manufacturer, operating system, chipset, or physical transport. The Foundation includes members from diverse sectors, such as automotive, consumer electronics, healthcare, industrial, etc. Another example is the LoRa Alliance, which works in the field of IoT standardisation. The Alliance has developed LoRaWAN – a Low-Power Wide-Area Networks (LPWAN) specification intended to provide seamless interoperability among IoT objects.

Governments are also becoming more and more aware of the opportunities brought by the IoT. They are launching various types of initiatives in this area. The EU, for example, has initiated the Horizon 2020 Work Programme 2016 /2017: Internet of Things Large Scale Pilots for Testing and Deployment, a funding programme aimed at encouraging the take up of IoT in Europe. In the USA, the NTIA has been looking into reviewing the IoT's technological and policy landscape, trying to identify possible roles for the federal government in fostering the advancement of IoT technologies in partnership with the private sector. The Chinese government has created the Chengdu Internet of Things Technology Institute, through which it funds research in various IoT related areas.

The main issues

The IoT generates massive amounts of data, and this has triggered major concerns related to privacy and data protection. Some IoT devices can collect and transmit data that are

of a personal nature (e.g. the case of medical IoT devices), and there are concerns about how the devices themselves are protected (ensuring their security),[81] as well as about how the data they collect is processed and analysed. While information transmitted by an IoT device might not cause privacy issues, when sets of data collected from multiple devices are put together, processed, and analysed, this may lead to sensitive information being disclosed.

The absence of data oversight also raises the issue of ownership of data. Many applications used in IoT are proprietary, alongside the data created and generated through them. There are overhauls in security and privacy (of data, protocol, and devices), hence new regulations might be needed. This is a future development that may require unified, global action and regulation, maybe more than any other in a realm of Internet governance. New social contracts need to be agreed.

With the IoT at the centre of artificial intelligence initiatives which seek to introduce robots, self-driving cars, and other digital systems that have to make judgements and decisions, ethical issues have arisen. Governments and the private sector are increasingly calling for a dialogue on what ethical principles should apply to developments in the fields of IoT and AI, and how could such principles be incorporated into IoT and AI systems.

Ethical issues

IoT, big data, and AI bring ethics into the focus of digital policy. Ethical concerns are not only related to privacy and security, but also to the ethics of decisions that automated machines make. For example, Jigsway, a Google subsidiary, has developed Conversation AI, a set of tools aimed at spotting abuse and harassment on the Internet. While potentially addressing problems related to misuse of the Internet public space, the software also raises a a major ethical issue: How can machines determine what is and what is not appropriate language?[82]

Debate on the ethical implications of new digital technologies has started in both the business and policy sectors. Major Internet companies (IBM, Facebook, Google, Microsoft, Amazon, and DeepMind) have launched a Partnership on Artificial Intelligence initiative, aimed at addressing the privacy, security, and ethical challenges of AI, and initiating a broader societal dialogue on the ethical aspects of new digital developments.[83] A draft report on robotics, prepared in the European Parliament in the first half of 2016 explores, among others, the ethical challenges brought by technological developments in the area of robotics, and recommends the adoption of a 'guiding ethical framework for the design, production, and use of robots', which 'should be based on the principles of beneficence, non-maleficence and autonomy, as well as on principles [...] such as human dignity and human rights, equality, justice and equity, non-discrimination and non-stigmatisation [...]'.[84] In the USA, the National Artificial Intelligence Research and Development Strategic Plan, released in October 2016, emphasises the need to 'determine how to best design architecture for AI systems that incorporate ethical reasoning'.[85] A report on robotics and AI prepared by the Science and Technology Committee in the UK Parliament calls on the government to take proactive measures to tackle ethical questions related to the use of autonomous technologies such as AI.[86]

www.igbook.info/iot

Convergence

Historically, telecommunication, broadcasting, and other related areas were separate industry segments; they used different technologies and were governed by different regulations. The broad and prevailing use of the Internet has aided in the convergence of technological platforms for telecommunication, broadcasting, and information delivery. Today, we can make telephone calls, watch TV, and share music on our computers via the Internet. Only a few years ago, such services were handled by different technological systems.

In the field of traditional telecommunication, the main point of convergence is VoIP. The growing popularity of VoIP systems such as Skype, WhatsApp, and Viber is based on lower price, the possibility of integrating data and voice communication lines, and the use of advanced PC- and mobile-device-based tools. With YouTube and similar services, the Internet is also converging with traditional multimedia and entertainment services. IPTV also sees the convergence between multimedia services and IP-based networks.

While technical convergence is going ahead at a rapid pace, its economic and legal consequences will require some time to evolve.

At international level, governance mechanisms are mainly used for the exchange of best practices and experiences in the field of convergence. The ITU's Telecommunication Development Sector (ITU-D) has a study group on the converging environment. The CoE has a steering committee on media and information, covering one aspect of convergence: the interplay between traditional and new digital media. Convergence is most directly related to net neutrality, the IoT, the role of intermediaries, e-commerce, consumer protection, and taxation.

The issues

The economic implications of convergence

At the economic level, convergence has started to reshape traditional markets by putting companies that previously operated in separate domains into direct competition. As a consequence, convergence has led to fears of the 'Uber syndrome' among business leaders: the scenario in which a competitor with a completely different business model enters the industry and flattens competition.[87] Such was the case when Uber entered the taxi market by innovating on the technological aspect; as a consequence, traditional taxi companies and drivers, who felt their businesses were threatened, filed lawsuits in courts across the world in protest against the new unregulated entrant in the market.

Companies use different strategies to cope with the challenges brought by convergence. One frequent approach has been merger and acquisition, where smaller, new-on-the-market OTT providers merge with or are acquired by larger companies. In a more recent approach, OTT providers and telecom providers have started to enter into partnerships, which bring advantages to both sides: for telecom providers, partnerships with OTT providers may bring them a competitive advantage, as well as added value for end-users; OTT providers, on the other hand, would have their services easier to find and access, thanks to partnerships with carriers.[88]

Regulation in a converging environment

The legal system is the slowest to adjust to the changes caused by technological and economic convergence. Each segment – telecommunication, broadcasting, and information delivery – has its own special regulatory framework. This convergence has opened up several governance and regulatory questions:

- What is going to happen to the existing national and international regimes in such fields as telephony and broadcasting?
- Is there a need for new regulatory regimes that focus mainly on converged services? Or should they be subject to the same regulatory frameworks as, for example, traditional electronic communications services?
- When it comes to competition and consumer protection, what rules, if any, should be imposed on providers of converged services?
- Should the regulation of convergence be carried out by public authorities (states and international organisations) or through self-regulation?

Countries are addressing such questions in various ways. Some countries, such as EU member states, India, and Kenya, have chosen flexible approaches towards regulating convergence, by simply addressing the issues in terms of net neutrality principles, in that users are allowed to choose any type of application or service provided over IP networks. Other countries have chosen to create new legal or regulatory frameworks for converged services; Korea, for example, has a dedicated Internet Multimedia Broadcasting Business Act, which contains provisions on the licensing requirements and service obligations for IPTV. In some countries, convergence is addressed through self-regulation. In Australia, for example, the Communications Alliance (representing various companies in the communications industry) has developed several guidelines on VoIP services.[89]

There are, however, several countries in which converged services, especially VoIP, are (or were, at a point) either explicitly banned through regulation, or simply blocked by telecom providers. Examples include Morocco, Belize, United Arab Emirates, among others.

www.igbook.info/convergence

Endnotes

[1] The terms Internet and www are sometimes used interchangeably; however, there is a difference. The Internet is a network of networks connected by TCP/IP. Sometimes, the term Internet is used to encompass infrastructure, applications (e-mail, ftp, Web), and content. The www is just one of many Internet applications, a system of interlinked documents connected with the help of the HyperText Transfer Protocol (HTTP).

[2] Following a policy of technological neutrality, the EU has been using the term 'electronic communications' instead of 'telecommunications'. This covers, for example, Internet traffic over the electrical grid, which is not part of the telecommunications infrastructure.

[3] Power Line Communications (PLC) allow the transmission of Internet data via the electrical grid. Given its deep capillarity, the use of the power grid would make the Internet more accessible to many users. For a technical and organisational review of this facility, please consult: Palet J (2003) *Addressing the Digital Divide with IPv6-enabled Broadband Power Line Communication,* Internet Society, ISOC Member Briefing No. 13. Available at http://www.isoc.org/briefings/013 [accessed 7 October 2016].

[4] Project Loon was launched by Google with the aim of increasing the broadband coverage and reach out to the most remote areas of the world which do not have any telecom infrastructure. The company is launching numerous balloons to the stratosphere, at about 20 km above ground, each of which act as a floating base station providing a signal to the end-users. The balloons are connected to each other and to the earth base stations through high-speed links, provided by partner telecom operators.

[5] According to the ITU, Television White Spaces are 'portions of spectrum left unused by [TV] broadcasting, also referred to as interleaved spectrum'. Since the unused frequencies belong to a part of the spectrum which enables 'advantageous propagation properties inherent to UHF [TV] spectrum (excellent outdoor and indoor coverage and non line-of-sight propagation properties)', as Cristian Gomez of the ITU Radiocommunication Bureau explains, the TVWS are seen as an alternative wide-range low-power technology that can serve both for broadband applications in rural areas and for machine-to-machine (M2M) communications important for the IoT applications. For more information, please consult: ITU (2012) Digital Dividend: Insights for Spectrum Decisions. Available at http://www.itu.int/ITU-D/tech/digital_broadcasting/Reports/DigitalDividend.pdf [accessed 7 October 2016], and Gomez C (2013) TV White Spaces: Managing spaces or better managing inefficiencies? Available at http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR_paper_WhiteSpaces_Gomez.pdf [accessed 18 July 2016].

[6] The liberalisation of telecommunications markets of WTO members was formalised in 1998 in the so-called Basic Telecommunication Agreement (BTA). Following the adoption of the BTA, more than 100 countries began the liberalisation process, characterised by the privatisation of national telecommunications monopolies, the introduction of competition, and the establishment of national regulatory authorities. The agreement is formally called *The Fourth Protocol to the General Agreement on Trade in Services* (adopted 30 April 1996 and entered into force 5 February 1998). Available at http://www.wto.org/english/tratop_e/serv_e/4prote_e.htm [accessed 7 October 2016].

[7] ITU (no date) Signatories of the Final Acts – WCIT-12. Available at http://www.itu.int/osg/wcit-12/highlights/signatories.html [accessed 7 October 2016].

[8] For more information about ITU's Internet-related activities, consult hhttp://www.itu.int/en/action/internet/Pages/default.aspx [accessed 7 October 2016].

[9] The Digital Object Architecture – a project initiated by Robert Kahn (one of the inventors of TCP/IP) – aims to associate unique identifiers to each digital object (data and devices). Such identifiers are intended to remain unchanged, irrespective of where the object is located in the networks, who owns it, what technology it is based on, etc. While responsibility for managing

aspects related to the DOA rests with the Swiss-based DONA Foundation, the ITU, through its Telecommunication Sector study groups, has been exploring the possibility of adopting the DOA as a standard for cloud computing and IoT devices. While some ITU member states argue for the adoption of DOA standards, invoking reasons such as combatting device counterfeiting, there are views that, by allowing devices to be tracked, the DOA could be misused to also track and control the flow of information, as well as user actions. For more details, consult: Corporation for National Research Initiatives (2010) A Brief Overview of the Digital Object Architecture and its Application to Identification, Discovery, Resolution and Access to Information in Digital Form. Available at http://www.cnri.reston.va.us/papers/Digital_Object_Architecture_Brief_Overview.pdf [accessed 20 October 2016]; Javed D (2016) ITU IoT Standards: Gateway to Government Control? Available at http://www.wileyconnect.com/home/2016/9/20/itu-iot-standards-gateway-to-government-control [accessed 20 October 2016].

[10] For more information about the WTO's role in the field of telecommunications, consult http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm [accessed 7 October 2016].

[11] This section is based on Kurbalija J (2016) From harmonising cyberpolicies to promoting twiplomacy: How diplomacy can strengthen Asia-Europe's digital connectivity. In Asia-Europe Foundation. *ASEF Outlook Report 2016/2017. Connectivity: Facts and Perspectives, Volume II: Connecting Asia and Europe*. Available at http://www.asef.org/images/docs/ASEF%20Outlook%20Report%202016-2017%20Vol2.pdf [accessed 20 October 2016].

[12] UNESCAP (2014) Problems and Challenges in Transit Connectivity Routes and International Gateways in Asia. *Discussion paper series,* 2014/1. Available at http://www.unescap.org/sites/default/files/Discussion%20Paper-Transit-Connectivity_0.pdf [accessed 20 October 2016].

[13] Verda M (2014) Trans-Eurasian Information Super Highway. Available at http://sam.az/uploads/PDF/TRANS-EURASIAN%20INFORMATION%20SUPER%20HIGHWAY.pdf [accessed 20 October 2016].

[14] The term Digital Silk Road is used informally as an umbrella concept that encompasses various cooperation projects between Asia and Europe in the digital field. For further reference, consult: Jia L and Shuang G (2015) Digital Silk Road to span Eurasia, *China Daily Europe*, 10 July. Available at http://europe.chinadaily.com.cn/epaper/2015-07/10/content_21241323.htm [accessed 20 October 2016]; and Zhao Huanxin Z (2015) Web companies asked to support 'digital Silk Road,' *China Daily Europe*, 8 September. Available at http://www.chinadaily.com.cn/business/2015chinaarabforum/2015-09/08/content_21823475.htm [accessed 20 October 2016]. The Digital Silk Road is part of the One Belt, One Road (*yidai-yilu*) initiative, which consists of the land-based Silk Road Economic Belt that should cross the continent and the Maritime Silk Road connecting China to the maritime regions of Southeast Asia, South Asia, the Middle East, East Africa, and the Mediterranean. The overall project is planned to cross 60 countries with a total population of 4.4 billion people, which accounts for 63% of the world's population. For further details, consult: Arase D (2015) China's Two Silk Roads Initiative: What It Means for Southeast Asia. *Southeast Asian Affairs* 41, pp. 25–45; and Tsao R (2015) One belt one road: A historical perspective. *Chinese American Forum 31*(1) pp. 11–14.

[15] For more information about the EU radio spectrum policy, consult http://ec.europa.eu/digital-agenda/en/what-radio-spectrum-policy [accessed 7 October 2016].

[16] In computer networking, peering is a voluntary interconnection of administratively separate Internet networks for the purpose of exchanging traffic between the customers of each network. The pure definition of peering is settlement-free or 'sender keeps all', meaning that neither party pays the other for the exchanged traffic; instead, each derives revenue from its own customers. Peering requires physical interconnection of the networks and an exchange of routing information through the Border Gateway Protocol (BGP) routing protocol. It is often accompanied by peering agreements of varying formality, from handshakes to thick contracts. (Source: Wikipedia).

[17] Tier 2 Internet Bandwidth Providers are usually called ICP (Internet connection points) or Internet gateways.

[18] Two related cases are mentioned in Spaink K (2002) *Freedom of the Internet, our new challenge.* Available at http://www.spaink.net/english/osce_internetfreedom.html [accessed 7 October 2016]. In the first case, legal action was launched against a web page with questionable Nazi content hosted by Flashback in Sweden. The courts decided that the page did not violate Swed-

ish anti-Nazi laws. Nevertheless, one committed anti-Nazi activist mounted a strong campaign against Flashback, thereby putting pressure on Flashback's ISP, Air2Net, and the main backbone operator MCI/WorldCom. Under pressure from this campaign, MCI/WorldCom decided to disconnect Flashback in spite of a lack of any legal basis for doing so. Flashback's attempts to find an alternative provider were unsuccessful, since most of them were also connected through the backbone operated by MCI/WorldCom. The second case took place in the Netherlands. A small Dutch ISP provider, Xtended Internet, was disconnected by its US-based upstream provider under pressure from the Scientology lobby.

[19] Metz C (2016) Facebook and Microsoft are laying a giant cable across the Atlantic. *Wired*, 26 May. Available at http://www.wired.com/2016/05/facebook-microsoft-laying-giant-cable-across-atlantic/ [accessed 7 October 2016].

[20] IANA describes itself as one of the Internet's oldest Institutions. Its functions date back to the 1970s, when they were performed by just one person – Jon Postel, a computer scientist working at that time with the University of Southern California. Starting in 1998, the IANA functions have been performed by ICANN, on the basis of a contract with the US government. Following the expiration of this contract, on 1 October 2016, the functions have continued to be performed by ICANN, through a newly established subsidiary - PTI. The IANA functions can be grouped into three categories: domain names (management of the DNS root, the .int and .arpa domains, and an IDN practices resource), number resources (coordination of the global pool of IP and Autonomous numbers, primarily providing them to RIRs), and protocol assignments (the management of the Internet protocol's numbering systems is done in conjunction with standards bodies). For more information, visit https://www.iana.org/about [accessed 7 October 2016].

[21] The current RIRs: ARIN (the American Registry for Internet Numbers), APNIC (the Asia Pacific Network Information Centre), LACNIC (the Latin American and Caribbean Network Information Centre), RIPE NCC (Reseaux IP Européens Network Coordination Centre – covering Europe and the Middle East) and AFRINIC (the African Network Information Centre). A detailed explanation of the RIR system is available at http://www.ripe.net/internet-coordination/internet-governance/internet-technical-community/the-rir-system [accessed 7 October 2016].

[22] Drake W *et al.,* Internet Fragmentation: An Overview. Available at http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf [accessed 7 October 2016].

[23] For example, in 2000, the IETF elaborated RFC 2893, Transition Mechanisms for IPv6 Hosts and Routers, which describes transition mechanisms that will 'allow IPv6 nodes to maintain complete compatibility with IPv4, which should greatly simplify the deployment of IPv6 in the Internet, and facilitate the eventual transition of the entire Internet to IPv6'. Available at https://www.ietf.org/rfc/rfc2893.txt [accessed 7 October 2016].

[24] After a successful World IPv6 Day event held on 8 June 2011, major ISPs, home networking equipment manufacturers, and web companies around the world came together to permanently enable IPv6 for their products and services by 6 June 2012 – the World IPv6 launch. In 2016, four years after the World IPv6 launch, it was reported that the global IPv6 traffic had grown more than 500%. For more details, refer to http://www.worldipv6launch.org [accessed 7 October 2016].

[25] For a comprehensive and highly technical survey of TCP/IP Security, consult: Chambers C *et al.* (no date) TCP/IP Security, Department of Computer and Information Science. Ohio State University. Available at http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html [accessed 7 October 2016].

[26] Bavisi J (2011) What Security Issues does IPv6 Pose? *eSecurity Planet*. Available at http://www.esecurityplanet.com/trends/article.php/3935356/What-Security-Issues-Does-IPv6-Pose.htm [accessed 25 July 2016].

[27] Ashford W (2011) IPv6: The security risks to business. *Computer Weekly,* 29 August. Available at http://www.computerweekly.com/feature/IPv6-The-security-risks-to-business [accessed 26 July 2016].

[28] More details about the group are available at http://www.etsi.org/technologies-clusters/technologies/next-generation-protocols [accessed 7 October 2016].

[29] One of the few referential documents on the DNS is RFC 1591 (March 1994), which specifies the governance structure of DNS. Available at http://www.ietf.org/rfc/rfc1591.txt [accessed 7 October 2016].

[30] ICANN (2016) Bylaws for Internet Corporation for Assigned Names and Numbers. Available at https://www.icann.org/resources/pages/governance/bylaws-en [accessed 7 October 2016].

[31] A list with current Registry Agreements is available at https://www.icann.org/resources/pages/registries/registries-agreements-en [accessed 7 October 2016].

[32] Registrars that want to provide domain name registration services under gTLDs, with a direct access to the gTLD registries, need to be accredited by ICANN. A list with such registrars is available at https://www.icann.org/registrar-reports/accredited-list.html [accessed 7 October 2016].

[33] Statistics about the new gTLDs, including a list with the delegated strings, is available at https://newgtlds.icann.org/en/program-status/statistics [accessed 7 October 2016].

[34] The IANA Report on the county code top-level domain for Palestine is available at http://www.iana.org/reports/ps-report-22mar00.htm [accessed 7 October 2016].

[35] Details about the registries for ccTLDs can be found in the IANA Root Zone Database, available at http://www.iana.org/domains/root/db [accessed 7 October 2016].

[36] The Brazilian model of the management of country domains is usually quoted as a successful example of a multistakeholder approach. The national body in charge of Brazilian domains is open to all key players, including government authorities, the business sector, and civil society. For more information, please consult: Alfonso C (2004) BR: CCTLD An asset of the commons, in MacLean D (ed) *Internet Governance: A Grand Collaboration*. New York: UN ICT Task Force, pp. 291–299; Excerpts are available at http://books.google.ro/books?id=pEFAypES4t0C&printsec=frontcover&hl=ro#v=onepage&q&f=false [accessed 14 October 2016].

[37] For example, South Africa used its sovereign rights as an argument in winning back control of its country domain. A law was adopted which specifies that the use of the country domain outside the parameters prescribed by the South African government would be considered a crime. Cambodia's transfer of country domain management from non-governmental to governmental control is often cited as an example of an unsuccessful transition. The government reduced the quality of services and introduced higher fees, which have made the registration of Cambodian domains much more difficult. For more information, consult Klien N (2004) Internet Governance: Perspectives from Cambodia in MacLean D (ed) *Internet Governance: A Grand Collaboration*. New York: UN ICT Task Force, pp. 227–237. Excerpts are available at http://books.google.ro/books?id=pEFAypES4t0C&printsec=frontcover&hl=ro#v=onepage&q&f=false [accessed 7 October 2016].

[38] For more details on the delegation and redelegation of a ccTLD, refer to the IANA guide on Delegating or redelegating a country-code top-level domain (ccTLD). Available at http://www.iana.org/help/cctld-delegation [accessed 7 October 2016].

[39] ICANN GAC (2005) Principles for the Delegation and Administration of Country Code Top-Level Domains. Available at https://gacweb.icann.org/display/GACADV/ccTLDs?preview=/28278844/28475457/ccTLD_Principles_0.pdf [accessed 14 October 2016].

[40] The root zone file is publicly available at http://www.iana.org/domains/root/files [accessed 7 October 2016].

[41] The list of root zone servers, their nodes and positions, and managing organisations is available at http://www.root-servers.org/ [accessed 7 October 2016].

[42] The list of the 13 named authorities in the DNS root zone is available at http://www.iana.org/domains/root/servers [accessed 9 October 2016].

[43] ISC Inc. (2003) Hierarchical Anycast for Global Distribution. Available at http://ftp.isc.org/isc/pubs/tn/isc-tn-2003-1.html [accessed 14 October 2016].

[44] For more details, refer to Das D (2015) List of top 4 alternative DNS servers to your ISP. Available at http://www.snaphow.com/4402/list-of-top-4-alternative-dns-servers-to-your-isp/ [accessed 7 October 2016].

[45] For more details on the Yeti DNS Project, refer to https://yeti-dns.org [accessed 7 October 2016].

[46] For a comprehensive analysis of challenges related to alternative root systems, refer to Bertola V (no date) Oversight and multiple root server systems. Available at http://wgig.org/docs/book/Vittorio_Bertola.html [accessed 7 October 2016].

[47] Signal transmission technologies – both for wireless, like Long Term Evolution (LTE), and optical cables, like Dense Wavelength Division Multiplexing (DWDM) – promise to solve the 'bandwidth exhaustion' problem with much greater bandwidth specifications (up to terabits per second). The demand-supply run, however, is perpetual.

[48] *The Economist* (2009) America insists on net neutrality: The rights of bits. 24 September. Available at http://www.economist.com/node/14517422 [accessed 7 October 2016].

[49] The full text of a Verizon and Google Legislative Framework Proposal for an Open Internet is available at http://www.google.com/googleblogs/pdfs/verizon_google_legislative_framework_proposal_081010.pdf [accessed 7 October 2016].

[50] The bandwidth (bit rate) agreed to in a contract with the ISP is, in fact, only the maximum available rather than a guaranteed effective speed.

[51] McCullagh D (2012) European ISPs defend UN Internet tax. *C|net*, 20 August. Available at http://news.cnet.com/8301-13578_3-57496581-38/european-isps-defend-u.n-internet-tax/ [accessed 7 October 2016].

[52] Those elements that are still controversial and to be negotiated about in future are in square brackets.

[53] Radunović V (2012) Network neutrality in law – a step forwards or a step backwards? Diplo Blog. Available at http://www.diplomacy.edu/blog/network-neutrality-law-%E2%80%93-step-forwards-or-step-backwards [accessed 14 October 2016].

[54] Federal Communications Commission (2015) Open Internet Order. Available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf [accessed 8 August 2016].

[55] The case was handled by the US Court of Appeals for the District of Columbia Circuit, and the Court decision is available at https://www.cadc.uscourts.gov/internet/opinions.nsf/3F95E49183E6F8AF85257FD200505A3A/$file/15-1063-1619173.pdf [accessed 14 October 2016].

[56] European Union (2015) Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) 531/2012 on roaming on public mobile communications networks within the Union. Available at http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32015R2120 [accessed 8 August 2016].

[57] When, in June 2016, BEREC published a draft set of guidelines on how the new net neutrality rules were to be implemented by national regulatory authorities, large European telecom providers reacted by arguing that the proposed guidelines would 'create significant uncertainties around 5G return on investment'. They explained that 5G brings in the concept of 'network slicing', aimed at allowing a wide-variety of industry business models on a common platform, at scale, and with service guarantees. In their view, the proposal is 'excessively prescriptive and could make telcos risk-averse thus hampering the exploitation of 5G, ignoring the fundamental agility and elastic nature of 5G network slicing to adapt in real time to changes in end-user/application and traffic demand'. Other entities, such as the European Broadcasting Union, disagree with this view, considering that robust net neutrality rules will be key for the development of an 'open and interoperable 5G technology platform'. For more details, refer to Patterson G *et al.* (2016) Manifesto for timely deployment of 5G in Europe. Available at http://telecoms.com/wp-content/blogs.dir/1/files/2016/07/5GManifestofortimelydeploymentof5GinEurope.pdf [accessed 9 August 2016]; and European Broadcasting Union (2016) EBU response to the public consultation of draft BEREC guidelines on implementation of net neutrality rules. Available at http://www.ebu.ch/files/live/sites/ebu/files/Publications/Position%20Papers/EBU_response_BEREC_consultation_NN_guidelines_final_version_18072016.pdf [accessed 9 August 2016].

[58] Body of European Regulators for Electronic Communications (2016) Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. Available at http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules [accessed 7 October 2016].

[59] The English version of the Brazilian *Marco Civil* is available at http://www.giplatform.org/resources/text-brazilsnew-marco-civil [accessed 8 October 2016].

[60] TechnoLlama (2012) Chile enforces net neutrality for the first time, sort of. Available at http://www.technollama.co.uk/chile-enforces-net-neutrality-for-the-first-time-sort-of [accessed 8 October 2016].

[61] European Digital Rights (2013) Slovenia has a net neutrality law. Available at https://edri.org/edrigramnumber11-2slovenia-net-neutrality/ [accessed 8 August 2016].

[62] Electronic Frontier Foundation (2012) The Netherlands passes net neutrality legislation. Available at https://www.eff.org/deeplinks/2012/05/netherlands-passes-net-neutrality-legislation [accessed 8 August 2016].

[63] Norwegian Communications Authority (2009) Guidelines for Internet neutrality. Available at http://eng.nkom.no/technical/internet/net-neutrality/net-neutrality/_attachment/9222?_ts=1409aa375c1 [accessed 7 October 2016].

[64] The integral text of the 2010 Declaration of the Committee of Ministers on network neutrality is available at https://wcd.coe.int/ViewDoc.jsp?id=1678287 [accessed 9 August 2016]. The text of the 2016 Recommendation of the Committee of Ministers on protecting and promoting the right to freedom of expression and the right to private life with regard to net neutrality is available at https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec(2016)1&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383&direct=true [accessed 9 August 2016].

[65] Internet Society (no date) Net Neutrality. Available at http://www.internetsociety.org/net-neutrality [accessed 3 November 2016].

[66] TACD (2015) Resolution on the open and neutral Internet. Available at http://tacd.org/wp-content/uploads/2015/06/TACD-INFOSOC-Resolution-on-Net-Neutrality-2015-GREEN.pdf [accessed 3 November 2016].

[67] Global Multistakeholder Meeting on the Future of Internet Governance (2014) NETmundial Multistakeholder Statement. Available at http://netmundial.br/netmundial-multistakeholder-statement/ [accessed 14 October 2016].

[68] Radunović V (2012) Can free choice hurt open Internet markets? Diplo Blog. Available at http://www.diplomacy.edu/blog/can-free-choice-hurt-open-internet-markets [accessed 7 October 2016].

[69] International Telecommunication Union (2016) ITU towards 'IMT for 2020 and beyond'. Available at http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx [accessed 7 October 2016].

[70] Updated lists of current Internet standards, draft standards, and proposed standards are available in the Official Internet Protocol Standards directory, available at https://www.rfc-editor.org/standards [accessed 7 October 2016].

[71] World Wide Web Consortium (no date) Standards. Available at http://www.w3.org/standards/ [accessed 14 October 2016].

[72] Latency refers to the amount of time it takes for a packet of data to get from one designated point to another within a network.

[73] Cisco (2015) Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are. Available at https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf [accessed 7 October 2016].

[74] Oracle (2016) Oracle Unveils Suite of Breakthrough Services to Help Simplify Cloud Adoption by Global Corporation. Available at https://www.oracle.com/corporate/pressrelease/oracle-cloud-at-customer-032416.html [accessed 7 October 2016].

[75] The Open Group (2013) Cloud Computing Portability and Interoperability. Available at http://www.opengroup.org/cloud/cloud_iop/ [accessed 7 October 2016].

[76] IDC (2014). The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things. Available at http://www.emc.com/leadership/digital-universe/2014iview/digital-universe-of-opportunities-vernon-turner.htm [accessed 7 October 2016].

[77] Verizon (2016) State of the Market: Internet of Things 2016. Available at http://www.verizon.com/about/our-company/state-of-the-market-internet-of-things [accessed 7 October 2016].

[78] IITU and Cisco Systems (2016) Harnessing the Internet of Things for Global Development. Available at http://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf [accessed 7 October 2016].

[79] Schmid S *et al.* (2016) EnLighting: An Indoor Visible Light Communication System Based on Networked Lights Bulbs. Available at https://s3-us-west-1.amazonaws.com/disneyresearch/wp-content/uploads/20160615205959/EnLighting-An-Indoor-Visible-Light-Communication-System-based-on-Networked-Light-Bulbs-Paper.pdf [accessed 7 October 2016].

[80] In the Netherlands, a nationwide dedicated network for IoT solutions (LoRa) was deployed in July 2016 by KPN, a Dutch telecom company. In South Korea, Samsung and SK Telecom have been working on the roll-out of a commercial IoT-dedicated network across the country.

[81] In September–October 2016, two large DDoS attacks, which made used of many IoT devices, rendered major websites inaccessible. More than a million devices were used in attacks on a US security researcher and a French network service provider. The second attack was directed at systems operated by DNS services provider Dyn, which suffered three attacks in one day; the attacks affected Twitter, PayPal, Netflix, Airbnb, Amazon, CNN, and several online journals. For details, refer to Rash W (2016) Weak Devices security turns IoT into powerful weapon in DDos attacks. *Eweek,* 1 October. Available at http://www.eweek.com/security/weak-device-security-turns-iot-into-powerful-weapon-in-ddos-attacks.html [accessed 12 November 2016]. Wikipedia (2016) 2016 Dyn cyberattack. Available at https://en.wikipedia.org/wiki/2016_Dyn_cyberattack [accessed 12 November 2016].

[82] Greenberg A (2016) Inside Google's Internet Justice League and its AI-powered war on trolls. *Wired*, 19 September. Available at https://www.wired.com/2016/09/inside-googles-internet-justice-league-ai-powered-war-trolls/ [accessed 20 October 2016].

[83] Romm T (2016) Tech companies launch new AI coalition. *Politico,* 11 October. Available at http://www.politico.com/story/2016/10/tech-companies-launch-new-ai-coalition-229600 [accessed 20 October 2016].

[84] European Parliament Committee on Legal Affairs (2016) Draft report with recommendations to the Commission on Civil Law Rules on Robotics. Available at http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2015/2103(INL)&l=en [accessed 7 October 2016].

[85] US National Science and Technology Council (2016) The National Artificial Intelligence Research and Development Strategic Plan. Available at https://www.whitehouse.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf [accessed 20 October 2016].

[86] UK Parliamentary Committee on Science and technology (2016) Robotics and artificial intelligence. Available at http://www.publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/14502.htm [accessed 20 October 2016].

[87] IBM Institute for Business Value (2016) Redefining Boundaries. Insights from the Global C-suite Study. Available at https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03695usen/GBE03695USEN.PDF [accessed 7 October 2016].

[88] For more details on partnerships between telecom providers and OTT providers, refer to Body of European Regulator for Electronic Communications (2016) Report on OTT services. Available at http://www.stibbe.com/~/media/03%20news/newsletters/brussels/bru%20tmt%20berec%20report%20on%20ott%20services.pdf [accessed 7 October 2016].

[89] For more details on the various legal and regulatory approaches towards convergence, read: ITU, infoDev (no date) Impact of Convergence. Available at http://www.ictregulationtoolkit.org/6.4 [accessed 7 October 2016].

Section 3

THE SECURITY BASKET

The security basket

Cybersecurity

The Internet was originally designed for use by a closed circle, mainly of academics. Communication was open. Security was not a concern.

Cybersecurity came into sharper focus with the Internet's expansion beyond the circle of Internet pioneers. The Internet reiterated the old truism that technology can be both enabling and threatening. What can be used to the advantage of society can also be used to its disadvantage.

The modern Internet, with more than 3 billion users, is the critical infrastructure (CI) of today's society. The vulnerability of the Internet is the vulnerability of modern society. The financial sector, governmental services, the security sector, schools, and hospitals are increasingly and irreversibly dependent on interconnectivity and the global network; so are citizens.

In addition, political tensions among countries are reflected in cyberspace, sometimes triggering cyber-incidents. Cyber-incidents – especially those related to the CI – may have dire consequences for the functionality of state, economy, and wellbeing; for instance, a country-scale cyber-attack on Switzerland could result in a direct loss of more than €500 million per day.[1]

Cybersecurity mapping

Cybersecurity issues can be classified according to three criteria:

- Type of action. Classification based on type of action may include data interception, data interference, illegal access, spyware, data corruption, sabotage, denial-of-service (DoS), and identity theft.

- Type of perpetrator. Possible perpetrators might include criminals, anarchists, hacktivists, revolutionaries, terrorists, secret services, and defence and military units.

- Type of target. Potential targets are numerous, ranging from individuals, private companies, civil society organisations, media entities, and public institutions, to core Internet infrastructure (telecom operators, ISPs, IXPs, data centres), critical society infrastructures (power and water supplies, industry facilities, traffic, etc.), and military assets.

The cybersecurity framework includes policy principles, instruments, and institutions dealing with cybersecurity. Cybersecurity is an umbrella concept covering several areas:

- Critical information infrastructure protection (CIIP) is increasingly important because the CIs, including energy, water, communications, and finance, now depend on

the Internet and other computer networks as the underlying information infrastructure. The critical information infrastructure (CII) includes not only the equipment and links (whose security is broadly referred to as network security), but also the protocols, data centres, and the critical Internet resources.

- Cybercrime is crime committed via the Internet and computer systems. It includes old, i.e., traditional, crimes now conducted through cyberspace (like various frauds), crimes that have evolved due to technology (e.g. credit card fraud, and online child sexual abuse and exploitation), new crimes that have emerged with the Internet (e.g. DoS attacks and pay-per-click frauds), and the commercialisation of cybercrime tools – mostly distributed through online dark markets – which are used to facilitate other crimes (e.g. viruses and botnets). Combating online child sexual abuse and exploitation is the most developed area of international cooperation against cybercrime. Increasing the safety of all users, and particularly children – referred to as Internet safety – mostly through education and awareness raising, is an important field for prevention of crime, scams, or bullying.

- Cyberconflicts, often popularly labelled as cyberwar, have high media visibility but a low level of policy and legal attention. Cooperation related to cyberconflicts falls into three main areas: conduct of cyberconflicts (i.e., can existing law, mainly The Hague Conventions, be applied to cyberspace; if not, what type of new legal instruments should be developed?); weapons and disarmament (i.e., how to introduce cyberweapons into the disarmament process); and humanitarian law (i.e., how to apply the Geneva Conventions to cyberconflicts). Economic cyber-espionage, hacks enabling leaking of political documents, and sabotage conduct that falls under the threshold of acts of war are coming to the top of the political and diplomatic agendas. Increasing use of the Internet by terrorists for information, communications, propaganda, and conducting attacks – sometimes labelled as cyberterrorism – is often politically framed as an issue of national and global security, even though its prosecution falls under the national criminal legislation.

Cybersecurity threats

Security threats can be caused by a variety of perpetrators and with several different motives. When attacking individuals, perpetrators seek to gain access to information and personal data, usually to obtain money or assets. Malware such as viruses or spyware, phishing, and e-scams are the most common threats to Internet users. In addition, more sophisticated attacks are conducted to penetrate complex corporate and government systems for espionage purposes. Similarly, a variety of cyber-weapons and attacks can be combined to disrupt an entire third party system or network.

The techniques used to facilitate the types of attacks that affect the confidentiality, integrity, and availability of data and systems are very diverse and more and more sophisticated.

Malicious software (malware) includes viruses, spyware, and other unwanted software that is installed on digital devices without permission and performs unwanted tasks, often for the benefit of the attacker. These programs can damage devices, and can be used to steal personal information, monitor and control online activity, send spam, and commit fraud, as well as infect other devices on the network. They also can deliver unwanted or inappropriate online advertisements.

Viruses, Trojan horses, adware, and spyware are all types of malware. A virus can replicate itself and spread to other devices, without the user being aware. Although some viruses are latent, most of them are intended to interfere with data or affect the performance of devices (reformatting the hard disk, using up computer memory, etc.). A Trojan horse is a program containing malicious or harmful content used to allow a backdoor that perpetrators can use to infiltrate a device and run additional remote operations. Trojans can be employed by cyber-thieves and hackers trying to gain access to a user's system. The user is typically tricked by some form of social engineering into loading and executing Trojans on their system. Once activated, Trojans can enable cyber-criminals to spy on users, steal sensitive data, and gain backdoor access into their systems.

Adware collects marketing data and other information without the user's knowledge, or redirects search requests to certain advertising websites. Spyware monitors users, gathers information about them, and transmits it to interested parties, without the user being aware. Types of information gathered can include the websites visited, browser and system information, the computer IP address, as well as more sensitive information such as e-mail addresses and passwords. Additionally, malware can cause browser hijacking, in which the user's browser settings are modified without permission. The software may create desktop shortcuts, display advertising pop-ups, as well as replace existing home pages or search pages with other pages.

Botnets are networks of hijacked devices that perform remotely commanded tasks without the knowledge of their owners. A device is turned into a bot after being infected with a specific type of malware which allows remote control. Botnets are used for a wide variety of crimes and attacks: distributing spam, extending malware infections to more devices, contributing to pay-per-click frauds, or identity theft. One of the most worrying uses of botnets is to perform distributed denial-of-service (DDoS) attacks (Figure 11).

Figure 11. Botnet

Researchers and cybersecurity companies have warned that botnets are becoming the biggest Internet security threat, as they are increasing the effects of viruses and other malicious programs, raising information theft, and boosting DoS attacks. As an illustration of the dimension of this threat, the Simda botnet, taken down in April 2015, affected computers in 190 countries and involved the use of 14 command-and-control servers in 5 countries.[2]

DoS attacks involve flooding a computer or website with requests for information, preventing them functioning properly. These attacks aim to exhaust the resources available to a network, application, or service to prevent users from accessing them. They are more frequently targeted at businesses, rather than individuals. DDoS attacks are those attacks in which multiple compromised computers attack a single target.

A DoS attack does not usually result in the theft of information or other security loss, but it can cause financial or time loss to the affected organisation or individual, because of its effects (particular network services becoming unavailable, websites ceasing operation, targeted e-mail accounts prevented from receiving legitimate e-mails, etc.).

Phishing is a form of social engineering through which a person is tricked into doing something that they normally should not do, such as providing confidential information (e.g. username and password), opening an unknown file, or following an unreliable link. One form of phishing consists of falsely claiming, through e-mail, social media, or other online services, to be an existing and trusted entity (such as a bank), so that the recipient provides personal or sensitive information.

E-scams refer to fraud schemes in which scammers use one or more online services – such as e-mails or websites – to contact potential victims with fraudulent offers (often in the form of business or investment opportunities, easy ways of making money, health scams, or significant discounts for online purchases). E-scams have been commonly associated with e-mail fraud, and, increasingly, with social media.

Cybersecurity policy and regulation

Many national, regional, and global initiatives focus on cybersecurity. At national level, a growing volume of legislation and jurisprudence deals with cybersecurity, with a focus on combating cybercrime, and increasingly, on the protection of the CII from sabotage and attacks as a result of terrorism or conflicts. It is difficult to find a developed country without some initiative focusing on cybersecurity. At regional and global level, there are many initiatives and activities.

Global cybersecurity activities

United Nations

The UN has held discussions on the issue of cybersecurity for some time. In 1998, the Russian Federation introduced a draft resolution in the First Committee of the UNGA on developments in the field of information and telecommunications in the context of information security.[3] Later, in 2004, the UN GGE was established with the aim of examining existing and potential threats from the cyber-sphere and possible cooperative measures to address them. The mandate of the group was re-confirmed in 2009, 2011, 2013, and 2015. The main outcome of the UN GGE 2013 report was re-confirmation of the principle that

existing international law applies to the use of ICT by states. In addition, the 2015 report specifies that a state should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of the CI.[4]

The UN Conference on Disarmament offers another possible venue for discussing cybersecurity at the high diplomatic level. So far, although some members, such as China, have proposed that cybersecurity be added to the agenda, the group has not been able to agree on a work plan.[5]

In the field of cybercrime, the UN Office on Drugs and Crime (UNODC) is the leading organisation. Some of the UNODC's legal instruments, such as the UN Convention against Transnational Organized Crime (UNTOC), are underused in fighting cybercrime. Most cybercrime is organised (committed by at least three people) and transboundary (organised in more than one state and, even, organised by groups in one state with substantial effects in another state).

International Telecommunication Union

The ITU was mandated by the outcomes of WSIS in 2005 to follow up on Action Line C5 of the Tunis Agenda, titled *Building Confidence and Security in the Use of ICTs*.

The ITU conducts several activities related to cybersecurity. However, only some of this work related to the security of the telecommunications infrastructure is of a decision-making (or rather, standard-setting) nature; much of it involves research, awareness, and capacity development.

One of the most visible activities is the ITU Global Cybersecurity Agenda (GCA),[6] launched in 2007 by the ITU Secretary-General as a framework for international cooperation aimed at enhancing confidence and security in the information society. The GCA is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners, and building on existing initiatives to avoid duplicating efforts. Through its partnership with the International Multilateral Partnership against Cyber Threats (IMPACT), the ITU also assists countries around the world in deploying cybersecurity solutions and policies. The GCA is built on five strategic pillars: legal measures, technical and procedural measures, organisational structures, capacity building, and international cooperation.

Another ITU activity is the Global Cybersecurity Index (GCI), a multistakeholder initiative aimed at measuring the commitment of countries to cybersecurity.[7]

Internet Governance Forum

Cybersecurity has been very prominent on the agenda of the IGF since its first meeting in 2006. For example, it was the topic of one of the main sessions and several workshop sessions at the IGF meeting in João Pessoa in Brazil in November 2015, with particular focus on security, encryption, and trust.[8] One-fifth of the workshops at IGF 2015 dealt with cybersecurity-related issues. In 2016, cybersecurity was chosen as a topic for an IGF Best Practice Forum, which focused on addressing cooperation and collaboration between stakeholder groups in the area of cybersecurity. While the IGF does not make decisions or recommendations, it provides an opportunity for open dialogue and partnership, exchange of information, and useful voluntary policy guidance through Best Practice Forums and reports from the thematic sessions held each year.

Global Conference on Cyberspace

The Global Conference on CyberSpace (GCCS) has emerged as a series of conferences which discuss principles related to 'governing behaviour in cyberspace'.[9] The conferences are sometime referred to as the London Process since the first conference was held in London in 2011. The second conference was in Budapest in 2012, the third in Seoul in 2013, and the fourth in The Hague in 2015.

The GCCS gathers representatives of governments, including many ministers, as well as high-level representatives of the corporate sector and civil society. It does not produce any conclusions or formal treaties, aside from the Statement of the Chair, yet it provides an important opportunity for discussion and cooperation, as well as a platform for negotiations on possible future agreements within other frameworks.

At the GCSC 2015, the Global Forum on Cyber Expertise (GFCE) was established with the aim of sharing experiences, identifying gaps, and complementing existing efforts in cyber capacity building. The Forum members are governments, international organisations, and private companies; they work together with the technical community, civil society organisations, and academia on developing initiatives in the area of cyber capacity building. All members adopted The Hague Declaration that emphasises the need for more capacity building, exchange of best practices, and strengthened international cooperation.[10]

NATO

NATO, being a collective defence organisation, focuses its cybersecurity-related efforts on cyber defence. NATO has followed the rapid changes in the threat landscape instigated by the increased dependence on technology and the Internet and has therefore firmly embedded cyber defence in its strategic and institutional framework. Changes even happened in the doctrinaire framework of the organisation, as the 28 member states agreed in 2016 to declare cyberspace as its fourth operational domain, in addition to air, land, and sea.[11]

The current NATO Policy on Cyber Defence, adopted in 2014, contains, among others, procedures for assisting member states in defining ways to take awareness, education, training, and exercise activities forward and emphasising the need for progress in further cooperation initiatives – with partner countries, other international organisations as well as with the industry. Although NATO's top priority in cyber defence is the protection of communication and information systems owned and operated by the organisation, it also relies on a reliable and secure national infrastructure of its member states.

The NATO-initiated Cooperative Cyber Defence Centre of Excellence (CCD COE), launched the Tallinn Manual Process in 2009 'as a leading effort in international cyber law research and education' which consisted of research and practitioner-oriented training programmes, with the Tallinn Manual on the International Law Applicable to Cyber Warfare as the key international document providing proposals related to the application of international law to cyberspace.[12] CCD COE has also developed a comprehensive National Cyber Security Framework Manual, which provides detailed background information and in-depth theoretical frameworks to help understand the various facets of national cybersecurity, according to different levels of public policy formulation. The four levels of government — political, strategic, operational and tactical/technical — each have their own perspectives on national cybersecurity, and each is addressed in individual sections within the Manual. Additionally, the Manual gives examples of relevant institutions in national cybersecurity, from top-level policy coordination bodies down to cyber crisis management structures and similar institutions.[13]

Regional cybersecurity activities

At regional level, more and more organisations are realising the importance of cybersecurity and are working on strategies, recommendations, and conventions, such as the CoE Convention on Cybercrime, the Asia-Pacific Economic Cooperation (APEC) Strategy on Secure Online Space, the EU Cybersecurity Strategy, the OSCE Decision on Confidence-Building Measures, and the African Cybersecurity Convention.

Europe

Europe was one of the first regions to address cybersecurity. The CoE adopted the Convention on Cybercrime,[14] which entered into force on 1 July 2004. The Convention has inspired many other regional and national regulations on cybercrime worldwide. It is still a major international legal instrument in the digital field, with ratification by European countries, as well as the USA, Canada, Japan, and several other countries outside Europe. Given that it has been ratified by several non-European countries, there have been discussions about having the Convention as a global cybercrime instrument. However, some countries are reserved about acceding to the Convention, for different reasons ranging from symbolic ones (not participating in negotiation of the instrument) to substantive ones (e.g. the possibility of cross-border investigations).

At EU level, the Cybersecurity Strategy and the Directive on the security of network and information systems (NIS Directive) are the two main documents in the area of cybersecurity. The Strategy outlines a series of strategic priorities and actions aimed at addressing security challenges in cyberspace, with a focus on achieving cyber-resilience, drastically reducing cybercrime, developing a cyberdefence policy and capabilities, developing industrial and technological resources for cybersecurity, and establishing a coherent international cyberspace policy for the EU.[15] The Directive contains provisions on measures to be implemented by member states with the aim of achieving a high common level of cybersecurity within the EU. Such measures include, among others, the adoption of national strategies on the security of network and information systems, the designation of national competent authorities and of Computer Security Incident Response Teams (CSIRTs), and the identification of operators of essential services upon which obligations will be imposed to take appropriate security measures.[16]

The OSCE also works on cybersecurity, and particularly on the development of confidence-building measures (CBMs). These measures are generally designed to help improve relations between states, achieve a peaceful settlement of a conflict, or to prevent the outbreak of military confrontation. Two decisions of the OSCE Permanent Council on CBMs are the most notable examples of the OSCE's involvement in cyber space. The first set of OSCE CBMs from 2013 aims to reduce the risks of conflict stemming from the use of ICTs.[17] These voluntary measures include sharing national views on threats and best practices, cooperating with competent national bodies, consulting to reduce risks of misperception and possible tension or conflict, building up national legislation to allow information sharing, and sharing and discussing national terminology related to cybersecurity. In 2016, the second set of CBMs expanded the coverage, in particular towards public-private partnerships (PPPs).[18]

It is expected that new sets of CBMs might be agreed within the OSCE in the near future; more importantly, as the success of the CBMs penetrates diplomatic communities, it is likely that the CBMs might also feed into the further work of the UN GGE.

Americas

In 2003, the Organization of American States (OAS) set up the Inter-American Cyber-Security Strategy,[19] which pools the efforts of three related groupings of the organisation: the Inter-American Committee against Terrorism (CICTE), Ministers of Justice or Other Ministers or Attorneys General of the Americas (REMJA), and the Inter-American Telecommunication Commission (CITEL). These groups work with member states to implement programmes that will prevent cybercrime and protect CI by legislative and other procedural measures. The Working Group on Cybercrime, part of REMJA, organises technical workshops to strengthen the capacity of member states to develop legislation and procedural measures related to cybercrime and electronic evidence.[20]

Asia

In Asia, the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF) addresses cybersecurity confidence building measures and combating cybercrime. In 2012, the ARF produced a ministerial statement aimed at intensifying regional cooperation on ICT security.[21] In 2013, the ARF had cybersecurity on its agenda again, focusing on countering terrorism and transnational crime, while its Senior Officials Meeting on Transnational Crime decided to set up a Working Group on Cybercrime.[22]

The Shanghai Cooperation Organisation (SCO), which includes China, Russia, and Central Asian countries, has very intensive activities in the field of cybersecurity. It has adopted an agreement about cooperation in the field of ensuring international information security. Moreover, at the end of 2011, members of the SCO proposed an International Code of Conduct for Information Security to the UN, which was reintroduced in 2015, in an updated version.[23]

Africa

In Africa, cybersecurity policy has centred on drafting the African Union Convention on Cyber Security and Personal Data Protection.[24] This convention is currently in the ratification process. In general, in Africa the main focus is on capacity development for national and regional institutions in dealing with cybersecurity.

Bilateral activities

Increasingly, countries use bilateral tracks to address cybersecurity matters. They range from bilateral treaties via coordination agreements to informal consultations. The USA uses Mutual Legal Assistance Treaties (MLATs), signed by more than 20 countries, for cooperation in cybercrime matters. Many countries have signed cybersecurity cooperation agreements which specify exchange of information and coordinated activities.

In addition, major cybersecurity actors use regular bilateral dialogues as a way of increasing cooperation and defusing potential conflict. For example, China has dialogue with both the USA and the EU. Australia has developed cyber dialogues with China, the USA, South Korea, India, and New Zealand. India and Russia have established a cybersecurity dialogue and, in 2016, the two countries concluded a formal cyber agreement.

Technical and academic initiatives

CERTs/CSIRTs have been the main vehicle for technical cooperation in the field of cybersecurity. CERTs cooperate across national borders through regional cooperation. The

Forum of Incident Response and Security Teams (FIRST) coordinates an international technical network of national CERTs.

Business initiatives

A growing number of initiatives for improving security are coming from the business sector, especially the largest producers of software and hardware. Their involvement in the overall international policy framework is motivated on the one hand by the need to introduce technological improvements along with regulatory ones, and on the other hand, by their own business interests in raising trust and confidence in technology by end-users.

Microsoft has proposed a set of cybersecurity norms to reduce conflict in cyber-space,[25] the first such initiative of a corporate player in the field of international peace, which is commonly the realm of diplomats and states. In cooperation with the international High Technology Crime Investigation Association (HTCIA), Microsoft launched a Digital Crimes Community Portal which can be accessed by law enforcement agencies, to help them with cybercrime investigations.

Cisco has developed a range of network security certifications for IT professionals and organisations.

The external research and university relations departments within several multinational software and hardware companies all over the world, including Microsoft, SAP, Cisco, and others, are dedicated to building strong relationships with leading universities, government agencies, professional organisations, and industry partners, to advance research, enhance the teaching and learning experience, and inspire technological innovation. The cooperation is realised through a variety of programmes: joint research work by local academic institutions and local research branches of these companies, research grants, conference support, fellowships for PhD studies, or other work with universities, institutions, and schools to disseminate innovative curricula.

Main challenges in addressing cybersecurity issues

Terminological confusion in cybersecurity

Internet public policy is a policy field in the making. Thus, there is still a lot of terminological confusion, ranging from rather benign differences such as the interchangeable use of prefixes (cyber/e/digital/net/virtual) through to core differences, when the use of different terms reflects different policy approaches. In the area of cybersecurity, the potential for confusion is significant, starting from the very name used to describe this policy field. China, Russia, and the SCO countries use the broader term information security, which also covers political and social stability. They consider cybersecurity as a technical subset of information security. For the USA, the EU, and the OECD countries, cybersecurity is an umbrella term focusing mainly on protection of the Internet infrastructure. For these countries, information security is a subset of cybersecurity dealing mainly with data and information.

There are also differences in the way various players understand concepts such as CII, cyber-weapons, and cyber-terrorism. Addressing this terminological confusion is of utmost importance. To reach a common understanding on cybersecurity, the international community would need a lot of time and prolonged negotiations. Unfortunately, the risks

posed by misunderstandings are immediate and should not underestimated. A first step could be to identify different terminologies and map their precise semantic coverage. After this first step of identifying differences, it should be possible to identify possible convergences and gradually develop a common vocabulary on cybersecurity.

Multidisciplinary approach to cybersecurity

Cybersecurity cannot be addressed in isolation from other aspects of digital policy such as human rights and economic development, as illustrated by the policy triangle in Figure 12.[26]

A meaningful systematic response to cybersecurity risks therefore depends on a deep understanding of the multidisciplinary aspects of cyberspace: the nexus of technology, law, psychology, sociology, economy, political science, and diplomacy. The efficiency of the response further depends on partnerships among stakeholders that can contribute to reducing the risks:

- Government and regulatory authorities with their ability to create a legal, regulatory, and policy environment for cybersecurity.
- Judicial institutions and law enforcement authorities with their competences and responsibility for criminal prosecution and cross-border cooperation mechanisms.
- The private sector and technical communities with their expertise and *de facto* control over the majority of infrastructure, services, and standards.
- NGOs and academia with their knowledge, networks, and capacity to reach out to end-users and alert them to the misuse of cyberspace.

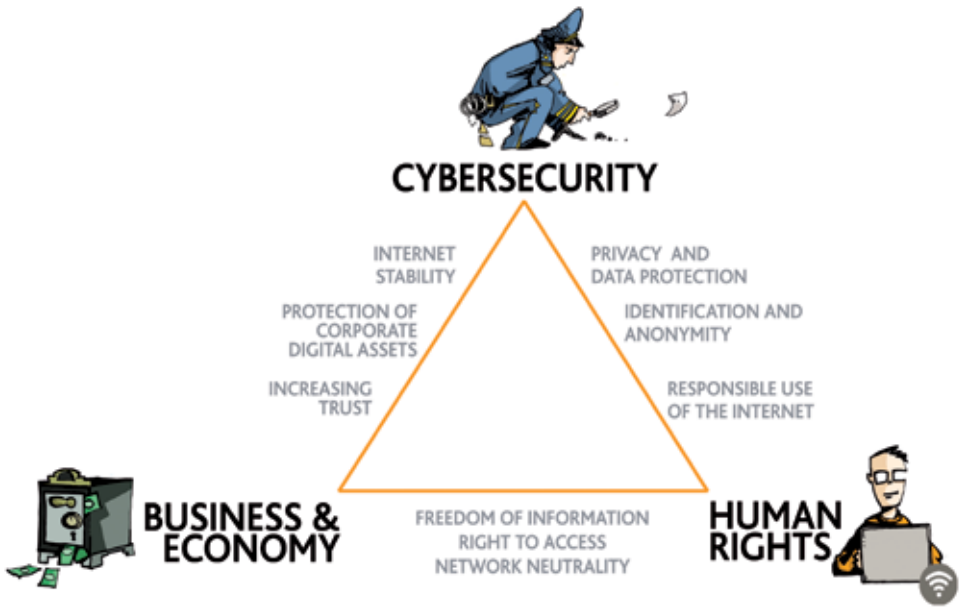

Figure 12. Cybersecurity policy triangle

Internet technical architecture and cybersecurity

The very nature of the Internet and how it is organised affects its security. Should we continue with the current approach of building security on a pre-existing, non-secure foundation or modify the basis of the Internet's infrastructure? How would such modifications affect other features of the Internet, especially its openness and its transparency? Most past development of Internet standards aimed at improving performance or introducing new applications. Security was not a priority. It is unclear whether the IETF will be able to change e-mail standards to provide proper authentication and, ultimately, reduce the misuse of the Internet (e.g. spam, cybercrime).

Given the controversy surrounding any changes to basic Internet standards, it is likely that security-related improvements in the basic Internet protocol will be gradual and slow. Yet important steps are starting to be implemented in this direction; the Domain Name System Security Extensions (DNSSEC)[27] is a good illustrative example. Following almost 12 years of research, trials, and debates within the technical community, DNSSEC was first deployed for some ccTLDs and from 2010 was also implemented at root server level. However, further challenges reside in the large-scale adoption of this new security standard down the ladder by the domain name registrars, ISPs, and website owners.

Important improvements to security, however, can be achieved through the proper configuration of the main Internet nodes such as the DNS servers around the world. Many incidents, such as the 2013 private cyberwar between two companies – CyberBunker and Spamhaus – that resulted in temporary congestion of large portions of the global Internet, are possible because of several dozens of millions of misconfigured DNS servers around the world known as open resolvers.[28] Besides, introducing security-by-design into all new technologies – software, hardware, and protocols – would bring additional security layers, which may include fortifications and blocking.

Cybersecurity, trust, and e-commerce

Cybersecurity is often mentioned as one of the preconditions for the rapid growth of e-commerce. Without a secure and reliable Internet, trust will be reduced and Internet users will be reluctant to provide confidential information online, such as credit card numbers. The same applies to online banking and the use of electronic money. We are seeing an increasing number of successful attacks on companies' servers to acquire customers' personal data and credit card numbers, such as the collection of over 1.2 billion user-name-and-password combinations and half a billion e-mail addresses stolen in 2014 by one group from Russia.[29] These incidents undermine user trust in online services. If general cybersecurity only slowly improves (and with an accompanying lack of standards), it is likely that the business sector will push for faster developments in cybersecurity. This may lead to further challenges for the principle of net neutrality and the development of 'a new Internet', which would facilitate, among other things, more secure Internet communication.

Surveillance and espionage

The 2013 revelations by NSA employee Edward Snowden confirmed that states – the USA included – exploit the vulnerabilities of the Internet for their own interests. The NSA's Personal Record Information System Methodology (PRISM) project based its surveillance capabilities on the ability to access the cables, routers, and cloud servers of major Internet companies (US-based telecoms, service, and content providers). In response, other coun-

tries – especially EU and BRICS (Brazil, Russia, India, China, and South Africa) – have started considering mitigation tactics, including laying their own intercontinental submarine cable connections,[30] and requiring Internet companies to store the personal data of their citizens in data centres within their jurisdictions.

Economic cyber espionage

In 2013, US-based security company Mandiant released a report about cyber-espionage attacks against US companies originated from China.[31] After the USA charged five Chinese 'military hackers', China in turn accused the USA of cyber-espionage, which resulted in the suspension of the activities of the China-US Cyber Working Group.[32] This crisis reached a peak before the visit of Chinese President Xi Jinping to the USA in September 2015, when the US government threatened sanctions against China because of economic cyber espionage. During the visit, the two countries agreed not to knowingly support cyber-espionage against the corporate sector.[33] This rule-in-the-making against economic cyber espionage received additional endorsement at the G20 meeting in Antalya (15–16 November 2015), where the G20 countries agreed 'that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors'.[34]

The increasing militarisation of cyberspace through the use of exploits and hacking tools by states is leading to increasing political tension. Such tension may accelerate the need for global efforts to prevent the proliferation of cyber-arms.

Cybersecurity and human rights

The link between cybersecurity and human rights is highly relevant for the future of the Internet. So far, these two fields are being addressed separately in their respective silos. However, recent experiences (SOPA, ACTA, PRISM/NSA) show that the protection of human rights (privacy, freedom of expression, access) is not only a value-based priority, it is also a very practical tool for ensuring that the Internet remains open and secure.

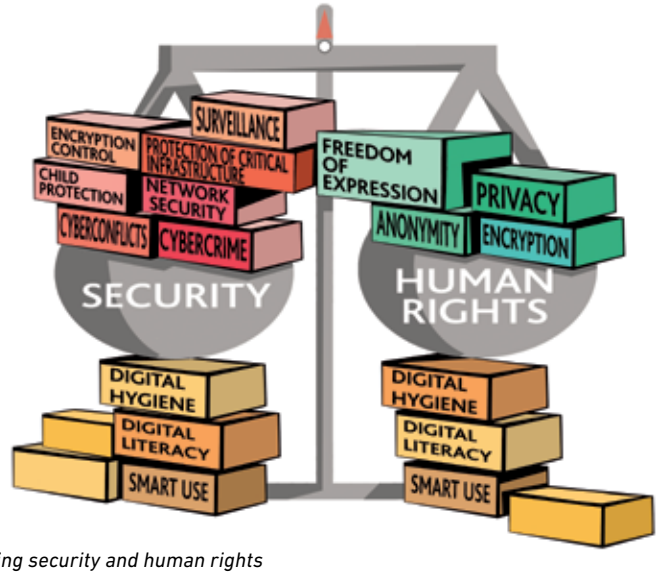

Figure 13. Balancing security and human rights

Individual Internet users are the pillars of cybersecurity. Yet they are often the weakest link when it comes to protection from cyber-attacks. Our personal computers are used to stage cyber-attacks (as part of botnets) and spread viruses and malware. Unprotected access to our computers and mobile devices offers a backdoor for access to the datasets of our companies or institutions, and compromises many more computers.

Concerns of the end-users, however, are usually not about possible greater damage (often due to ignorance) as a result of their compromised computer, but rather about the protection of their own data, and thus integrity and privacy in general. Post-PRISM discussions emphasise making personal computers more 'surveillance-safe', including how to employ encryption, regular patches and updates, IPSec, and VPNs[35] – awareness measures that would, in fact, also prevent unprotected access and contribute to better general cybersecurity.

Global cybersecurity – built around the important role of individual Internet users – has human rights as one of its cornerstones. The recognition of this link has already started emerging in policy documents. The EU's Cybersecurity Strategy, for instance, considers preserving an open, free, and secure cyberspace – including support for the promotion and protection of fundamental rights – as one of its five strategy pillars.

Cybersecurity and privacy are often depicted as offsetting each other in a balance, as can be seen in Figure 13. This is not always the case.

The main challenge is to aim for win/win solutions: more security implies more human rights and vice versa. In fact, there are many win/win areas in empowering and protecting individuals as pillars of the cybersecurity system (access to information, privacy protection), which should be given priority. Ultimately, human rights are a matter of cybersecurity realpolitik.

www.igbook.info/cybersecurity

Cybercrime

A dichotomy between real law and cyberlaw exists in the discussion of cybercrime. The real-law approach stresses that a cybercrime is the same as an offline crime, but is committed using using digital tools. The crime is the same, only the tools are different. The cyberlaw approach stresses that the unique elements of cybercrime warrant special treatment, especially when it comes to enforcement and prevention.

The drafters of the CoE Convention on Cybercrime were closer to the real-law approach, stressing that the only specific aspect of cybercrime is the use of ICT as a means of committing crime. The convention, which entered into force on 1 July 2004, is the main international instrument in this field.

The prominence of the cybercrime topic put it on the agenda of several international, regional, and local organisations, due to the continuous occurrence and diversification of crimes committed in relation to or by using electronic networking systems.[36] One example is the Commonwealth Cybercrime Initiative[37] that was born within the Commonwealth Internet Governance Forum (CIGF). The business sector has also recognised the importance of fighting cybercrime and has started private initiatives to support awareness campaigns and improvement of legal provisions.

The issues

Definition of cybercrime

Cybercrime is defined as crime committed via the Internet and computer systems. One category of cybercrimes is those affecting the confidentiality, integrity, and availability of data and computer systems. They include unauthorised access to computer systems, illegal interception of data transmissions, data interference (damaging, deletion, deterioration, alteration of suppression of data), system interference (the hindering without right of the functioning of a computer or other device), forgery, fraud, and identity theft. Other types of cybercrimes are content-related, and involve the production, offering, distribution, procurement, and possession of online content deemed as illegal according to national laws: online child sexual abuse material, material advocating a terrorist-related act, extremist material (material encouraging hate, violence, or acts of terrorism), cyber-bullying (engaging in offensive, menacing, or harassing behaviour using technology).

Cybercrime and the protection of human rights

The Convention on Cybercrime reinforced the discussion about the balance between security and human rights. Civil society actors have expressed concerns that the Convention provides state authorities with too broad a power, including the right to check personal computers, to undertake surveillance of communication, and more. These broad powers could potentially endanger some human rights, particularly privacy and freedom of expression.[38] The fact that the CoE – which deposits the Convention – actively promotes human rights, may help in establishing the necessary balance between the fight against cybercrime and the protection of human rights. In this context, it is worthwhile mentioning that the Council's Committee of Ministers adopted, in 2014, a Recommendation to member states on a Guide to human rights for Internet users, which outlines, among other provisions, that 'no one should be subject to unlawful, unnecessary, or disproportionate interference with the exercise of their human rights and fundamental freedoms when using the Internet.'[39]

Gathering and preserving evidence

One of the main challenges in fighting cybercrime is gathering evidence for court cases. The speed of today's communication requires a fast response from law-enforcement agencies. One possibility for preserving evidence is to be found in the network logs, which provide information about who accessed particular Internet resources, and when they did so. The Convention on Cybercrime specifies the obligation to preserve Internet traffic data.

Under the growing pressure of cyber threats and terrorist attacks, the EU took a step further and adopted a Data Retention Directive that required ISPs to retain traffic and location data 'for the purpose of the investigation, detection, and prosecution of serious crime, as defined by each member state in its national law'.[40] This provision faced strong criticism on privacy grounds and several states have either failed to enact national legislation to comply with the directive or have had such laws annulled as unconstitutional.[41] In December 2013, CJEU declared the Data Retention Directive incompatible with the Charter of Fundamental Rights.[42]

www.igbook.info/cybercrime

Critical infrastructure

According to the European Commission, CI consists of 'physical and information technology facilities, networks, services and assets' whose disruption or destruction could endanger the 'health, safety, security, or economic well-being of citizens or the effective functioning of governments'.[43] Examples of such infrastructures include those running the energy, transportation, and water supplies, communications, financial, and health services. Countries define their own CI depending on their national context; while most developed countries have already taken such a step and defined their CI, this is not yet the case for many developing countries.

More and more, CI relies on control systems that are based on digital code (such as supervisory control and data acquisition (SCADA) industrial control systems) and connected through IP-based networks (an Intranet, or, often, virtual private networks through the public Internet). While allowing for resource optimisation, this also leaves CI at risk of cyber-attacks. Such attacks may involve DDoS attacks (Figure 14), remote control over industrial systems, collection of sensitive information, or disruption of the regular work of the facilities by changing the control and command parameters – as was the case with the Stuxnet virus, or during the cyber-attack on a German steel factory at the end of 2014.[44]

Critical (information) infrastructure protection

A specific sub-group of CI is CII. The IETF Security Glossary defines CII as 'systems that are so vital to a nation that their incapacity or destruction would have a debilitating effect on national security, the economy, or public health and safety'.[45]

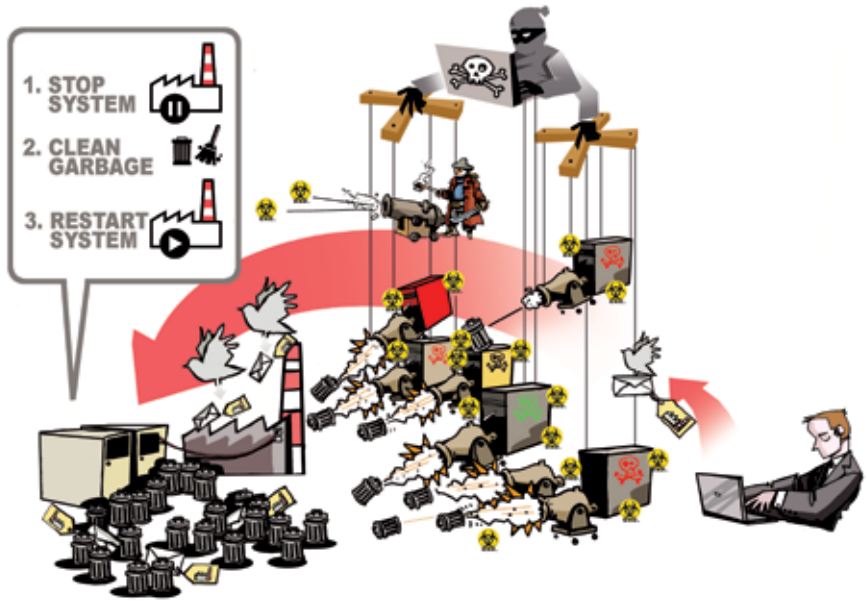

Figure 14. DDos attack on critical infrastructure

CII protection refers to rules, strategies, plans, and procedures that deal with preventing, preparing for, responding to, and recovering from disasters and emergencies. Usually several strategies are put together to protect CI. These strategies tackle aspects such as law enforcement and crime prevention, counter-terrorism, national security and defence, emergency management, business continuity planning, protective security, e-security, natural disaster planning and preparedness, risk management, professional networking, market regulation, planning and infrastructure development, and organisational resilience.

In the USA, the Presidential Policy Directive (PPD21) Critical Infrastructure Security and Resilience[46] of 2013 covers both the physical and virtual systems. In the EU, the European Programme for Critical Infrastructure Protection (EPCIP)[47] and the Directive on the identification and designation of European critical infrastructures[48] focus on the ICT sector as the key element. The EU Directive on network and information security, paired with the EU Cybersecurity Strategy, set a more specific guidance to member states on CIIP measures, including the setting up of CERTs. At the same time, the EU Agency for Network and Information Security (ENISA) is in charge of following up on the implementation of CIIP measures, and providing capacity-building measures and resources.

The OECD Recommendation of the Council on the protection of critical information infrastructures[49] outlines several steps that member states could take to protect their CII: at national level, states are invited to, among others, develop national strategies; identify government agencies and organisations responsible for CIIP; develop organisational structures for prevention and response, including independent CERTs; and consult with the private sector and build trusted PPPs. At international level, states are encouraged to enhance information sharing and strengthen cooperation across institutions in charge of CIIP.

www.igbook.info/critical

Cyberterrorism

There are various definitions of cyberterrorism. Many have simply used the definition of terrorism and applied it to the virtual world. There are countries, such as the UK, which define terrorism, but have no legal definition of cyberterrorism.[50] From academia, one – somewhat narrow – definition states that cyberterrorism is the 'use of information technology and means by terrorist groups and agents'.[51] A more comprehensive and broader definition states that cyberterrorism comprises 'unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives'.[52]

In practice, cyberterrorism is understood as including one or more of the following three aspects:

- Use of the Internet for conducting attacks by terrorist groups (DoS attacks, hacking attacks).
- Use of the Internet for preparing and organising of terrorist attacks.
- Use of the Internet for promoting terrorists' causes and recruiting terrorists.

Countering the distribution of terrorist propaganda and violent extremism materials online

The online distribution of terrorist propaganda and violent extremist material has become a recurrent theme in international politics, as well as a cause of concern for Internet companies.

As terrorists are growing increasingly sophisticated in using social media, and as these online platforms can reach more and more people around the world, the threat of online radicalisation has come into focus for many decision-makers. In April 2016, foreign ministers of China, India, and Russia made a joint statement highlighting the need to counter the rise of online terrorist content.[53] This topic also reached the level of the UN Security Council, which held an open debate on countering the narratives and ideologies of terrorism,[54] and it was further addressed by the G7 leaders[55] in Japan, in May 2016.

In addition to discussions on a political level, this has also become a concern for the private sector, most notably the Internet industry. In May 2016, Microsoft published its policies related to online terrorist content, as it feels 'a responsibility…not to contribute, however indirectly, to terrible acts'.[56] Google's tech incubator, Jigsaw, has been experimenting with YouTube videos by altering search engine algorithms in such a way that online searches for terrorist propaganda could redirect the user to anti-terrorist content instead.[57]

The practical operation of counter-extremist campaigns needs to be very carefully balanced with the right to freedom of expression. There is a delicate line between protecting security and promoting online censorship, and the location of this line is very much open to interpretation. This concern was highlighted by David Kaye, UN Special Rapporteur on Freedom of Expression, who argued that 'violent extremism' could be used as the 'perfect excuse' by governments to limit freedom of expression.[58] The right formula for content policy, one that ensures the maximum possible level of freedom of expression, while lowering radicalisation to a minimum, can only be found through a continued dialogue between security and human rights communities.

Initiatives to combat cyberterrorism

The lack of agreement on the definition of cyberterrorism can lead to misinterpretation and could possibly impact cooperation in mitigating threats and occurrences globally. But, despite that, countries are beginning to take the threat of cyberterrorism seriously. In 2012, the US Department of Defense was reported as accepting proposals for the development of software to predict 'cyberterrorism events' by detecting how criminal groups and hackers interact on the Internet.[59] The Clean IT Project, run by the Dutch Ministry of Security and Justice between 2011 and 2013, aimed to 'start a constructive dialogue between governments, businesses and civil society to explore how to reduce the terrorist use of the Internet'. It resulted in a set of general principles and an overview of best practices.[60]

The UN has been also paying increased attention to the issue of cyberterrorism. In September 2006, the UNGA adopted the United Nations Global Counter-Terrorism Strategy,[61] through which member states committed, among others, to coordinate efforts at the international and regional levels to counter terrorism in all its forms and manifestations on the Internet. Consequently, a Working Group on Countering the Use of the Internet for Terrorist Purposes was created within the UN Counter-Terrorism Implementation Task

Force, with the task of coordinating the activities of the UN system regarding the implementation of the strategy.

In 2012, the Working Group, in cooperation with the UNODC, issued a report exploring existing legal frameworks and practice at national and international levels related to the criminalisation, investigation, and prosecution of terrorist cases involving the Internet, while outlining a series of recommendations for states to enhance their cooperation in this field.[62] The Counter-Terrorism Committee of the UN Security Council has also been considering aspects and issues related to the use of the Internet for terrorist purposes. In December 2015, it held a meeting with UN member states, Internet companies, and civil society organisations, on preventing terrorists from exploiting the Internet and social media to recruit terrorist and incite terrorist acts, while respecting human rights and fundamental freedoms. Recommendations were made during the meeting on how states and the private sector could prevent and combat the use of cyberspace for terrorist purposes, while being compliant with human rights international instruments.[63]

www.igbook.info/cybercrime

Cyberconflict and warfare

Established international law regulates the conduct of traditional armed conflict and seeks to limit its effects. While there is growing agreement that existing international legal frameworks apply to online conflict as well, it is less clear how these frameworks apply in practice.

An additional challenge is the lack of common understanding of what constitutes an act of war in cyberspace. One possible definition suggests that cyberwar involves 'actions by a nation state to penetrate another nation's computers for the purpose of causing damage or disruption'.[64] Nevertheless, there is no agreement over definitions, especially among the key global powers.

A major characteristic of cyber-attacks is that they are almost impossible to attribute to certain perpetrators, let alone to states, due to the very complex and sophisticated weapons used which work through several proxy layers (including botnets). Moreover, unlike traditional warfare, cyber-conflicts do not take place between two nations while other countries silently watch. The Internet is a global resource and cyber-weapons, such as botnets, employ the computing resources of other nations without their consent, making cyberwarfare effectively global.

The landmark event that opened vast political debates about cyber-conflict and warfare was the country-scale attacks experienced by Estonia in April 2007. Estonia suffered DDoS attacks on its Internet infrastructure, foreign and defence ministries, leading newspapers, and banks.[65] Although circumstantial evidence pointed to connections between the attacks and Russia's opposition to the relocation of a monument of Soviet soldiers in Tallinn, there was no clear evidence of the involvement of Russian officials in the attacks. A case more often associated with cyberwarfare is the attacks on the Georgian online media and government servers during the conflict between Russia and Georgia in 2008. The case was referred to as 'cyber war',[66] even though there was no evidence of a state-sponsored attack by Russia.

The US and Israeli governments made the news for their alleged involvement in cyber-attacks on computer systems that run Iran's main nuclear enrichment facilities, unveiling the systematic use of cyber-weapons.[67] Iran, in turn, has been accused of mounting attacks on US banks and companies in retaliation for the USA's earlier actions.[68] The US government's accusations of North Korea hacking Sony in late 2014 went a step further, when the USA introduced economic sanctions.[69]

More subtle approaches to cyberwarfare have also been seen. The USA has accused China of systematically launching cyber-espionage activities against its government and corporate information infrastructures (such as Google and Microsoft), which China denies.[70] When 2014 reports from US-based security company Mandiant revealed details of the expanding Chinese cyber-espionage attempts, China responded that it was a victim, itself, linking these counter-accusations to a PRISM surveillance programme disclosed by Snowden revelations and warning that these incidents were jeopardising China-USA cooperation.[71]

Cyber-attacks in 'hybrid warfare'

The outputs of the 2015 Munich Security Conference see cyber-attacks as an important segment of hybrid warfare.[72] They refer to cyber-operations in peacetime aimed at harming the opponent's stability and growth without triggering actual war.

Utilising botnets and similar powerful Internet-based weaponry for conflicts and cross-border attacks has the same objective as traditional war: to gain the economic resources of another territory or to destroy enemy resources. Cyber-weapons can target the control systems of critical infrastructures such as power grids, air traffic control networks, or nuclear power plant safety systems (Figure 15).

Figure 15. Cyber-weapons

What is specific about cyber-attacks is that they are a cost-effective way of attacking enemies. For instance, research shows that investment in robust and powerful DDoS facilities that could perform a country-scale DDoS attack does not need to go above several thousand euro, while the economic damage of a such an attack would vary from €10 million per day for a transition country like Serbia, to over half a billion euro per day for a developed country like Switzerland.[73] Cyber-weapons can thus give additional power to players with limited resources.

Cyber-weapons may be used mainly as an addition to conventional operations rather than as an independent means of waging a war.

www.igbook.info/cyberconflict

Encryption

Encryption refers to the scrambling of electronic documents and communication into an unreadable format which can be accessed after decoding. Traditionally, governments were the only players who had the power and the know-how to develop and deploy powerful encryption in their military and diplomatic communications. Encryption became affordable to Internet users with applications such as Pretty Good Privacy. Recently, there have been many platforms offering encryption-protection communication, including Silent Circle, Telegraph, and Proton. In addition, Internet companies have started using powerful encryption for protection of their internal communication and users' data.

With encryption becoming affordable for basically all Internet users, including criminals and terrorists, the possible misuses of encryption tools have triggered one of the key digital policy debates worldwide among governments and business. The core of this debate is striking the right balance between the need to respect the privacy of communication of Internet users and the need for governments to monitor some types of communication of relevance for national security (potential criminal and terrorist activity remains an issue).

Main applications

Most often, we perceive encryption as a tool to protect the confidentiality of communications. On one hand, we should encrypt the content that is stored on our computer or in the cloud by using encryption tools, or demanding our cloud service operators to encrypt our content on their servers. On the other hand, we should also encrypt the content while it travels between our computer and the destination (be it a social network website or a friend's mailbox). Since the encryption process requires time and computing capacities, it may not be the default setting of many public providers of cloud or communication services due to mass of data they would need to encrypt, often in real-time. Yet more and more companies see encryption as an optional offer that can meet the increasing demand of the clients, thereby also increasing their competitiveness; the case of Apple and WhatsApp is the leading trend. There are also several available, and often free-source, software solutions for online anonymity that are based on encryption, such as the Tor network (an open software that was developed to protect privacy and fundamental freedoms by anonymising and preventing traffic analysis and surveillance).

Encryption is a critical component for additional security of key Internet protocols as well. IPSec, DNSSEC, and Border Gateway Protocol Security (BGPSec) are based on the distribution of digital certificates for servers and routers to be able to verify the identity of the IP numbers, domain names, and chosen routes and prevent spoofing and false impersonation by rogue servers. Similarly, the SSL (Secure Sockets Layer) establishes an encrypted link between a web server and a browser, ensuring that the communication between the two remain confidential and integral.

Encryption and standardisation

The advance of computing power enables faster encryption, but also faster cryptanalysis, forcing standards to change more regularly. The decision about which are the most sophisticated algorithms that should become *de facto* standards to be implemented in commercial products is made by engineers and scientists within their organisations such as the IETF, private non-for-profit organisations dealing with standards such as the American National Standards Institute, and national standardisation bodies of the economically most powerful nations (that can invest in cryptography), such as the US National Institute of Standards and Technology. With the growing geopolitical interest in Internet surveillance, confronted by a variety of trends for mass-use of encryption, national security services have started to show more interest in the scientist-driven standardisation processes: following Snowden revelations, *Der Spiegel* has reported that 'NSA agents travel to the meetings of the Internet Engineering Task Force (IETF), an organization that develops such standards, to gather information but presumably also to influence the discussions there.'[74]

International regimes for encryption tools

The international aspects of encryption policy involve coordination at the security and business levels.

For example, the US policy of export control of encryption software was not very successful because it could not control international distribution. US software companies initiated a strong lobbying campaign arguing that export controls do not increase national security, but rather undermine US business interests.

Encryption has been tackled in two contexts: the Wassenaar Arrangement and the OECD. The Wassenaar Arrangement is an international regime adopted by 41 countries to restrict the export of conventional weapons and 'dual use' technologies to countries at war or considered to be 'pariah states'.[75] The arrangement established a secretariat in Vienna. US lobbying, with the Wassenaar Group, aimed to extend the Clipper Approach[76] internationally, by controlling encryption software through a key escrow. This was resisted by many countries, especially Japan and the Scandinavian countries.

A compromise was reached in 1998 through the introduction of cryptography guidelines, which included a dual-use control list of hardware and software cryptography products above 56 bits. This extension included Internet tools, such as web browsers and e-mail. It is interesting to note that this arrangement does not cover 'intangible' transfers, such as downloading. The failure to introduce an international version of Clipper contributed to the withdrawal of this proposal internally in the USA itself. In this example of the link between national and international arenas, international developments had a decisive impact on national ones.

The OECD is another forum for international cooperation in the field of encryption. Although the OECD does not produce legally binding documents, its guidelines on various issues are highly respected. They are the result of an expert approach and a consensus-based decision-making process. Most of its guidelines are eventually incorporated into national laws. The question of encryption was a highly controversial topic in OECD activities. It was initiated in 1996 with a US proposal for the adoption of a key escrow as an international standard. Similar to Wassenaar, negotiations on the US proposal to adopt a key escrow with international standards were strongly opposed by Japan and the Scandinavian countries. The result was a compromise specification of the main encryption policy elements.

A few attempts to develop an international regime for encryption, mainly within the context of the Wassenaar Arrangement, did not result in the development of an effective international regime. It is still possible to obtain powerful encryption software on the Internet.

Security and human rights concerns

Encryption empowers citizens to protect their privacy. Encryption is also used by criminals and terrorists to protect their communications. They are becoming increasingly skilful in using the Internet to support logistics, such as purchasing weapons through the Internet, as in the case of the Paris terrorist attacks in 2015.[77] The use of publicly available anonymous proxy servers and anonymising services such as Tor to access the dark web, combined with money transfer through cryptocurrencies such as Bitcoin, leave very few traces and make online surveillance and digital forensics highly complex. In addition, increasingly secure mobile devices with cutting-edge encryption technology, such as iPhone or Silent Circle, and a variety of mobile applications for encrypted chat such as Telegram or Signal – while protecting lives of whistle-blowers and opposition activists around the world – also provide safe ground for internal coordination by terrorists while avoiding communication interception.

In response, governments and security services in many countries, including the UK, France, and the USA, are trying to introduce limits to the strength of encryption algorithms within mainstream products and services, and create mechanisms that would allow government agencies to access encrypted data if necessary. Moreover, some countries, such as the USA, the UK, and Russia, have also been working on introducing specific legislation that would require tech companies to allow law enforcement agencies to access encrypted data and/or devices (under more or less defined circumstances), or to assist them in accessing such data. Governments argue that access to encrypted data is becoming increasingly important for their actions aimed to prevent and prosecut serious crime, and ensure public safety.

Civil society and human rights communities have voiced strong concerns about these developments, additionally fuelled by the Snowden revelations, suggesting that such measures could be used for political censorship and disproportionate (mass) surveillance, while at the same time could compromise the identity of political activists, bloggers, and journalists in authoritarian states thereby risking their individual security. In addition, there have also been studies arguing that encryption may not protect criminals as much as law enforcement agencies tend to argue,[78] and that the introduction of mandatory backdoors into encrypted products would be ineffective.[79]

From a human rights standpoint, the right to privacy and other human rights should be protected, and encryption tools – including pervasive encryption – are essential to protect

privacy. The need for greater protection for encryption and anonymity was highlighted, for example, in the Report of the Special Rapporteur to the UNHRC on the use of encryption and anonymity to exercise the rights to freedom of opinion and expression in the digital age.[80]

Security and human rights aspects of encryption have been extensively debated at international level, especially following the highly publicised Apple-FBI case, which gained a lot of attention in the first half of 2016. The case, which involved a court order asking Apple to assist the FBI in unlocking an iPhone, triggered two opposing views. On one side, Apple, backed by other Internet companies, as well as human rights activists, argued that complying with the request would create a dangerous precedent and would seriously undermine the privacy and security of its users. On the other side, authorities argued that the case did not involve backdoors or decryption of devices, but rather a 'one-time' solution, necessary in the case; they also accused Apple of giving more value to its business interests than to a terrorism investigation. Although the case was eventually dropped (as the US Justice Department announced that it was able to unlock the iPhone with the assistance of a third party), it brought up several questions that remain open. On one hand, under what circumstances are authorities entitled to request tech companies to break the security systems they created for their devices? What safeguards are, or should be, in place? Should authorities be allowed to influence the way companies design their products? And on the other hand, to what extent should companies protect the privacy of their users? Should privacy be protected whatever the cost?[81]

There is increasing tension between the Internet industry which is looking at recovering trust, lost after the Snowden revelations, through introducing strong encryption by default, and security and intelligence services which are looking for ways to survey digital communications – and ultimately put an end to further open development and implementation of encryption tools. Should authorities have the right to explore existing vulnerabilities in commercial systems? Under what circumstances? Should they be obliged to disclose the identified vulnerabilities publicly or to a vendor, to enable patching of the service?

While these and other similar questions remain open, many Internet and technology companies continue to implement encryption in their products and services, and to search for solutions that would make such encrypted products and services unbreakable even for the producers (thus making obsolete any governmental request for assistance to break the encryption mechanisms or access the encrypted data).

www.igbook.info/encryption

The current situation

Spam is usually defined as unsolicited e-mail that is sent to a wide number of Internet users. Spam is mainly used for commercial promotion. Its other uses include social activism, political campaigning, and the distribution of pornographic materials, and, increasingly, malware. Besides the fact that it is annoying, spam also causes considerable economic loss, both in terms of bandwidth used and lost time spent checking/deleting it, but also because of the malware content delivered more and more often through spam (and which often results in bank account details and other economically sensitive information being stolen).[82]

Figure 16. Spam

Whereas 10 years ago spam was one of the key governance issues, today it is less prominent thanks to highly sophisticated technological filters. According to statistics for 2015, spam represented 54% of total inbound e-mail, compared to 84.9% in 2010.[83] However, researchers warn that, while the level of spam in e-mail traffic has constantly decreased in recent years, the quantity of e-mails with malicious content has increased significantly (Figure 16). For example, Kaspersky Lab noticed that the number of malicious spam e-mails sent in the first quarter of 2016 was 3.3 times higher than during the same period in 2015.[84] As an example, the 'famous' ransomware Trojan Locky, first identified in February 2016, has propagated around the world via spam e-mail messages; reports from April 2016 showed that there have been attempts to infect users with the Trojan in more than 110 countries.[85]

Spam can be combated through both technical and legal means. On the technical side, many applications for filtering messages and detecting spam are available. Several best practices have been developed by the technical community, include those by the Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG), the Spamhaus Project, the GSMA, and the Internet Society.

The legal response

Technical methods to combat spam have only a limited effect and require complementary legal measures. On the legal side, many states have reacted by introducing new anti-spam laws. In the USA, the Can-Spam Law involves a delicate balance between allowing e-mail-based promotion and preventing spam.[86] Although the law prescribes severe penalties for distributing spam, including prison terms of up to five years,[87] some of its provisions, according to critics, tolerate or might even encourage spam activity. The starting, default, position set out in the law is that spam is allowed until the receiver of spam messages says 'stop' (by using an opt-out clause).

In July 2003, the EU introduced its own anti-spam law as part of its Directive on privacy and electronic communications.[88] The EU law provides, as a general rule, that the sending

of e-mails for direct marketing may be allowed only if users have given their prior consent (the opt-in approach). However, there are exceptions in the case of pre-existing business or commercial relationships: the use of electronic contact details for direct marketing is allowed if users are given the opportunity to object to this either at the time of data collection, or at later stages (the opt-out approach). The directive also encourages self-regulation and private sector initiatives that would lead towards a reduction in spam.

Both of the anti-spam laws adopted in the USA and in the EU, have one weakness: a lack of provision for preventing cross-border spam. A similar conclusion was reached in a study on the EU anti-spam law carried out by the Institute for Information Law at the University of Amsterdam: 'The simple fact that most spam originates from outside the EU restricts the European Union's Directive's effectiveness considerably.'[89] A global solution is required, implemented through an international treaty or some similar mechanism.

An MoU signed in 2013 by Australia, Korea, and the UK is one of the first examples of international cooperation in the anti-spam campaign. The memorandum encourages cooperation in minimising spam originating in each country and being sent to end-users in each country. More recently, in June 2016, another MoU on fighting spam was signed between authorities in Canada, the USA, Australia, the Netherlands, Korea, New Zealand, and South Africa.[90]

The OECD has established a task force on spam and has prepared an anti-spam toolkit. The ITU has also been undertaking a series of activities aimed at combating spam. The ITRs contain provisions on the prevention of 'unsolicited bulk electronic communications', which are interpreted by some as also including e-mail spam. However, these provisions do not contain binding language; rather, they merely state that countries 'should endeavour to take the necessary measures' and encourages them to cooperate.

Refer to Section 4 for further discussion on the ITRs.

Similarly, a 2012 resolution of the ITU World Telecommunication Standardization Assembly (WTSA) invites states to take appropriate steps to combat spam, and refers only to national frameworks.[91] On the practical side, the ITU, through its Telecommunication Standardization Sector (ITU-T) works on identifying suitable modalities for combating spam; for example, the ITU-T Study Group 17 – Security carries out studies on potential measures to combat spam, and works on developing technical recommendations covering new forms of spam. Aspects tackled by the group include forms on spam in existing and future networks, effects of spam, technologies that empower the creation and spreading of spam, and solutions for countering spam. At regional level, APEC has prepared a set of Principles for Action against Spam,[92] and the AU has included provisions on 'advertising by electronic means' (including e-mail) in its Convention on Cyberspace Security and Protection of Personal Data.[93]

Another initiative dedicated to the fight against spam is the London Action Plan, which functions as a framework for international cooperation in enforcing spam-related legislation and addressing similar challenges such as online fraud, malware, phishing, and dissemination of viruses. The network, established in 2004, gathers regulatory authorities in more than 25 countries, as well as representatives of the technical community and the business sector.

The issues

Filtering systems

There are various issues associated with spam. From a technical perspective, one of the main problems with filtering systems is that they are known to delete non-spam messages, too. For instance, Verizon's anti-spam filtering led to a court case as it also blocked legitimate messages causing inconvenience for users who did not receive their legitimate e-mail. However, the anti-spam industry is a growing sector, developing increasingly sophisticated applications capable of distinguishing spam from regular messages.

Different definitions of spam

Different understandings of spam affect the anti-spam campaign. In the USA, a general concern about the protection of the freedom of speech and the First Amendment affect the anti-spam campaign as well. US legislators consider spam to be only 'unsolicited commercial e-mail' leaving out other types of spam, including political activism and pornography. In most other countries, spam is considered to be any 'unsolicited bulk e-mail' regardless of its content. Since most spam is generated from the USA,[94] this difference in definitions seriously limits any possibility of introducing an effective international anti-spam mechanism.

Spam and e-mail authentication

One of the structural enablers of spam is the possibility of sending e-mail messages with a fake sender's address. There is a possible technical solution to this problem, which would require changes in existing Internet e-mail standards. The IETF has been considering changes to the e-mail protocol, which would ensure the authentication of e-mail. This is an example of how technical issues (standards) may affect policy. A possible trade-off that the introduction of e-mail authentication would bring is the restriction of anonymity on the Internet.

The need for global action

Most spam originates from outside a given country. It is a global problem requiring a global solution. There are various initiatives that could lead towards improved global cooperation. Some of them, such as bilateral and multilateral MoUs, have already been mentioned. Other measures include capacity building and information exchange. A more comprehensive solution would involve some sort of global anti-spam instrument. So far, developed countries prefer the strengthening of national measures coupled with bilateral or regional anti-spam campaigns. Given their disadvantaged position of receiving a 'global public bad' originating mainly from developed countries, most developing countries are interested in shaping a global response to the spam problem.

www.igbook.info/spam

Digital signatures

Broadly speaking, digital signatures[95] are linked to the authentication of individuals on the Internet, and are important in the areas of jurisdiction, cybercrime, and e-commerce. The use of digital signatures should contribute to building trust on the Internet. Digital authen-

tication in general is often considered part of the e-commerce framework, as it is aimed at facilitating e-commerce transactions through the conclusion of e-contracts. For example, is an agreement valid and binding if it is completed via e-mail or through a website? In many countries, the law requires that contracts must be 'in writing' or 'signed'. What does this mean in terms of the Internet? How can the integrity of an electronically signed document be verified? Faced with these dilemmas and pressured to establish an e-commerce-enabling environment, many governments have started adopting legislation on digital signatures.

When it comes to digital signatures, the main challenge is that governments are not regulating an existing problem, such as cybercrime or copyright infringement, but creating a new regulatory environment for a development that is relatively new. This has resulted in a variety of solutions in the provisions on digital signatures. Three major approaches to the regulation of digital signatures have emerged.[96]

The first is a minimalist approach, specifying that electronic signatures cannot be denied because they are in electronic form. This approach specifies a very broad use of digital signatures and has been adopted in common law countries: the USA, Canada, New Zealand, and Australia.

The second approach is maximalist, specifying a framework and procedures for digital signatures, including cryptography and the use of public key identifiers. This approach usually specifies the establishment of dedicated certificate authorities, which can certify future users of digital signatures. This approach has prevailed in the laws of European countries, such as Germany and Italy.

The third approach combines the first two approaches. It has a minimalist provision for the recognition of signatures supplied via an electronic medium. The maximalist approach is also recognised through granting that 'advanced electronic signatures' will have stronger legal effect in the legal system (e.g. it will be easier to prove these signatures in court cases). This approach was adopted by the EU in its 1999 Directive on Electronic Signatures and its replacement, the Regulation on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation).[97] The EU regulation redefines the concept of advanced electronic signatures, introduces electronic trust services, and ensures a unified legal framework across the EU.

At global level, in 2001, the United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Signatures,[98] which grants the same status to digital signatures as to handwritten ones, provided some technical requirements are met.

Public key infrastructure (PKI) initiatives are directly related to digital signatures. Two organisations, the ITU and the IETF, are involved with PKI standardisation.

The issues

Authentication of users

Digital signatures are part of the broader consideration of the relationship between privacy and authentication on the Internet. They are just one of the important techniques used to identify individuals on the Internet.[99] For instance, in some countries where digital signature legislation or standards and procedures have not yet been set up, SMS authentication via mobile phones is used by banks to approve customers' online transactions.

The need for detailed implementation standards

Although many developed countries have adopted broad digital signature legislation, it often lacks detailed implementation standards and procedures. Given the novelty of the issues involved, many countries are waiting to see in which direction concrete standards will develop. Standardisation initiatives occur at various levels, including international organisations (ITU and ISO), regional bodies (European Committee for Standardization – CEN, ETSI, etc.), local bodies (such as the US National Institute of Standards and Technology) and professional associations (IETF).

Technological neutrality

New types of electronic signatures, such as biometrics, are being increasingly adopted in many countries. As with many other fields, especially those where technology and innovation evolve at a fast rate, legislators need to strike a balance between codifying such mechanisms, and at the same time legislating in technology-neutral ways to avoid the risk of legislation become obsolete quickly.

The risk of incompatibility

The variety of approaches and standards in the field of digital signatures could lead to incompatibility between different national systems. Patchwork solutions could restrict the development of e-commerce at a global level. The necessary harmonisation should be provided through regional and global bodies.

www.igbook.info/esignature

Child safety online

Children's use of the Internet is increasing. The Internet presents many benefits for children and young people,[100] including opportunities for their education, personal development, self-expression, and interaction with others. At the same time, it also presents risks to which children and young people are especially vulnerable.

When it comes to promoting the benefits of technology for children while at the same time fostering a safe and secure online environment, stakeholders need to strike a careful balance: on the one hand, children need to be protected against inappropriate content and risky behaviour; on the other hand, their rights to access to information and freedom of speech, among other rights, need to be respected.

Refer to Section 8 for further discussion on children's digital rights.

The challenges

Understanding how children use technology and the Internet is crucial for informing policy and initiatives related to children's online safety. The environment evolves quickly and

is constantly producing new technology that has a significant impact on the lives of children and their safety. Although there is no single blueprint that can universally apply to protecting children online, their attitudes and use of technology informs the policy-making processes and mobilises stakeholders to act.

Online risks for children

Despite the Internet's numerous benefits, children and young people face certain online risks when using the Internet and technology. While users of any age can face risks, children are particularly vulnerable, as they are still in the process of development. Based on various typologies,[101] we can summarise the risks to include:

Inappropriate content**.** Children can be exposed to content which is inappropriate for their age, including adult content and violent content. Violent games, for example, are rapidly becoming dominant over 'passive' violent movies, and often involve sophisticated weapons showing features of real weapons, and bloodshed.

Inappropriate contact. Children can be exposed to harmful contact, such as bullying and harassment, and are particularly vulnerable to this kind of contact when using the online communication tools such as social networks. While children often fall victim of their own peers, inappropriate contact can include more dangerous contact such as grooming by potential perpetrators of sexual abuse.

Inappropriate conduct. Children and young people often fail to fully comprehend the implications for themselves and others of their long-term 'digital footprints'. Inappropriate conduct includes publishing inappropriate comments, or revealing sensitive personal information or images that may have negative consequences. Sexting, or the sharing of sexual content predominantly through mobile technology, is an increasingly prevalent practice, and research has shown that young people are under more and more pressure to engage in it.

Consumer-related issues. Also referred to as commercial risks, consumer-related issues include being the target or recipient of inappropriate advertising, being exposed to hidden costs (such as applications inviting users to purchase a service) and receiving spam. Children also face risks related to online privacy and the collection of data, including geo-location data.

Despite the wide range of risks, research carried out in Europe suggests[102] that while children and young people may be more exposed to risks, not every risk leads to actual harm. Much depends on the child's age, gender, and resilience and resources to cope with the risks. Parents, guardians, educators, government, the business sector, and other stakeholders play an important role in protecting children online, and in helping them deal appropriately with risks.

Online child sexual abuse and exploitation

While the issue of child sexual abuse is not new, the Internet has exacerbated the problem. Predators are often able to explore their inclinations anonymously, and to find means of evading law enforcement. Some of the online risks described herein may result in sexual violence of one kind or another: children can be exposed to predators, leading to grooming and sexual exploitation; they can also become perpetrators, such as being persuaded to create and share sexual images of themselves, which may then be used to harass or threaten them.

When using social networks – which are often also used by abusers – children and young people are often not aware of the pitfalls of hidden identities. The masked identity is one of the most frequent approaches undertaken by abusers on the Internet, where virtual conduct can transform to offline contact, increasing the risk of abuse and exploitation of children, paedophilia, the solicitation of minors for sexual purposes, and even child trafficking.

Child sexual abuse images – commonly referred to as 'child pornography' in legislation[103] – are typically the digital representation of real-world sexual assault. Research shows that the victims of online child sexual abuse content are often very young, and the abuse violent and inhuman.

While the actual quantity of child sexual abuse content being shared online is admittedly difficult to determine, most content is found in the 'deep web', where content is not normally picked up by search engines. As many offenders become more security savvy and gain in-depth technical knowledge, Darknet is becoming very popular with predators and paedophiles.

Almost all child sexual abuse content circulating openly on the Internet is old content being recirculated; new content often indicates a new victim. When content depicting a child being sexually abused is discovered online, there are two clear priorities: to remove the content from public view, and to find the victim of abuse. The victim can then be removed from harm and offered the appropriate support.

Addressing the challenges

When it comes to online risks, an approach combining appropriate legislation and policy (including legislation, self- and co-regulation, and other policy measures), as well as technical tools, education, and awareness, can be used to tackle the risks in a broad way.

Legislative measures

From a normative point of view, many countries have enacted legislation that makes certain content illegal, even though definitions and interpretations may vary from country to country. On an international level, the key instruments are the UN Convention on the Rights of the Child and the Second Optional Protocol on the sale of children, child prostitution and child pornography; the CoE Convention on Cybercrime and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (also known as the Lanzarote Convention). The International Centre for Missing & Exploited Children (ICMEC) developed its framework for assessing national legislation, and uses it regularly to review legislation across countries.

Self- and co-regulatory measures

Self-regulation (voluntary agreement on the part of the industry) and co-regulation (combination of government and private regulation) are found to be effective approaches, especially by the industry. For example, ISPs may voluntarily provide for notice-and-take-down measures and may also filter certain types of illegal content; social media platforms can set minimum age requirements for children. A good working relationship between the industry and law enforcement, along with clearly defined processes and protocols for working together, is also important. In 2008, the CoE pub-

lished Guidelines for cooperation between law enforcement and ISPs against cybercrime.[104]

Technical measures

Various technical and process-based measures – which should be used in conjunction with other measures – can combat child sexual abuse. Hotline reporting mechanisms and notice-and-take-down requests often work together. The International Association of Internet Hotlines (INHOPE), a collaborative network of 51 hotlines across 45 countries (to date), processes thousands of reports annually, most of which are forwarded to law enforcement agencies within a day. Other technical measures include maintaining victim-identification databases and preventing access to certain sites, and the use of digital fingerprinting, data mining, and analytics to assist investigations.

Awareness raising and education

Many campaigns targeting children and young people, parents and guardians, and educators, have taken place at national, regional, and international levels. A wealth of awareness-raising resources is also available online. ITU's Child Online Protection (COP) initiative provides guidelines for children, parents and guardians, educators, the industry, and policymakers.[105] The Network of Safer Internet Centers (INSAFE), a European network of 31 national awareness centres, provides family toolkits in different languages. The Safer Internet Day, celebrated in several countries every February, is aimed at promoting the safer use of the Internet especially among children and young people worldwide.

Coordinated approach

Child online protection and combating online child sexual abuse and exploitation also require the concerted effort of stakeholders, who must act together in an effective and coordinated way.

Parents and educators have a responsibility to guide and support children, and play an important role in education and awareness, which is considered an important first line of defence. Governments have a primary responsibility to protect children, and in many countries, child online protection features high on national policy agendas. Law enforcement plays an important role in making the Internet safer from criminals, and also works at regional and international levels to combat online child sexual abuse. The European Police Office (Europol) and the International Criminal Police Organization (INTERPOL) both operate various databases that help identify victims of child sexual abuse.

The industry has the responsibility of ensuring that the online environment is safe and secure. Service providers can play a key role in creating such an environment, and many tools – such as filters and reporting mechanisms – can be used to this effect. Industry coalitions include the Technology Coalition; financial coalitions including the Financial Coalition Against Child Pornography in the USA, the Asia Pacific Financial Coalition, and the European Financial Coalition; and the global GSMA Mobile Alliance Against Child Sexual Abuse Content.

Many professionals who are experts in the field are likely to be active in civil society organisations, which can provide invaluable input through knowledge and experience. National

NGOs may cooperate through international networks, such as ECPAT International and ICMEC. Several regional initiatives and organisations also focus on child online safety.

Children's NGOs and child helplines are also key stakeholders in the fight against child sexual abuse and exploitation – both online and offline – and are valuable partners in understanding the scale and nature of the problem, and also in providing counselling and support for victims of abuse.

www.igbook.info/childsafety

Endnotes

1 Radunović V (2013) DDoS – Available Weapon of Mass Disruption. P*roceedings of the 21st Telecommunications Forum (TELFOR)*, 26–28 November, Belgrade, Serbia, pp. 5–9.

2 Goodin D (2015) Botnet that enslaved 770,000 PCs worldwide comes crashing down. *Arstechnica*, 13 April. Available at http://arstechnica.com/security/2015/04/botnet-that-enslaved-770000-pcs-worldwide-comes-crashing-down/ [accessed 21 October 2016].

3 United Nations General Assembly (1999) Resolution A/53/70. Developments in the Field of Information and Telecommunications in the Context of International Security. Available at http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70 [accessed 8 February 2016].

4 United Nations (2015) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Available at http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 [accessed 6 June 2016].

5 Grigsby A (2015) The UN GGE on cybersecurity: What is the UN's role? *Council on Foreign Relations Blog*, 15 April. Available at http://blogs.cfr.org/cyber/2015/04/15/the-un-gge-on-cybersecurity-what-is-the-uns-role/ [accessed 8 February 2016].

6 ITU (no date) Global Cybersecurity Agenda. Available at http://www.itu.int/osg/csd/cybersecurity/gca/ [accessed 22 October 2016].

7 ITU (no date) Global Cybersecurity Index. Available at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx [accessed 22 October 2016].

8 DiploFoundation (2015) IGF Summary. Just-in-time Reporting from the 2015 Internet Governance Forum. Available at http://digitalwatch.giplatform.org/sites/default/files/IGFReportWEB.pdf [accessed 8 February 2016].

9 Hague W (2011) London Conference on Cyberspace – Chairman's Summary. Available at https://www.gccs2015.com/sites/default/files/documents/London%20Conference%20on%20Cyberspace%20-%20Chair's%20Summary%20-%201-2%20Nov%202011%20_1_.pdf [accessed 8 February 2016].

10 Global Forum on Cyber Expertise (2015) The Hague Declaration on the GFCE. Available at https://www.thegfce.com/documents/publications/2015/04/16/the-hague-declaration-on-the-gfce [accessed 22 October 2016].

11 Statement by NATO Secretary General following the North Atlantic Council meeting at the level of NATO Defence Minister. Available at http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en [accessed 12 August 2016].

12 NATO Cooperative Cyber Defence Centre of Excellence (2013) Tallinn Manual on the International Law Applicable to Cyber Warfare. Available at https://ccdcoe.org/research.html [accessed 22 October 2016].

13 Klimburg A (Ed.) (2012) National Cyber Security Framework Manual. NATO Cooperative Cyber Defence Centre of Excellence Publication. Available at https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf [accessed 22 October 2016].

14 Council of Europe (2001) Convention on Cybercrime. Available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [accessed 21 October 2016].

15 European Union (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Available at https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-–-open-safe-and-secure-cyberspace [accessed 22 October 2016].

16 European Union (2016) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG [accessed 18 August 2016].

[17] OSCE (2013) Decision No. 1106 Initial Set of OSCE Confidence-building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies. Available at http://www.osce.org/pc/109168?download=true [accessed 22 October 2016].

[18] OSCE (2016) Decision No. 1202 OSCE Confidence-building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies. Available at http://www.osce.org/pc/227281?download=true [accessed 22 October 2016].

[19] Organization of American States General Assembly (2003) Resolution AG/RES.1939 (XXXIII-O/03). Development of an Inter-American Strategy to Combat Threats to Cybersecurity. Available at http://www.oas.org/juridico/english/agres_1939.pdf [accessed 22 October 2016].

[20] Organization of American States (2011) Inter-American Cooperation Portal on Cyber-crime. Available at http://www.oas.org/juridico/english/cyber.htm [accessed 8 February 2016].

[21] ASEAN Regional Forum (2012) Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security. Available at https://ccdcoe.org/sites/default/files/documents/ASEAN-120712-ARFStatementCS.pdf [accessed 8 February 2016].

[22] ASEAN (2014) ASEAN's Cyber Confidence Building Measures. Presentation by the ASEAN Secretariat. UNIDIR Cyber Stability Seminar 'Preventing Cyber Conflict', 10 February 2014, Geneva, Switzerland. Available at http://www.unidir.ch/files/conferences/pdfs/the-asean-s-cyber-confidence-building-measures-en-1-958.pdf [accessed 8 February 2016].

[23] Grigsby A (2015) Will China and Russia's updated code of conduct get more traction in a post-Snowden era? *Council on Foreign Relations blog*, 28 January. Available at http://blogs.cfr.org/cyber/2015/01/28/will-china-and-russias-updated-code-of-conduct-get-more-traction-in-a-post-snowden-era/ [accessed 22 October 2016].

[24] African Union (2014) African Union Convention on Cyber Security and Personal Data Protection. Available at http://www.au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection [accessed 6 June 2016].

[25] Microsoft (2015) International Cybersecurity Norms: Reducing Conflict in an Internet-dependent World. Available at http://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CFC36FD44/International_Cybersecurity_%20Norms.pdf [accessed 8 February 2016].

[26] For an in-depth analysis of the interplay in this policy triangle, consult the report from the 2015 IGF Workshop: Cybersecurity, human rights and Internet business triangle. Available at http://digitalwatch.giplatform.org/sessions/cybersecurity-human-rights-and-internet-business-triangle [accessed 6 June 2016].

[27] Domain Name System Security Extensions explained. Available at http://everything.explained.at/DNSSEC/ [accessed 21 October 2016].

[28] Radunović V (2013) Waging a (private) cyber war. Available at https://www.diplomacy.edu/blog/waging-private-cyberwar [accessed 22 October 2016].

[29] Perlroth N and Gellese D (2014) Russian gang said to amass more than a billion stolen Internet credentials. *New York Times*, 5 August. Available at http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html [accessed 22 October 2016].

[30] *RT* (2014) Brazil and the EU have pushed forward their dialogue on developing a direct submarine link. 24 February. Available at https://www.rt.com/news/brazil-eu-cable-spying-504/ [accessed 22 October 2016].

[31] Keck Z (2014) China expands cyber spying. *The Diplomat,* 12 April. Available at http://thediplomat.com/2014/04/china-expands-cyber-spying/ [accessed 22 October 2016].

[32] Ranger S (2014) We're the real hacking victims, says China. *ZDNet*, 20 May. Available at hhttp://www.zdnet.com/article/were-the-real-hacking-victims-says-china/ [accessed 22 October 2016].

[33] Spetalnick M and Martina M (2015) Obama announces 'understanding' with China's Xi on cyber theft but remains wary. *Reuters*, 26 September. Available at http://www.reuters.com/article/us-usa-china-idUSKCN0RO2HQ20150926 [accessed 8 February 2016].

[34] G20 (2015) G20 Leaders' Communiqué. Antalya Summit, 15–16 November 2015. Available at http://g20.org/English/Documents/PastPresidency/201512/P020151228335504307519.pdf [accessed 8 February 2016].

[35] Schneier B (2013) NSA surveillance: A guide to staying secure. *The Guardian*, 6 September. Available at https://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance [accessed 22 October 2016].

[36] For a listing of anti-cybercrime networks, organisations and initiatives worldwide, refer to the CoE's resources page. Available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/networks/Networks_en.asp [accessed 22 October 2016].

[37] The Commonwealth (no date) Commonwealth Cybercrime Initiative. Available at http://thecommonwealth.org/commonwealth-cybercrime-initiative [accessed 22 October 2016].

[38] Bailey C (2002) The International Convention on Cybercrime. Association for Progressive Communications. Available at http://rights.apc.org/privacy/treaties_icc_bailey.shtml [accessed 7 March 2016].

[39] Council of Europe (2014) Recommendation CM/Rec (2014)6 of the Committee of Ministers to member states on a Guide to human rights for Internet users. Available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d5b31 [accessed 20 October 2016].

[40] European Union (2006) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF [accessed 22 October 2016].

[41] For a detailed overview of the data retention issues in EU, refer to European Commission (2011) Evaluation report on the Data Retention Directive (Directive 2006/24/EC). Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF [accessed 22 October 2016].

[42] CJEU (2014) Judgement of the Court in Joined Cases C-293/12 and C-594/12: Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and Others. Available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=106306 [accessed 22 October 2016].

[43] European Commission (2004) Critical Infrastructure Protection in the Fight Against Terrorism. Communication from the Commission to the Council and the European Parliament. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52004DC0702 [accessed 22 October 2016].

[44] Essers L (2014) Cyberattack on German steel factory causes 'massive damage'. *IT World*, 19 December. Available at http://www.itworld.com/article/2861675/cyberattack-on-german-steel-factory-causes-massive-damage.html [accessed 22 October 2016].

[45] IETF (2007) Internet Security Glossary, Version 2. Available at https://tools.ietf.org/html/rfc4949 [accessed 18 August 2016].

[46] USA White House (2013) Presidential Policy Directive – Critical Infrastructure Security and Resilience. Available at https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [accessed 18 August 2016].

[47] European Commission (2006) European Programme for Critical Infrastructure Protection. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33260 [accessed 18 August 2016].

[48] European Union (2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF [accessed 18 August 2016].

[49] OECD (2008) Recommendation of the Council on the Protection of Critical Information Infrastructures. Available at http://webnet.oecd.org/OECDACTS/Instruments/ShowInstrumentView.aspx?InstrumentID=121&InstrumentPID=117&Lang=en&Book= [accessed 22 October 2016].

[50] The Cyberterrorism Project (2013) What is cyberterrorism? UK Legal Definition. Available at http://www.cyberterrorism-project.org/what-is-cyberterrorism [accessed 22 October 2016].

[51] Krasavin S (2009) What is Cyber-terrorism? Computer Crime Research Center. Available at http://www.crime-research.org/library/Cyber-terrorism.htm [accessed 22 October 2016].

[52] Denning D (2000) Statement. Available at http://fas.org/irp/congress/2000_hr/00-05-23denning.htm [accessed 22 October 2016].

[53] Joint Communiqué of the 14th Meeting of the Foreign Ministers of the Russian Federation, the Republic of India and the People's Republic of China, 18 April 2016. Available at http://mea.gov.in/bilateral-documents.htm?dtl/26628/Joint_Communiqu_of_the_14th_Meeting_of_the_Foreign_Ministers_of_the_Russian_Federation_the_Republic_of_India_and_the_Peoples_Republic_of_China [accessed 22 October 2016].

[54] UN News Centre (2016) Security Council requests UN panel to propose global framework on countering terrorist propaganda. 11 May. Available at http://www.un.org/apps/news/story.asp?NewsID=53909#.WAszjTeZIqZ [accessed 22 October 2016].

[55] G7 (2016) G7 Action Plan on Countering Terrorism and Violent Extremism. Available at http://www.mofa.go.jp/files/000160278.pdf [accessed 22 October 2016].

[56] Microsoft (2016) Microsoft's approach to terrorist content online. Available at http://blogs.microsoft.com/on-the-issues/2016/05/20/microsofts-approach-terrorist-content-online/#sm.00001i30hhw72cdzpxr8cky3uuvbs [accessed 22 October 2016].

[57] Greenberg A (2016) Google's clever plan to stop aspiring ISIS recruits. *Wired*, 17 September. Available at https://www.wired.com/2016/09/googles-clever-plan-stop-aspiring-isis-recruits/ [accessed 22 October 2016].

[58] UN News Centre (2016) UN expert warns combat against violent extremism could be used as 'excuse' to curb free speech. 3 May. Available at http://www.un.org/apps/news/story.asp?NewsID=53841#. WAs1FjeZIqb [accessed 22 October 2016].

[59] GCN (2012) DOD wants cyberterrorism-prediction software. 31 July. Available at http://gcn.com/articles/2012/07/31/agg-dod-small-biz-software-support.aspx [accessed on 22 October 2016].

[60] The Clean IT Project (2012) About the project. Available at http://www.cleanitproject.eu/about-the-project/ [accessed 18 August 2016].

[61] United Nations General Assembly (2006) Resolution A/60/288. The United Nations Global Counter-Terrorism Strategy. Available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/60/288 [accessed 22 October 2016].

[62] UNODC (2012) The use of the Internet for terrorist purposes. Available at https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf [accessed 22 October 2016].

[63] UN Security Council Counter-Terrorism Committee (2015) Special Meeting of the Counter-Terrorism Committee and technical sessions of the Counter-Terrorism Committee Executive Directorate on preventing and combating abuse of ICT for terrorist purposes. Available at http://www.un.org/en/sc/ctc/news/2015-11-18_CTED_SpecialMeeting_ICT.html [accessed 22 October 2016].

[64] Berenger RD (2012) Cyber Warfare. In Yan Z [ed] *Encyclopedia of Cyber Behavior*. Hershey, PA: Information Science Reference, pp. 1074–1087.

[65] *BBC News* (2007) Estonia hit by 'Moscow cyber war'. 17 May. Available at http://news.bbc.co.uk/2/hi/europe/6665145.stm [accessed 22 October 2016].

[66] Swaine J (2008) Georgia: Russia 'conducting cyber war'. *The Telegraph*, 11 August. Available at http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html [accessed 22 October 2016].

[67] Sanger D (2012) Obama sped up wave of cyberattacks against Iran. *New York Times*, 1 June. Available at http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html [accessed 22 October 2016].

[68] Nakashima E (2012) Iran blamed for cyberattacks on U.S. banks and companies. *The Washington Post*, 21 September. Available at https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html [accessed 22 October 2016].

[69] Lee C and Solomon J (2015) US targets North Korea in retaliation for Sony hack. *The Wall Street Journal*, 3 January. Available at http://www.wsj.com/articles/u-s-penalizes-north-korea-in-retaliation-for-sony-hack-1420225942 [accessed 22 October 2016].

[70] Foster P (2013) China denies Pentagon cyber-attack claims. *The Telegraph*, 7 May. Available at http://www.telegraph.co.uk/news/worldnews/asia/china/10040757/China-denies-Pentagon-cyber-attack-claims.html [accessed 22 October 2016].

[71] Ranger S (2014) We're the real hacking victims, says China. *ZDNet*, 20 May. Available at http://www.zdnet.com/article/were-the-real-hacking-victims-says-china/ [accessed 22 October 2016].

[72] Munich Security Conference (2015) Collapsing Order, Reluctant Guardians? Munich Security Report 2015. Munich Security Conference. Available at https://www.securityconference.de/en/activities/munich-security-report/ [accessed 22 October 2016].

[73] Radunović V (2013) DDoS – Available Weapon of Mass Disruption. *Proceedings of the 21st Telecommunications Forum (TELFOR)*, 26–28 November, Belgrade, Serbia, pp. 5–9.

[74] Appelbaum *et al.* (2014) Prying Eyes: Inside the NSA's War on Internet Security. *Der Spiegel*, 28 December. Available at http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html [accessed 11 August 2016].

[75] The Wassenaar Arrangement. Available at http://www.wassenaar.org/ [accessed 22 October 2016].

[76] The Clipper approach was proposed by the US government back in 1993. At its core was the use of a Clipper chip which was supposed to be used in all telephones and other voice communication tools. The Clipper chip had a 'backdoor' which could be used by governments for lawful surveillance. After strong opposition from human rights activists and the general public, the US government dropped this proposal in 1995. Denning D (1995) The case for clipper. *MIT Technology Review*. MIT: Cambridge, MA, USA. Available at http://encryption_policies.tripod.com/us/denning_0795_clipper.htm [accessed 22 October 2016].

[77] Huggler J (2015) Man arrested in Germany on suspicion of illegal arm dealing in terror crackdown. *The Telegraph*, 27 November. Available at http://www.telegraph.co.uk/news/worldnews/europe/germany/12020249/Paris-attackers-bought-weapons-from-arms-dealer-in-Germany.html [accessed 11 August 2016].

[78] A study published by the Berkman Centre for Internet and Society at Harvard University argues that 'the "going dark" metaphor does not fully describe the future of the government's capacity to access the communications of suspected terrorists and criminals. The increased availability of encryption technologies certainly impedes government surveillance under certain circumstances, and in this sense, the government is losing some surveillance opportunities. However, [...] the combination of technological developments and market forces is likely to fill some of these gaps and, more broadly, to ensure that the government will gain new opportunities to gather critical information from surveillance.' For more details, refer to The Berkman Center for Internet and Society at Harvard University (2016). Don't Panic. Making Progress on the 'Going Dark' Debate. Available at https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [accessed 12 July 2016].

[79] A survey looking into 865 hardware or software products incorporation encryption, from 55 country, points out to the fact that, because of the wide availability of such products, any mandatory backdoors required for by law enforcement authorities 'will be ineffective'. This is because such backdoors are easy to be evaded, given that the marketplace for encryption products is international and criminals can switch to products that are not covered by national legislation in a certain jurisdiction. Instead, any national law mandating backdoors will affect the 'innocent users of those products', leave people in the respective country 'vulnerable to abuse of those backdoors by cybercriminals and other governments'. For more details, refer to Schneier B, Seidel K and Vijayakumar S (2016) A Worldwide Survey of Encryption Products. Available at https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf [accessed 12 July 2016].

[80] The report is available at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32 [accessed 12 July 2016].

[81] DiploFoundation (2016) Apple vs FBI: A Socratic dialogue on privacy and security DiploFoundation blog 22 March. Available at https://www.diplomacy.edu/blog/apple-vs-fbi-socratic-dialogue-privacy-and-security [accessed 11 August 2016].

[82] The Dridex financial Trojan caused serious concerns in 2016, with cybersecurity firms describing it as 'one of the most serious online threats facing consumers and businesses'. The Trojan, distributed through large spam campaigns, is capable of collecting banking credentials from customers of hundreds of banks and other financial institutions around the world. For more

details, read: O'Brien D (2016) Dridex: Tidal waves of spam pushing dangerous financial Trojan. Symantec. Available at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf [accessed 14 July 2016].

[83] Trustwave (2016) Global Security Report. Available at https://www.trustwave.com/Resources/Trustwave-Blog/Introducing-the-2016-Trustwave-Global-Security-Report/ [accessed 13 July 2016].

[84] Gudkova D *et al.* (2016) Spam and phishing in Q1 2016. Kaspersky Lab. Available at https://securelist.com/analysis/quarterly-spam-reports/74682/spam-and-phishing-in-q1-2016/ [accessed 13 July 2016].

[85] The way Locky works is simple: users are tricked into opening malicious attachments sent through spam e-mails. Once installed on the users' devices, the Trojan encrypts all data and the user is then asked to pay a ransom to get the files decrypted. For more information about Locky, read: Sinitsyn F (2016) Locky: the encryptor taking the world by storm. Kaspersky Lab. Available at https://securelist.com/blog/research/74398/locky-the-encryptor-taking-the-world-by-storm/ [accessed 14 July 2016].

[86] More references to Can-Spam are available at the Bureau of Consumer Protection (2009). The CAN-SPAM Act: A Compliance Guide for Business. Available at https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business [accessed 22 October 2016].

[87] In June 2016, a US citizen was sentenced to two and a half years in prison and was ordered to pay USD310,628.55 in restitution for sending over 27 million spam messages to Facebook users. According to the Office of the US Attorney for the Northern District of California, the man illegally obtained, stored, and exploited Facebook user accounts' information and earned money by directing users to other websites. The scheme, which was executed between November 2008 and March 2009, compromised approximately 500,000 legitimate Facebook accounts. For more details, read the press release from the Office of the US Attorney for the Northern District of California. Available at https://www.justice.gov/usao-ndca/pr/sanford-spam-king-wallace-sentenced-two-and-half-years-custody-spamming-facebook-users [accessed 13 July 2016].

[88] European Union (2012) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002L0058 [accessed 22 October 2016].

[89] *BBC NEWS* (2004) European anti-spam laws lack bite. 28 April. Available at http://news.bbc.co.uk/2/hi/technology/3666585.stm [accessed 6 October 2016].

[90] New Zealand Law Society (2016) NZ signatory to international anti-spam MOU. 15 June. Available at https://www.lawsociety.org.nz/news-and-communications/latest-news/news/nz-signatory-to-international-anti-spam-mou [accessed 22 October 2016].

[91] ITU (2012) Resolution 52 of the World Telecommunication Standardization Assembly: Countering and combating spam. Available at https://ccdcoe.org/sites/default/files/documents/ITU-121129-CombSpamWTSARes52.pdf [accessed 22 October 2016].

[92] APEC (2012) APEC Principles for Action against Spam. Available at http://www.apec.org/Meeting-Papers/Sectoral-Ministerial-Meetings/Telecommunications-and-Information/2005_tel/annex_e.aspx [accessed 22 October 2016].

[93] African Union (2014) African Union Convention on Cyber Security and Personal Data Protection. Available at http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf [accessed 22 October 2016].

[94] Up-to-date statistics on spam-enabling countries are provided by The Spamhaus Project, and can be found at https://www.spamhaus.org/statistics/countries/ [accessed 14 July 2016]. Spamhaus also provides statistical information on several other spam-related issues, such as spam support ISPs, worst spammers, countries with the highest number of detected spam-bots, the most spam-abused TLDs, etc.

[95] The authentication and verification of an electronic record using cryptographic algorithms; 'electronic signatures' is a broader term that includes a wider range of authentication techniques such as digital signatures and biometrics.

[96] For a more detailed explanation of these three approaches, consult: ILPF (1999) Survey of International Electronic and Digital Signature Initiatives. Available at http://www.ilpf.org/groups/survey.htm#IB [accessed 21 August 2016].

[97] European Union (2014) Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG [accessed 12 August 2016].

[98] UNCITRAL (2001) Model Law on Electronic Signatures. Available at http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/2001Model_signatures.html [accessed 22 October 2016].

[99] Longmuir G (2000) Privacy and Digital Authentication. Available at www.longmuir.net/papers/Research%20Paper.doc [accessed 20 August 2016]. This paper focuses on the personal, community, and governmental aspects of the need for authentication in a digital world.

[100] In line with legal instruments and international practice, a 'child' is understood to include is any person under the age of 18 years.

[101] Typologies include Barbosa A *et al.* (2013) Risks and Safety on the Internet: Comparing Brazilian and European Results. London: LSE. Available at http://eprints.lse.ac.uk/54801/ [accessed 9 August 2016]; OECD (2012) The Protection of Children Online; Recommendation of the OECD Council. Available at http://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf [accessed 9August 2016].

[102] EU Kids Online (2014) *EU Kids Online: Findings, Methods, Recommendations.* London: LSE. Available at http://eprints.lse.ac.uk/60512/ [accessed 9 August 2016].

[103] The term 'child pornography' poses a problem as it is typically associated with depictions of sexual activity between consenting adults. Since the terms fails to highlight the abusive and exploitative aspects, it is increasingly avoided in favour of more preferred terminology, including 'child sexual abuse material', and 'child sexual exploitation material'. Interagency Working Group on Sexual Exploitation of Children (2016) Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Available at http://www.ilo.org/ipec/Informationresources/WCMS_490167/lang--en/index.htm [accessed 12 August 2016].

[104] Council of Europe (2008) Guidelines for the cooperation between law enforcement and Internet service providers against cybercrime. Available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3ba [accessed 22 October 2016].

[105] ITU (no date) Guidelines for Child Online Protection. Available at http://www.itu.int/en/cop/Pages/guidelines.aspx [accessed 22 October 2016].

Section 4

THE LEGAL BASKET

The legal basket

The core social functions of the law remain as relevant in the Internet era as they were thousands of years ago, when our far predecessors started using rules to organise human society. Law is about regulating rights and responsibilities among individuals and the entities they establish, from companies to national states. Rule of law and legal certainty are essential for the further growth of the Internet, as a medium of social communication, and as a driver of economic development.

The legal regulation of the Internet has evolved from cyberlaw to a real-law approach. In the early days of the Internet, the cyberlaw approach prevailed, based on the assumption that the Internet introduced new types of social relationships in cyberspace. Consequently, there was a need to formulate new cyberlaws to regulate cyberspace. One argument for this approach was that the sheer speed and volume of Internet-facilitated cross-border communication would hinder the enforcement of existing legal rules. Another frequent argument was that traditional regulation (e.g. related to crime, taxation) would not be efficient enough.[1] It is, however, important to keep in mind that laws do not make prohibited behaviour impossible, only punishable.

More recently, however, with the mainstreaming of the Internet into social life, the real-law approach has gained prominence. According to this approach, the Internet is essentially treated no differently from previous telecommunications technologies, in the long evolution from smoke signals to the telephone. Consequently, existing legal rules can also be applied to the Internet. For example, the 2013 report of the UN GGE reiterated that existing international law applies to the use of ICT by states.[2] This conclusion was later welcomed by the UNGA, during the WSIS+10 review process.[3] In the field of human rights, resolutions of the UNGA and the UNHRC have firmly established the principle that the same human rights that people enjoy offline must also be protected online.[4]

While the answer to the question *if* existing law is applicable to the Internet is positive, the main remaining question is *how* to implement existing rules. For example, an important challenge is to ensure legal redress in cases related to the Internet that contain international elements. Individuals and companies can rely on international private law, while national governments can use international public law mechanisms. Both approaches have a long tradition, and were originally developed in an era of less intensive exchanges across national borders. They need to be examined and, when needed, further developed to provide affordable access to justice in Internet matters to individuals and institutions worldwide.

Legal instruments

A wide variety of legal instruments exist that have either already been applied or could be applied to the Internet field. They are classified as instruments applicable at national level and instruments applicable at international level.

National legal instruments, social norms, and self-regulation

Most Internet-related legal regulation happens at national level. This creates an unavoidable tension with the predominantly cross-border nature of Internet communication. Some court decisions, as in the case of the right to be forgotten, have a broader impact beyond their jurisdictional space. It is expected that citizens and companies will increasingly use national courts (in the case of the EU, the supranational CJEU) to protect their legal rights and interests on the Internet.

Legislation

Legislative activities have progressively intensified in the field of the Internet. This is especially the case within countries where the Internet is widely used and has a high degree of impact on economic and social relations. To date, the priority areas for Internet legislation have been privacy and data protection, intellectual property, taxation, and cybercrime.

Continuous progress in the technological field has also led to the adoption of the principle of technological neutrality, which is to be followed when legislation that touches on technology-related issues is elaborated. In practice, this principle means that the law should not make explicit reference to specific technologies, or favour one technology over another; rather, general terms are to be used that would allow the law to remain neutral.

Yet, social relations are too complex to be regulated only by legislators. Society is dynamic and legislation always lags behind societal change. This is particularly noticeable today, when technological developments are reshaping social reality much faster than legislators can follow. Sometimes, rules become obsolete even before they come into force. The risk of legal obsolescence is an important consideration in Internet regulation.

Social norms (customs)

Like legislation, social norms proscribe certain behaviour. Unlike legislation, no state power enforces these norms. They are enforced by the community through peer-to-peer pressure. In the early days of the Internet, its use was ruled by a set of social norms labelled 'netiquette', where peer pressure and exclusion were the main sanctions. During this period – in which the Internet was used primarily by relatively small, mainly academic communities – social norms were widely observed. The growth of the Internet has made those rules ineffective. This type of regulation, however, can still be used within restricted groups with strong community ties. For example, the Wikipedia community is governed by social norms regulating how Wikipedia articles are edited and how conflicts over articles are settled. Through codification into policy and guidelines, Wikipedia norms have been gradually evolving into self-regulation.

Self-regulation

The US government's 1998 White Paper on Internet Governance[5] that paved the way for the foundation of ICANN, introduced self-regulation as the preferred regulatory mechanism for the Internet. Self-regulation has elements in common with social norms. The main difference is that unlike social norms, which typically involve tacit and diffused rules, self-regulation is based on an explicit and well-organised set of rules. Self-regulation usually codifies a set of rules of what is considered proper form of ethical conduct.

The trend towards self-regulation is particularly noticeable among ISPs. In many countries, ISPs are under increasing pressure from government authorities to enforce rules

related to content policy. ISPs try to answer this pressure through self-regulation, by imposing certain standards of behaviour for their customers.

While self-regulation can be a useful regulatory technique, some risks remain in using it for regulating areas of high public interest, such as content policy, freedom of expression, and protection of privacy. Reliance on self-regulation raises several questions, such as: Can and should ISPs make decisions in lieu of legal authorities? Can and should they judge what is acceptable content?

Jurisprudence

Jurisprudence (court decisions) has had a significant impact on legal developments related to the Internet. In early phases, when most of the Internet developments happened in the USA, jurisprudence, as the cornerstone of the US legal system, played the key role in Internet-related legal developments. The Internet, as a new phenomenon, was regulated through court cases (precedents in the Anglo-Saxon law). Judges had to decide cases even if they did not have the necessary tools, i.e., legal rules. Through precedents, they started developing a new law.

More recently, the jurisprudence of European courts has become particularly important for online legal developments. For example, a CJEU judgement from May 2014 introduced new rules on the right to be forgotten, or more precisely, the right to be de-indexed, with implications for online content in Europe and beyond. Another judgement, in October 2015, which invalidated the Safe Harbour agreement between the USA and the EU, had a similar impact, as it forced the two sides to negotiate and agree on a new agreement on the transfer of personal data across the Atlantic.

Refer to Section 8 for further discussion on CJEU decisions in the field of privacy and data protection.

International legal instruments

The cross-border nature of Internet activities implies the need to use international legal tools. In discussions on international law, there is a terminological confusion that could have substantive consequences. The term *international law* is mainly used as a synonym for international *public* law, established by nation states, usually through the adoption of treaties and conventions. International public law applies to many areas of the Internet including telecommunications, human rights, and cybercrime, to name a few. However, international *private* law is equally, if not more, important, for dealing with Internet issues, since most Internet court cases involve aspects such as contracts, torts, and commercial responsibilities.

International private law

Given the global nature of the Internet, legal disputes involving individuals and institutions from different national jurisdictions are frequent. The rules of international private law specify the criteria for establishing applicable jurisdiction and law in legal cases with foreign elements (e.g. legal relations involving two or more entities from different countries), for example, who has jurisdiction in potential legal cases between Internet companies (e.g. Facebook, Twitter) and their users scattered all over the world. The jurisdiction criteria include the link between an individual and national jurisdiction (e.g. national-

ity, domicile) and the link between a particular transaction and national jurisdiction (e.g. where the contract was concluded, where the exchange of goods took place).

However, only rarely has international private law been used to settle Internet-based issues, possibly because its procedures are usually complex, slow, and expensive. The main mechanisms of international private law were developed at a time when cross-border interaction was less frequent and intensive, and proportionally fewer cases involved individuals and entities from different jurisdictions. International private law needs to become faster, cheaper, and more flexible in order to ensure legal redress in Internet-related legal cases.

International public law

International public law regulates relations between nation states. Some international public law instruments already deal with areas of relevance to Internet governance (e.g. telecommunications regulations, human rights conventions, international trade treaties). A number of elements of international public law could be used for Internet governance, including treaties and conventions, customary law, soft law, and *ius cogens* (compelling law – a peremptory norm).

International conventions

International conventions are legally binding agreements between states. The main set of conventions that are seen by some as touching on Internet-related issues is the ITU's ITRs. Adopted in 1988, at a time when the Internet was still in its early stages of development, the ITRs did not contain specific provisions on the Internet. Discussions on whether the ITRs should be expanded to explicitly cover the Internet were held at WCIT-12. Several proposals were made at that time that could have had a significant impact on how the Internet functions, on its underlying principles, as well as on Internet security and Internet content-related issues. Member states could not reach an agreement on this issue, and the revised 2012 ITRs still do not contain explicit references to the Internet. Nevertheless, some ITU member states considered that several provisions in the revised ITRs could be interpreted as potentially covering sensitive Internet-related issues, which, in their view, should be outside of the scope of ITU activities.[6] These states decided not to sign the revised regulations, thus continuing to remain bound by the 1988 version.

Apart from the ITU conventions, the only convention that deals directly with Internet-related issues is the CoE Convention on Cybercrime. However, many other international legal instruments are applicable to Internet issues, from the UN Charter to more specific instruments dealing with, for example, human rights, trade, and IPR.

International customary law

The development of customary law includes two elements: general practice *(consuetudo)* and recognition that such practice is legally binding *(opinio juris)*. It usually requires a lengthy time-span for customary law to emerge. For example, the Law of the Sea rules were crystallised over the centuries through established practices of national governments, until these rules were codified in the UN Law of the Sea Convention (1982). However, the faster pace of modern developments requires a shorter time-span for development of customary rules. One possible solution for overcoming the tension between fast Internet growth and the slow development process of customary law, was proposed by Italian jurist, Roberto Ago, who introduced the concept of *diritto spontaneo* or 'instant customary international law'.[7]

Soft law

The term 'soft law' is frequently used in the Internet governance debate. Most definitions of soft law focus on what it is not: it is not a legally binding instrument. Typically, soft law instruments contain principles and norms, which are usually found in international documents such as declarations and resolutions. Since it is not legally binding, soft law cannot be enforced through international courts or other dispute resolution mechanisms.

The main WSIS documents – including the Final Declaration, the Geneva Plan of Action, the Tunis Agenda for the Information Society, and Regional Declarations – have the potential to develop certain soft law norms. They are not legally binding, but they are usually the result of prolonged negotiations and acceptance by nation states. The commitment that nation states and other stakeholders have to make in negotiating soft law instruments and reaching a necessary consensus creates the first element in considering that such documents are more than simple political declarations.

Soft law provides certain advantages in addressing Internet governance issues. First, it is a less formal approach, not requiring ratification by states and, thereby, not requiring prolonged negotiations. Second, it is flexible enough to facilitate the testing of new approaches and adjust to rapid developments in the field of Internet governance. Third, soft law provides greater opportunity for a multistakeholder approach than does an international legal approach restricted to states and international organisations.

Ius cogens

Ius cogens is described by the Vienna Convention on the Law of Treaties[8] in Article 53 as a 'norm, accepted and recognised by the international community of States as a whole, from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character'. Professor Ian Brownlie, former fellow of All Souls College at the University of Oxford, listed the following examples of *ius cogens* rules:

- The prohibition of the use of force.
- The law of genocide.
- The principle of racial non-discrimination.
- Crimes against humanity.
- Rules prohibiting trade in slaves and piracy.[9]

In Internet governance, *ius cogens* could be relevant in dealing with online activities that promote and/or facilitate the organisation of activities prohibited by *ius cogens* (such as genocide, racial discrimination, slavery, etc.)

Jurisdiction

Jurisdiction is the authority of the court and state organs to decide on legal cases. The relationship between jurisdiction and the Internet has been ambiguous, since jurisdiction rests predominantly on the geographical division of the globe into national territories.

Each state has the sovereign right to exercise jurisdiction over its territory. However, the Internet facilitates considerable cross-border exchange, difficult (although not impossible) to monitor via traditional government mechanisms. The question of jurisdiction on the Internet highlights one of the central dilemmas associated with Internet governance: How is it possible to anchor the Internet within existing legal and political geography?[10]

In recent years, courts have been faced with an increasing number of cases with a strong jurisdictional element. The judgments on the right to be forgotten, cases involving authorities requesting data located in other jurisdictions, and the invalidation of the Safe Harbour Framework are notable examples. In these cases, the jurisdiction 'arm' was extended beyond national or EU territories.

Several of these cases have been decided in European courts, with numerous consequences:

- European courts are asserting their jurisdiction over a growing number of cases involving US companies.
- The role of regulators in Europe, especially data protection authorities, is more prominent.
- Global jurisprudence concerning Internet-related issues is increasingly being shaped by European courts.

Jurisdiction principles

Three main considerations are important when deciding on jurisdiction:

- Which court or state authority has the proper authority? (procedural jurisdiction)
- Which rules should apply? (substantive jurisdiction)
- How should court decisions be implemented? (enforcement jurisdiction)

The following criteria establish jurisdiction in particular cases:

- Territorial Principle – the right of the state to rule over people and property within its territory.
- Personality Principle – the right of the state to rule over its citizens wherever they might be (nationality principle).
- Effects Principle – the right of the state to rule on economic and legal effects on its territory, stemming from activities conducted abroad.

Another important principle introduced by modern international law is that of universal jurisdiction.[11] 'The concept of universal jurisdiction in its broad sense [is] the power of a state to punish certain crimes, wherever and by whomsoever they have been committed, without any required connection to territory, nationality, or special state interest.'[12]

Universal jurisdiction covers such crimes as piracy, war crimes, and genocide. However, the Internet has functionally introduced universal jurisdiction to a much broader

set of cases based on the principle of accessibility. According to this principle, accessing the Internet from a specific country is sufficient basis for the jurisdiction of the country's courts to apply. This principle was used by the French court in the Yahoo! case,[13] as well as the CJEU in the eData[14] and Pinckney[15] cases. The possibility of invoking jurisdiction through a limited criterion such as Internet access could give rise to several issues, including forum-shopping. Namely, the court proceeding could be initiated from any country with access to the Internet.

Conflict of jurisdiction

The conflict of jurisdiction arises when more than one state claims jurisdiction on a particular legal case. This usually happens when a legal case involves an extra-territorial component (e.g. involves individuals from different states, or international transactions). The relevant jurisdiction is established by one of the following elements: territoriality, nationality, or effect of action. When placing content, or interacting on the Internet, it is difficult to know which national law, if any, might be violated. In this context, almost every Internet activity has an international aspect that could lead to multiple jurisdictions or a so-called spill-over effect.[16]

Jurisdiction and access to content

One of the early and frequently quoted cases that exemplify the problem of multiple jurisdictions is the 2001 Yahoo! case in France. It was prompted by a breach of French law, which prohibits the exhibition and sale of Nazi objects, even though the website that provided these items – the Yahoo.com auction website – was hosted in the USA, where the display of such material is legal. The court case was solved using a technical solution (geo-location software and filtering of access). Yahoo! was forced to identify users who accessed the site from France and block their access to the web pages showcasing Nazi materials.[17]

Similarly, the right to be forgotten judgment (Google *et al.* v Mario Costeja Gonzalez *et al.*) imposed upon search engines the obligation to consider requests from European users to remove certain results from searches. The judgment was further shaped by rulings of data protection authorities in Europe. Applying reasoning similar to the one used in the Yahoo! case, the French regulator, for example, ruled[18] that the delisting of results must be enforced by Google globally, and not only across its European extensions (such as .fr, .es, and .uk).

Jurisdiction and data protection

The protection of EU citizens' personal data stored beyond Europe's borders has contributed to some of the most disputed cases in recent years. In 2013, Maximilian Schrems, an Austrian national, filed a complaint asking the Irish Data Protection Commissioner to prohibit Facebook from transferring his personal data to the USA. Schrems argued that the USA does not provide adequate protection to users' data since the data is subject to mass surveillance under US laws. As the Commissioner denied the request, Schrems contested the decision in court. The case was eventually brought to the CJEU, which ruled that the Safe Harbour Framework governing the transfer of personal data between the EU and the USA was invalid.[19] This led to the Safe Harbour agreement being later replaced with the EU-US Privacy Shield Framework.

Refer to Section 8 for further discussion on Safe Harbour and Privacy Shield.

Considerations about data protection have contributed to two developments. The first is that several companies have moved their data centres and data processing functions to jurisdictions known for adopting a more relaxed regulatory approach, most notably Ireland. While this has not spared companies from court proceedings, a 2016 ruling involving Microsoft confirmed that the USA cannot utilise a local search warrant to obtain access to data stored in Ireland.[20]

The second is that some countries, such as China and Russia, have enacted legislation requiring the data of users to be stored locally. The storage of data on servers located within the national territory is an important pillar of the Chinese policy towards achieving cyber-sovereignty.

Jurisdiction and terms of use

The jurisdiction provision in companies' terms of use has also been in focus in many court rulings, with many court cases involving Facebook.

One prominent case involved a French teacher whose Facebook account was suspended after posting images of a nude painting which hangs at the Musée d'Orsay. The Paris Court of Appeal ruled[21] that Facebook could be sued in France, rejecting the social network's argument that its terms of use state that California has jurisdiction. The French court paved the way for other lawsuits against the company outside US jurisdiction.

In June 2016, an Israeli court ruled that a clause in Facebook's terms of use requiring all suits to be heard in California courts is invalid, and approved a class action case against Facebook.[22] The case argued that Facebook had violated users' privacy by using private posts to determine which advertisements users should see, without obtaining their prior consent.

Besides technical solutions (geo-location and filtering techniques), other approaches for solving the conflict of jurisdiction include the harmonisation of national laws and the use of alternative dispute resolution mechanisms.

The harmonisation of national laws

The harmonisation of national laws could result in the establishment of one set of compatible rules at global level. With harmonised rules in place, the question of jurisdiction would become less relevant. Harmonisation might be achieved in areas where a high level of global consensus already exists, for example, regarding child sexual abuse content, piracy, slavery, and terrorism. Views are converging on other issues, too, such as cybercrime. In some fields, however, including content policy, it is not very likely that a global consensus on the basic rules will be reached, since cultural differences continue to clash in the online environment more saliently than in the offline world.[23]

Another potential consequence of a lack of harmonisation is the migration of content to countries with lower levels of Internet regulation. Using the analogy of the Law of the Sea, some countries could become 'flags of convenience' for online content.

www.igbook.info/jurisdiction

Alternative dispute resolution

The alternative dispute resolution (ADR) is a mechanism available in place of traditional courts. ADR tools include arbitration and mediation. Online dispute rresolution (ODR) uses the Internet and technology in the process of dispute resolution.

When it comes to Internet cases, these mechanisms – in particular, arbitration – are used extensively to fill the gap engendered by the inability of current international private law to deal with numerous Internet legal cases. An example is the UDRP, developed by WIPO and ICANN as the primary dispute resolution procedure in issues related to domain name registrations.

In arbitration, decisions are made by one or more independent individuals chosen by the disputants. The mechanism is usually set out in a private contract, which also specifies issues such as place of arbitration, procedures, and choice of law. International arbitration within the business sector has a long-standing tradition.

Table 2 presents a short overview of the main differences between traditional court systems and arbitration.

Table 2. Differences between court and arbitration

Elements	Court	Arbitration
Organisation	Established by national laws and treaties	Permanent and ad hoc arbitrations (settled and/ or selected by parties)
Applicable law	The law of the court (the judge decides the applicable law)	Parties can choose the law; if they do not, then the law indicated in the contract is used; if there is no indication, then the law of the arbitration body is used
Procedure	Court procedures settled by laws/treaties	Settled by parties (temporary, ad hoc) Settled by arbitration body regulation (permanent)
Enforcement	Enforced by national authorities	Enforced in accordance with the arbitration agreement and the New York Convention

In comparison to traditional courts, arbitration offers many advantages, including higher flexibility, lower expenses, speed, choice of jurisdiction, and the easier enforcement of foreign arbitration awards.

One of the main advantages of arbitration is that it overcomes the potential conflict of jurisdiction. Arbitration has particular advantages regarding one of the most difficult tasks in Internet-related court cases – enforcement of court judgements. The New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards[24] regulates the enforcement of arbitration awards. According to this convention, national courts are obliged to enforce arbitration awards. It is often easier to enforce arbitration awards in foreign countries by using the New York Convention regime rather than to enforce foreign court judgement.

The main limitation of arbitration is that it cannot address issues of higher public interest such as protection of human rights; these require the intervention of state-established courts. Other limitations also exist:

- Since arbitration is usually established by prior agreement, it does not cover a wide area of issues when no agreement between parties has been set in advance (libel, various types of responsibilities, cybercrime).

- Many view the current practice of attaching an arbitration clause to regular contracts as disadvantageous for the weaker side in the contract (usually an Internet user or an e-commerce customer).

- Some are concerned that arbitration extends precedent-based law (US/UK legal system) globally and gradually suppresses other national legal systems. In the case of e-commerce, this might prove to be more acceptable, given the already high level of harmonisation of commercial regulations in precedent law. However, an extension of precedent law has become more delicate in sociocultural issues such as Internet content, where a national legal system reflects a specific cultural context.

Arbitration has been used extensively in commercial disputes. There is a well-developed system of rules and institutions dealing with commercial disputes. The main international instrument is the United Nations Commission on International Trade Law (UNCITRAL) 1985 Model Law on International Commercial Arbitration.[25] The leading international arbitrations are usually attached to chambers of commerce.

ADR, ODR, and the Internet

Arbitration and other alternative dispute resolution systems are used extensively in Internet-related cases, and the previously mentioned UDRP is one example in this regard. Since the beginning of its work under the UDRP in December 1999, the WIPO Arbitration and Mediation Center has administered more than 35 000 domain name cases.[26]

The UDRP is stipulated in advance as a dispute resolution mechanism in all contracts involving the registration of domain names under gTLDs (e.g. .com, .edu, .org, .net) and some ccTLDs as well. Its unique aspect is that arbitration awards are applied directly through changes regarding the disputed domain name (the cancellation of the domain name, or the transfer of the domain name registration to the complainant), without resorting to enforcement through national courts.

The EU introduced a new dispute resolution platform in 2016. The Online Dispute Resolution platform, operational since February 2016, aims to help consumers and traders settle their online disputes over online domestic and cross-border purchases.[27]

A number of Internet companies (e.g. Google, Facebook, and Twitter) have also developed their own mechanisms. Following the CJEU ruling on the right to be forgotten, Google established a special mechanism allowing individuals to request the removal of websites from search results. From May 2014 to October 2016, Google received over 575 000 requests for removal.[28]

This dispute resolution practice opened a wide range of questions: Should private companies provide dispute resolution? What are the procedural and substantive rules to be applied? How can access to these mechanisms be ensured for affected Internet users?

www.igbook.info/arbitration

Intellectual property rights

Knowledge and ideas are key resources in the global economy. The protection of knowledge and expression of ideas, through IPR has become one of the predominant issues in the Internet governance debate, and has a strong development-oriented component. IPR have been affected by the development of the Internet, mainly through the digitisation of knowledge and information, as well as through new possibilities for their manipulation. Internet-related IPR include copyright, trademarks, and patents. Other IPR include designs, utility models, trade secrets, geographical indications, and plant varieties.

© Copyright

Copyright is a legal term which describes the rights that creators have over their original works. Copyright only protects the expression of an idea when it is materialised in various forms, such as a book, CD, or computer file. The idea itself is not protected by copyright. In practice, however, it is sometimes difficult to make a clear distinction between the idea and its expression.

The copyright regime has closely followed the evolution of technology. Every new invention, such as the printing press, radio, television, and the VCR, has affected both the form and the application of copyright rules. The Internet is no exception. The traditional concept of copyright has been challenged in numerous ways, from those as simple as cutting and pasting texts from the web to more complex activities, such as the massive distribution of music and video materials via the Internet.

The Internet also empowers copyright holders by providing them with more powerful technical tools for protecting and monitoring the use of copyrighted material. These developments endanger the delicate balance between authors' rights and public interest, which is the very basis of the copyright law (Figure 17).

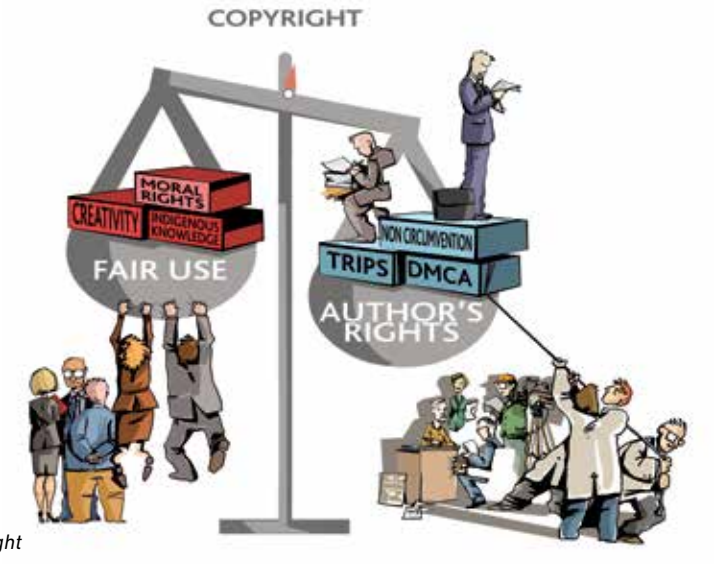

Figure 17. Copyright

So far, copyright holders, represented by major record and multimedia companies, have been very active in protecting their IPR. The public interest is often seen as having been vaguely perceived and not sufficiently protected. This, however, has gradually been changing, mainly through numerous global initiatives focusing on the open access to knowledge and information (e.g. Creative Commons).

The current situation

Stricter copyright protection at national and international level

The recording and entertainment industries have been lobbying intensively at national and international levels to strengthen copyright protection. At international level, the protection of digital artefacts was introduced in the WIPO Copyright Treaty[29] (1996). This treaty also contains provisions for tightening the copyright protection regime, such as stricter provisions for the limitations of authors' exclusive rights, the prohibition of circumventing the technological protection of copyright, and other related measures. At a regional level, the IPR provisions in the Trans-Pacific Partnership Agreement, a trade agreement among 12 Pacific Rim countries, signed in February 2016, carry tough enforcement rules in addition to increasing the copyright term.[30] In the USA, stricter protection of copyright was introduced through the US DMCA[31] of 1998.

Several regulations have been proposed at national and international level, aiming to enforce tighter control by forcing Internet intermediaries to filter or monitor the dissemination of copyrighted content. They triggered strong public protest, which stopped the adoption of these regulations. In 2011, in the USA, two bills were promoted – SOPA[32] and the PROTECT IP Act (PIPA)[33] – which provided new means to fight online piracy, including blocking access to infringing websites and banning search engines from linking to such sites. Both bills were postponed, following protests. At international level, ACTA[34] tried to address IPR infringements in a way that may have opened the possibility for private (companies) enforcement and policing actions. After strong protests in Europe, the European Parliament voted against ACTA.

These regulatory actions have been harshly criticised by academics and civil liberties groups on the grounds of human rights and freedoms. Individual Internet users have joined online and offline protests.[35]

Software against copyright infringement

Copyright offenders use software tools, for example, to distribute music and videos illegally online. Copyright defenders can use software, too. Traditionally, state authorities and businesses carried out their responsibilities in this field through legal mechanisms. However, the use of 'alternative' software tools by the business sector against copyright offenders is increasing.

Some software-based tactics used or advocated over time by recording/entertainment companies aim to protect their copyrights:

- A Trojan redirects users to websites where they can legitimately buy the copyright-protected work (e.g. a song) they tried to download.
- Freeze software blocks computers for a period of time and displays a warning about downloading pirated content.
- Hard drive scans find and attempt to delete any pirated files found.
- Interdiction prevents access to the Internet for those who try to download or share pirated content.

Such measures have been seen by some as having the potential of being illegal.[36] The question being raised is whether companies using such self-help measures are breaking the law.

Technologies for digital rights management

As a long-term and more structural approach, the business sector introduced various technologies for managing access to copyright-protected materials. Microsoft introduced digital rights management software to manage the downloading of sound files, movies, and other copyrighted materials. Similar systems were developed by Xerox (ContentGuard), Philips, and Sony (InterTrust).

The use of technological tools for copyright protection finds legal basis in the WIPO Copyright Treaty and in the DMCA. Moreover, the DMCA criminalises activity aimed at circumventing the technological protection of copyrighted materials.

The issues

Amend existing or develop new copyright mechanisms?

How should copyright mechanisms be adjusted to reflect the profound changes effected by ICT and Internet developments? One answer suggested by the US government's White Paper on Intellectual Property and the National Information Infrastructure[37] is that only minor changes are needed in existing regulation, mainly through 'dematerialising' the copyright concepts of 'fixation', 'distribution', 'transmission', and 'publication'. This approach was followed in the main international copyright treaties, including the Trade-Related aspects of Intellectual Property Rights (TRIPS) agreement and the WIPO Copyright Treaty.

However, the opposite view argues that changes in the legal system must be profound, since copyright in the digital era no longer simply refers to the 'right to prevent copying' but also to the 'right to prevent access'. Ultimately, with ever-greater technical possibilities of restricting access to digital materials, the question is whether copyright protection is necessary at all. It remains to be seen how the public interest, the second part of the copyright equation, will be protected.

Protection of public interest – the fair use of copyrighted materials

Copyright was initially designed to encourage creativity and invention. It combines two elements: the protection of the author's rights and the protection of the public interest. The main challenge is to stipulate how the public could access copyrighted materials to enhance creativity, knowledge, and global wellbeing. Operationally speaking, the protection of the public interest is ensured through the concept of the 'fair use' of protected materials.[38]

Copyright and development

The stricter the application of copyright is, the more affected developing countries are. The Internet provides researchers, students, and others from developing countries with a powerful tool for participating in global academic and scientific exchanges. A more restrictive copyright regime could have a negative impact on the development of human capacity in developing countries. Another aspect is the increasing digitisation of cultural and artistic crafts from developing countries. In the most paradoxical scenario, developing countries may end up having to pay for their cultural and artistic heritage when it is digitised, repackaged, and owned by foreign entertainment and media companies.

WIPO and WTO

Two main international regimes exist for IPR. WIPO manages the IPR regime based on the Berne and the Paris conventions. Another regime is run by the WTO and is based on TRIPS. The shift of international IPR coordination from WIPO to the WTO was carried out to strengthen rights protection, especially in the field of enforcement.

Some developing countries have been concerned by this development. Their concern is that the WTO's strict enforcement mechanisms could reduce the manoeuvring room of developing countries and the possibility of balancing development needs with the protection of international IPR. So far, the main focus of the WTO and TRIPS has been on various interpretations of IPR for pharmaceutical products. It is very likely that discussions will extend to IPR and the Internet.

www.igbook.info/copyright

Trademarks

A trademark is a symbol or a word(s) legally registered or established by use that represents a company or product. Trademarks are relevant to the Internet mainly because of the registration of domain names. In the early phase of Internet development, the registration of domain names was done on a first come, first served basis. This led to cybersquatting, the practice of registering names of companies and selling them later at a higher price.

This situation compelled the business sector to place the question of the protection of trademarks at the centre of the reform of Internet governance, leading to the establishment of ICANN in 1998. In the White Paper on the Management of Internet Names and Addresses, the US government called for the development and implementation of a mechanism for the protection of trademarks in the field of domain names.[39] Soon after its formation, ICANN introduced the UDRP.[40]

Trademark concerns came into sharper focus when the domain name space was extended by introducing new gTLDs such as '.doctor', '.lawyer', '.berlin', etc. One example of such a controversy is the application for the gTLD '.amazon'. The Internet company Amazon applied to register '.amazon', as the trademark holder for this name. Countries from the Amazon basin objected within ICANN's GAC, arguing that this name refers to a geographical area that is important for the region, and the company should not be allocated the gTLD it for its exclusive use. Based on GAC advice, the ICANN Board rejected the application in May 2014, but the decision was later contested by Amazon, through ICANN's Independent Review Process (IRP). As of October 2016, the case was still open, with the IRP on-going, and a hearing tentatively scheduled for February-March 2017.[41]

www.igbook.info/trademarks

Patents

A patent confers the patent owner the exclusive right to exclude others from making, using, or selling an invention. Traditionally, a patent protects a new process or product of a mainly technical or production nature. Only recently have patents been granted for software.

With the continuous evolution of Internet technologies, more and more companies are applying for patents (covering technologies in the field of VoIP, IoT, etc.). This is especially the case in the USA, where more patent registrations also result in more court cases among companies, involving huge amounts of money. As an example, in September 2016, in a case that began in 2010, a judge in the US state of Texas ordered Apple to pay $302.4 million to another US company, for infringing patents covering secure computer and mobile communications.[42]

Some patents have been granted for business processes, and some of these were controversial, such as British Telecom's request for licence fees for the patent on hypertext links, which it registered in the 1980s. In August 2002, the case was dismissed.[43] If British Telecom had won this case, Internet users would have had to pay a fee for each hypertext link created or used.

Granting patents to software is a rather complex issue in Europe and other regions. As the European Patent Office explains, 'under the European Patent Convention, a computer program claimed "as such" is not a patentable invention [...]. For a patent to be granted for a computer-implemented invention, a technical problem has to be solved in a novel and non-obvious manner'.[44]

Labour law

The Internet has changed the way we work. The notion of tele-working has gained relevance, and the number of temporary and short-term work has grown. The term 'permatemp' was coined for employees who are kept for long periods on regularly reviewed short-term contracts. This introduces a lower level of social protection of the workforce (Figure 18).

New labour models, such as on-demand labour and independent worker models, are a more recent development to business models shaped by Uber, Amazon, and other Internet companies. In the process, the new models have raised several questions. For example, are Uber drivers independent contractors or Uber employees? This has attracted different opinions across US states: authorities in California[45] and Oregon[46] consider drivers as Uber employees, while Florida[47] qualifies them as contractors.

Figure 18. Labour law

In the field of labour law, one important issue is the question of privacy in the workplace. Is an employer allowed to monitor employees' use of the Internet (such as the content of e-mail messages or website access)? Jurisprudence is gradually developing in this field.

While a 2007 decision of the European Court of Human Rights (ECHR) declared that the monitoring of an employee's use of e-mail or Internet at the place of work breached the employee's human right,[48] a 2016 decision by the same court ruled that employers may read private communications of employees made during office hours. The court's justification in Bărbulescu v Romania (January 2016) was that it is not unreasonable for an employer to want to verify that the employees are completing their professional tasks during working hours. However, the employer must provide prior notice of any monitoring activities. In Denmark, courts considered a case involving an employee's dismissal for sending private e-mails and accessing a sexually oriented chat website. The court ruled that dismissal was not lawful

since the employer did not have an Internet use policy in place banning the unofficial use of the Internet. The ECHR judgment in Bărbulescu v Romania also highlights the need for a policy: 'A comprehensive Internet usage policy in the workplace must be put in place, including specific rules on the use of email, instant messaging, social networks, blogging and web surfing. Although policy may be tailor-made to the needs of each corporation as a whole and each sector of the corporation infrastructure in particular, the rights and obligations of employees should be set out clearly, with transparent rules on how the Internet may be used, how monitoring is conducted, how data is secured, used and destroyed, and who has access to it.'[49]

An additional point of concern arising with the ever-growing use of social networking is the delimitation between private and working life. Recent cases[50] showed that employees' behaviour and comments on social networking sites may address various topics, from workplace and co-workers to employer's strategies and products, deemed as personal (and private) opinions, but which may considerably affect the image and reputation of companies and colleagues.

Labour law has traditionally been a national issue. However, globalisation in general and the Internet in particular have led to the internationalisation of labour issues. With an increasing number of individuals working for foreign entities and interacting with work teams on a global basis, an increasing need arises for appropriate international regulatory mechanisms. This aspect was recognised in the WSIS Declaration of Principles, which, in paragraph 47, calls for the respect of all relevant international norms in the field of the ICT labour market.[51]

www.igbook.info/labourlaw

Intermediaries

Intermediaries[52] play a vital role in ensuring Internet functionality. They include ISPs (which ensure the connection between end-users), as well as providers of services such as online hosting, search engines, and social media platforms.

Given their role in facilitating the transmission and availability of online content, intermediaries are increasingly called on to assist in the enforcement of legal rules in areas such as copyright infringement, spam, and the right to be forgotten. This has given rise to extensive discussions as to whether intermediaries are or should be held liable for the online content to which they facilitate access.

At national level, ISPs are often the most direct way for governments and law enforcement agencies to enforce legal rules online.

Hosts of online content and operators of search engines and social media platforms typically act as conduits for content, or bridges between content and Internet users. Although headquartered in one country (some having regional headquarters), their reach and user-base is likely to be global, and consequently, they are often exposed to jurisdiction in multiple countries.

Intermediary liability is often discussed at IGF meetings and in other forums. The OECD includes the role of intermediaries among its 14 principles for Internet policy-mak-

ing,[53] while the CoE has established a Committee of experts on Internet Intermediaries (MSI-NET), tasked with the preparation of a set of proposals on the roles and responsibilities of intermediaries. UNESCO has explored the mediating role Internet intermediaries play between authors of content and Internet users, as well as its impact on freedom of expression and associated fundamental rights such as privacy.[54]

The issues

Intermediary responsibility for copyright infringement

In general, legal frameworks dealing with intermediary responsibility include the principle that an Internet intermediary cannot be held responsible for hosting materials that breach copyrights if it is not aware of the violation. This is, for example, the approach taken by the DMCA and the EU directives,[55] which exempts the service provider from liability for the information transmitted or stored at the direction of the users.

The main difference between the various legal systems lies in the legal action taken after the intermediary becomes aware that the material it is hosting is in breach of copyright. US and EU law demand that the service providers act on a 'notice and take down' procedure.[56] Japanese law takes a more balanced approach, through the Notice-Notice-Take-Down procedure, which provides the user of the material with the right to complain about the request for removal. Both solutions provide some comfort to intermediaries, as they are safe from legal sanctions, but also potentially transforms them into content judges[57] and only partially solves the problem, since the contested content may be simply moved to another online location.

The approach of placing limited liability on intermediaries has been generally supported by jurisprudence. Some of the most important cases where ISPs were freed of responsibility for hosting materials in breach of copyright law are the Scientology Case (the Netherlands),[58] RIAA v Verizon (United States),[59] SOCAN v CAIP (Canada),[60] and Scarlet v SABAM (Belgium).[61] A more nuanced ruling issued by the CJEU in September 2016, in the case GS Media BV v Sanoma Media Netherlands BV and Others, says that operators of websites linking to materials that infringe copyright can be found guilty of copyright infringement, if the operators knew or could reasonably have known that the material constituted an infringement. According to the court, operators would be presumed to know about the infringements if the links are provided for 'the pursuit of financial gain'.[62]

Nevertheless, recent years have witnessed an increased pressure on intermediaries to handle copyright matters, since their position of gatekeepers between end-users and Internet content places them in the best position to control access. This argument was speculated in promoting legal provisions such as Hadopi Law[63] in France forcing ISPs to intervene in case of suspicions of copyright infringements.

The role of intermediaries in content policy

Under growing official pressure, ISPs, hosting services providers, and operators of search engines and social network platforms are gradually, albeit reluctantly, becoming involved with content policy (e.g. defamatory or fraudulent content). In doing so, they might have to follow two possible routes. The first is to enforce government regulation. The second, based on self-regulation, is for intermediaries to decide on what is appropriate content themselves. This runs the risk of privatising content control, with intermediaries taking over

governments' responsibilities, but carries the advantage of adopting flexible approaches to keep up with the fast pace of technology. This is especially relevant in the field of child online protection.

Courts of law are increasingly imposing rules on intermediaries. In 2013, the ECHR confirmed a ruling by the Estonian courts which found the news portal Delfi liable for offensive comments posted on its website.[64] In June 2015, the Grand Chamber of the ECHR confirmed the 2013 judgment: the Estonian courts' decision was justifiable and proportionate, as the comments were extreme and had been posted in reaction to an article published by Delfi on its professionally managed news portal run on a commercial basis.[65] (The judgment, however, does not concern other online spaces where third-party comments can be disseminated, such as an Internet discussion forum, a bulletin board, or a social media platform.)

The role of intermediaries in anti-spam policy

ISPs are commonly seen as the primary institutions involved with anti-spam initiatives. Usually, ISPs have their own initiatives for reducing spam, either through technical filtering or the introduction of anti-spam policy. An ITU report from 2006 suggested that ISPs should be liable for spam and proposed an anti-spam code of conduct, with two main provisions:

- An ISP must prohibit its users from spamming.
- An ISP must not peer with ISPs that do not accept a similar code of conduct.[66]

The problem of spam exposed ISPs to new difficulties. For instance, Verizon's anti-spam filtering led to a court case as it also blocked legitimate messages causing inconvenience for users who did not receive their legitimate e-mail.[67] Admittedly, self- and co-regulation approaches adopted by ISPs, together with international cooperation and the use of sophisticated filters, has minimised the policy relevance of spam.

www.igbook.info/intermediaries

Endnotes

1 Some of the first arguments for the real-law approach were provided by Judge Frank Easterbrook who is quoted as saying: 'Go home; cyberlaw does not exist.' In the article *Cyberspace and the Law of the Horse*, he argues that although horses were very important, there was never a Law of the Horse. Judge Easterbrook argues that there is a need to concentrate on the core legal instruments, such as contracts, responsibility, etc. Available at http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2147&context=journal_articles [accessed 24 October 2016]. Easterbrook's argument provoked several reactions, including one from Lawrence Lessig in *The Law of the Horse: What Cyberlaw Might Teach*. Available at http://cyber.law.harvard.edu/works/lessig/LNC_Q_D2.PDF [accessed 24 October 2016]. Further discussion of the real-law and cyberlaw approaches can also be found on The Oxford Comma blog: Shaping Internet Governance: Tensions Between 'Real' and 'Cyber' Laws. Available at http://wizardsqu1rrel.blogspot.com.mt/2014/01/shaping-internet-governance-tensions.html [accessed 24 October 2016].

2 United Nations (2013) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Available at http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf [accessed 29 October 2016].

3 United Nations General Assembly (2015) Resolution A/70/125. Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society. Available at http://workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf [accessed 27 October 2016].

4 United Nations General Assembly (2014) Resolution A/69/166. The right to privacy in the digital age. Available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166 [accessed 29 October 2016]. United Nations Human Rights Council. Resolution A/HRC/20/L.13. The promotion, protection and enjoyment of human rights on the Internet. Available at http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280 [accessed 29 October 2016].

5 NTIA (1988) Statement of Policy on the Management of Internet Names and Addresses. Available at https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses [accessed 24 October 2016].

6 For example, the new provision according to which the regulations would be applicable to 'those operating agencies, authorized or recognized by a Member State, to establish, operate and engage in international telecommunications services to the public' was seen as broadening the scope of the ITRs to include ISPs. Controversy also surrounded the introduction of provisions concerning network security and unsolicited electronic communications. As they are associated with the broader concept of cybersecurity (including in relation to spam in the context of emails), it was argued that it is difficult to interpret these provisions as being applicable only to traditional telecommunications (and not to the Internet). In addition to the different interpretations of such provisions, the telecommunication definition itself (unchanged as compared to the 1988 ITRs) is seen by some as also covering communications made via the Internet: 'any transmission, emission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical, or other electromagnetic systems'.

7 Ago R (1956) Science juridique et droit international. Receuil des Cours Academie de Droit International (RCADI), 1956-II, 855–954, La Haye

8 Vienna Convention on the Law of Treaties. Available at http://www.ilsa.org/jessup/jessup11/basicmats/VCLT.pdf [accessed 28 October 2016].

9 Brownlie I (1999) *Principles of Public International Law,* 5th Ed. Oxford: Oxford University Press, p. 513.

10 Salis RP (2001) A Summary of the American Bar Association's (ABA) Jurisdiction in Cyberspace Project: Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdic-

tion Issues Created by the Internet. Available at http://www.jstor.org/discover/10.2307/40687955?uid=3738216&uid=2&uid=4&sid=21103388060741 [accessed 28 October 2016].

[11] Among the most important resources in this field is the *Princeton Principles on Universal Jurisdiction* (2001). Available at http://www1.umn.edu/humanrts/instree/princeton.html [accessed 28 October 2016].

[12] Malanczuk P (1997) *Akehurst's Modern Introduction to International Law.* London: Routledge, p. 113.

[13] EDRI-gram (2006) French anti-hate groups win case against Yahoo! Available at http://edri.gn.apc.org/edrigram/number4.1/yahoocase [accessed 24 October 2016].

[14] CJEU (2011) Judgement of the Court in Joined Cases Cases C-509/09 and C-161/10: eDate Advertising GmbH v X, and Olivier Martinez, Robert Martinez v MGN Limited. Available at http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-509/09&td=ALL [accessed 29 October 2016].

[15] CJEU (2013) Judgement of the Court in Case C-170/12: Peter Pinckney v KDG Mediatech AG. Available at http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-170/12&td=ALL [accessed 29 October 2016].

[16] For an overview of cases involving extraterritorial jurisdiction related to Internet content, refer to Timofeeva YA (2005) Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis. *Connecticut Journal of International Law, 20*, 199. Available at http://ssrn.com/abstract=637961 [accessed 24 October 2016].

[17] One relatively similar case was the German Federal Court of Justice case against Fredrick Toben, a former German national with Australian nationality, who had posted on an Australian-based website, materials questioning the existence of the holocaust. Available at http://www.ihr.org/jhr/v18/v18n4p-2_Toben.html [accessed 24 October 2016].

[18] Commission Nationale de l'Informatique et des Libertés (2015) Right to delisting: Google informal appeal rejected. Available at https://www.cnil.fr/fr/node/15814 [accessed 11 October 2016].

[19] CJEU (2015) Judgement of the Court in Case C-362/14: Maximillian Schrems v Data Protection Commissioner. Available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2015 [accessed 21 October 2016].

[20] United States Court of Appeals for the Second Circuit (2016) Decision in the matter of a warrant to search a certain e-mail account controlled and maintained by Microsoft Corporation: Microsoft Corporation v USA. Available at http://www.ediscoverylaw.com/wp-content/uploads/2016/07/In-re-Matter-of-a-Warrant.pdf [accessed 24 October 2016].

[21] The court order, in French, can be found at http://www.cottineau.net/wp-content/uploads/2016/02/facebook-jugement-cour-appel-paris-12-fevrier-2016.pdf [accessed 12 October 2016].

[22] Yaron O (2016) Israeli judge approves $400 million class action against Facebook for violating privacy. *Haaretz*, 17 June. Available at http://www.haaretz.com/israel-news/business/1.725512 [accessed 12 October 2016].

[23] Example of controversial issues include: racist content, pornography, online gambling, tobacco advertising, and the sale of drugs.

[24] UNCITRAL (1958) The New York Convention. Available at http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/NYConvention.html [accessed 24 October 2016].

[25] UNCITRAL (1985) Model Law in International Commercial Arbitration. Available at http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/1985Model_arbitration.html [accessed 24 October 2016].

[26] WIPO (no date) Domain Name Dispute Resolution. Available at http://www.wipo.int/amc/en/domains/ [accessed 25 October 2016].

[27] European Commission (2016) Settling consumer disputes online. Available at http://ec.europa.eu/consumers/solving_consumer_disputes/docs/adr-odr.factsheet_web.pdf [accessed 25 October 2016].

[28] Google (2016) Transparency Report. European privacy requests for search removals. Available at https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en [accessed 29 October 2016].

[29] WIPO (no date) WIPO Copyright Treaty. Available at http://www.wipo.int/treaties/en/ip/wct/ [accessed 1 November 2016].

[30] Office of the United States Trade Representative (no date) The Trans-Pacific Partnership. Available at https://ustr.gov/tpp/ [accessed 1 November 2016].

[31] US Congress (1998) Digital Millennium Copyright Act. Available at http://www.copyright.gov/legislation/hr2281.pdf [accessed 1 November 2016].

[32] US Congress (2011) Stop Online Piracy Act. Available at https://www.congress.gov/bill/112th-congress/house-bill/3261 [accessed 24 October 2016].

[33] US Congress (2011) Protect IP Act. Available at https://www.congress.gov/bill/112th-congress/senate-bill/968 [accessed 24 October 2016].

[34] Anti-Counterfeiting Trade Agreement (2011) Available at http://trade.ec.europa.eu/doclib/docs/2011/may/tradoc_147937.pdf [accessed 24 October 2016].

[35] La Quadrature du Net, a civil rights advocacy group, has followed closely the developments on Hadopi law and has instrumented a comprehensive file on ACTA. Available at http://www.laquadrature.net/en/ACTA [accessed 25 October 2016]. On protests against US bills, refer to Vijayan J (2012) Protests against SOPA, PIPA go viral. *Computerworld*, 18 January. Available at http://www.computerworld.com.au/article/412655/protests_against_sopa_pipa_go_viral/ [accessed 25 October 2016].

[36] Sorkin AR (2003) Software bullet is sought to kill musical piracy. *New York Times*, 4 May. Available at http://www.nytimes.com/2003/05/04/business/04MUSI.html [accessed 25 October 2016].

[37] US Patents and Trademark Office (no date) Intellectual Property and the National Information Infrastructure. Available at http://www.uspto.gov/web/offices/com/doc/ipnii/ [accessed 25 October 2016].

[38] For an explanation of the concept of fair use and examples, refer to The UK Copyright Service (no date) Copyright Law fact sheet P-09: Understanding Fair Use. Available at http://www.copyrightservice.co.uk/copyright/p09_fair_use [accessed 25 October 2016].

[39] NTIA (1998) Statement of Policy on the Management of Internet Names and Addresses. Available at https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses [accessed 1 November 2016].

[40] For a comprehensive survey of the main issues involving UDRP, please consult WIPO (2011) WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Second Edition (WIPO Overview 2.0) Available at http://www.wipo.int/amc/en/domains/search/overview2.0/ [accessed 25 October 2016].

[41] For more details about the .amazon case, consult Murphy K (2016) Amazon files appeal on rejected .amazon domain. *The Register,* 3 March 2016. Available at http://domainincite.com/20105-amazon-files-appeal-on-rejected-amazon-domain [accessed 25 October 2016]. For details on the IRP initiated by Amazon, consult ICANN (no date) Amazon EU S.à.r.l. v ICANN (.AMAZON). Available at https://www.icann.org/resources/pages/irp-amazon-v-icann-2016-03-04-en [accessed 25 October 2016].

[42] Decker S and Robertson D (2016) VirnetX Wins $302.4 Million Trial Against Apple in Texas. *Bloomberg*, 30 September. Available at https://www.bloomberg.com/news/articles/2016-10-01/virnetx-wins-302-4-million-trial-against-apple-in-texas [accessed 25 October 2016].

[43] Loney M (2002) Hyperlink patent case fails to click. *CNET*, 23 August. Available at https://www.cnet.com/news/hyperlink-patent-case-fails-to-click/ [accessed 25 October 2016].

[44] European Patent Office (no date) Patents for software? European law and practice. Available at https://www.epo.org/news-issues/issues/software.html [accessed 25 October 2016].

[45] Somerville H (2015) Former Uber driver was an employee, rules California department. *Reuters*, 9 September. Available at http://www.reuters.com/article/uber-tech-california-ruling-idUSL1N11F1KT20150910 [accessed 29 October 2016].

[46] Bureau of Labour and Industries of the State of Oregon (2016) Advisory opinion of the Commissioner of the Bureau of Labor and Industries regarding the employment status of Uber drivers. Available at http://media.oregonlive.com/commuting/other/101415%20Advisory%20Opinion%20on%20the%20Employment%20Status%20of%20Uber%20Drivers.pdf [accessed 29 October 2016].

[47] Ampel C (2015) Florida: Uber drivers are contractors, not employees. *Daily Business Review*, 4 December. Available at http://www.dailybusinessreview.com/id=1202743938454/Florida-Uber-Drivers-Are-Contractors-Not-Employees?slreturn=20160929162026 [accessed 29 October 2016].

[48] ECHR (2007) Judgement of the Court in the Case Copland v the United Kingdom (Application no. 62617/00). Available at http://hudoc.echr.coe.int/eng?i=001-79996 [accessed 29 October 2016].

[49] ECHR (2016) Judgement of the Court in the Case Bărbulescu v Romania (Application no. 61496/08). Available at http://hudoc.echr.coe.int/eng?i=001-159906 [accessed 29 October 2016].

[50] Refer to the following articles for example: Holding R *(2011)* Can You Be Fired for Bad-Mouthing Your Boss on Facebook? *Time U.S.*, 4 March. Available at http://www.time.com/time/nation/article/0,8599,2055927,00.html [accessed 25 October 2016]. Broughton A *et al.* (2009) Workplaces and Social Networking. The Implications for Employment Relations. Available at http://www.acas.org.uk/media/pdf/d/6/1111_Workplaces_and_Social_Networking.pdf [accessed 25 October 2016].

[51] WSIS (2003) Declaration of Principles. Building the Information Society: a global challenge in the new Millennium. Available at http://www.itu.int/net/wsis/docs/geneva/official/dop.html [accessed 29 October 2016].

[52] The OECD's working definition of intermediaries attempts to identify the various categories of service providers that fall under the notion of intermediaries: 'Internet intermediaries bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties.' In: OECD (2011) The Role of Internet Intermediaries in Advancing Public Policy Objectives. Available at http://www.oecd.org/sti/ieconomy/theroleofinternetintermediariesinadvancingpublicpolicyobjectives.htm [accessed 29 October 2016].

[53] OECD (2011) OECD Council Recommendation on Principles for Internet Policy Making. Available at http://www.oecd.org/internet/ieconomy/49258588.pdf [accessed 10 October 2016].

[54] MacKinnon R *et al.* (2014) Fostering Freedom Online. The Role of Internet Intermediaries. UNESCO/Internet Society. Available at http://unesdoc.unesco.org/images/0023/002311/231162e.pdf [accessed 10 October 2016].

[55] European Union (2000) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Available at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32000L0031 [accessed 25 October 2016]. European Union (2001) Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1477400249287&uri=CELEX:32001L0029 [accessed 25 October 2016].

[56] The 'Notice and Take Down' procedure refers to the obligation of service providers to remove content from websites under their administration if they receive a notification or complaint regarding the legality of that specific content.

[57] For fear of facing potential legal sanctions, some ISPs prefer to restrict access to indicated content even when no infringement has taken place. For details, please consult the following case studies: For Europe (the Netherlands): Nas S (2004) *The Multatuli Project ISP Notice & Take Down,* Bits of Freedom. Available at https://www-old.bof.nl/docs/researchpaperSANE.pdf [accessed 28 October 2016]. For the USA: Urban J and Quilter L (2006) *Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act.* Available at http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1500&context=facpubs [accessed 28 October 2016].

[58] 'The Court of Appeal of The Hague ruled against the Church of Scientology in its copyright infringement suit against a Dutch writer and her ISP, XS4ALL. The writer, formerly a practicing Scientologist, posted to a website parts of confidential church documents, and the church sued under the Dutch Copyright Act of 1912. In 1999, the District Court ruled in favour of the defendants, citing freedom of speech concerns. However, that court also ruled that ISPs should be held liable for posted materials that might violate existing copyrights. The Court of Appeal affirmed the first ruling, but reversed the second, holding that ISPs were not liable for posted materials.' For more informa-

tion, consult Gelman L (2003) Church of Scientology Loses Copyright Infringement Case in Dutch Court. Available at http://cyberlaw.stanford.edu/packets001638.shtml [accessed 25 October 2016].

[59] For more information on this case, refer to Electronic Privacy Information Center (2004) RIAA *v* Verizon. Available at http://epic.org/privacy/copyright/verizon/ [accessed 25 October 2016].

[60] The Supreme Court of Canada rejected the argument of the Society of Composers, Authors and Music Publishers of Canada that Canadian ISPs should pay royalties because some of their customers download copyrighted works (SOCAN *vs* CAIP). More information available at http://www.canlii.org/en/ca/scc/doc/2004/2004scc45/2004scc45.html [accessed 25 October 2016].

[61] 'SABAM (the Belgian collective society – *Société belge des auteurs, compositeurs et* éditeurs) wanted the ISP Scarlet to install a generalised filtering system for all incoming and outgoing electronic communications passing through its services and to block potentially unlawful communications. In First Instance, while refusing the liability of the ISP, the Brussels Court concluded that the SABAM's claim was legitimate and that a filtering system had to be deployed. Scarlet appealed and the case was referred to the Court of Justice of the European Union. In its decision, the Court of Justice ruled that a filtering and blocking system for all its customers for an unlimited period, *in abstracto* and as preventive measure, violates fundamental rights, more particularly the right to privacy, freedom of communication and freedom of information. In addition, it breaches the freedom of ISPs to conduct business.' For more information, consult CJEU (2011) Judgement of the Court in Case C-70/10: Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). Available at http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-70/10&td=ALL [accessed 25 October 2016].

[62] CJEU (2016) Judgement of the Court in Case C-160/15: GS Media BV v Sanoma Media Netherlands BV, Playboy Enterprises International Inc., Britt Geertruida Dekker. Available at http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-160/15&td=ALL [accessed 25 October 2016].

[63] In 2013, part of the Hadopi Law was revoked as the penalty of suspending Internet access to the infringer was deemed disproportionate.

[64] ECHR (2013) Judgement of the Court (First Section) in the Case Delfi AS v Estonia (Application no. 64569/09). Available at http://hudoc.echr.coe.int/eng?i=001-126635 [accessed 29 October 2016].

[65] ECHR (2015) Judgement of the Court (Grand Chamber) in the Case Delfi AS v Estonia (Application no. 64569/09). Available at http://hudoc.echr.coe.int/eng?i=001-155105 [accessed 29 October 2016].

[66] Palfrey J (2006) Stemming the International Tide of Spam. In: ITU (2006) Trends in Telecommunication reforms 2006. Available at http://www.itu.int/ITU-D/treg/publications/Chap%207_Trends_2006_E.pdf [accessed 29 October 2016].

[67] Shannon V (2006) The end user: Junk payout in spam case – Technology – International Herald Tribune. *The New York Times,* 26 April. Available at http://www.nytimes.com/2006/04/12/technology/12iht-PTEND13.1523942.html [accessed 28 October 2016].

Section 5

THE ECONOMIC BASKET

The economic basket

We know how to route packets.
What we don't know how to do is route dollars.

David Clark – Chief Internet Protocol Architect

This quote from David Clark reflects the spirit of the early Internet community, where the non-profit Internet project was supported mainly by US research grants. But, in the 1990s and early 2000s, new business models for 'routing dollars' started to emerge in Silicon Valley, centered mainly on income from online advertising.

Economic issues in Internet governance are mainly related to this evolution of the Internet from a non-profit project to one of the main business facilities and engines of economic growth in modern society. The flow of ideas and creativity facilitated by the Internet since its early days has been complemented by and, increasingly, finds itself in competition with the flow of money. More money has introduced more tangible business and policy interests. The creative 'blue sky is the limit' approach of the early Internet community has begun to converge with the 'bottom line' logic of the business community. This interplay between high creativity and robust economic support triggered a real economic revolution geographically centred on the Bay Area in California.

Digital policy both affects and is affected by economic developments and the flow of money.[1] An enabling digital policy is essential for economic growth. One of the reasons for fast digital growth in Silicon Valley, for example, has been the functional regulatory system; this system has protected Internet companies' intellectual property and encouraged investment, and much more besides. The relevance of 'analogue' supplements (an enabling policy environment) for the digital economy was analysed by the World Bank in its World Development Report 2016: Digital Dividends.[2]

Digital policy is also affected by Internet companies. They have developed powerful lobbying machines, which are particularly active in the major digital policy centres such as Washington D.C., Brussels, and Geneva.

Our analysis of Internet-related economic issues focuses on four main domains where monetary and non-monetary business transactions occur:

- E-commerce: traditional commercial activities conducted via the Internet.
- Internet DATA economy: the new advertising-based business model.
- Internet ACCESS economy: the telecommunications industry in the Internet era.
- E-banking, e-money, and virtual currencies.

In addition, we look at two other policy issues of economic relevance: consumer protection and taxation.

E-commerce

E-commerce has been one of the main engines driving the growth of the Internet over the past 15 years. The importance of e-commerce is illustrated by the title of the document that initiated the reform of Internet governance and paved the way towards the creation of ICANN: the 1997 Framework for Global Electronic Commerce,[3] which states that 'the private sector should lead' the Internet governance process and that the main function of this governance will be to 'enforce a predictable, minimalist, consistent, and simple legal environment for commerce'.

Nowadays, the impact of e-commerce on individuals and businesses is far-reaching. E-commerce has brought about numerous advantages for consumers, such as the convenience of online shopping, the flexibility and ease-of-access to different markets, and the less time-consuming online banking and e-payment operations. From a business perspective, e-commerce has influenced supply chain management, and has enabled companies to reach their customers more easily through online advertising and marketing and other avenues. However, businesses face tougher competition and added complexities when serving an online market.

Definition

The choice of a definition for e-commerce has many practical and legal implications. Specific rules are applied depending on whether a particular transaction is classified as e-commerce, such as those regulating taxation and customs.

For the US government, the key element distinguishing traditional commerce from e-commerce is the online commitment to selling goods or services. This means that any commercial deal concluded online should be considered an e-commerce transaction, even if the realisation of the deal involves physical delivery. For example, purchasing a book via Amazon.com is considered an e-commerce transaction even though the book is usually delivered via traditional mail. The WTO defines e-commerce more precisely as: 'the production, distribution, marketing, sale, or delivery of goods and services by electronic means'.[4] The EU approach to e-commerce deals with 'information society services' that cover 'any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service'.[5]

E-commerce takes several forms:

- Business-to-consumer (B2C) – the most familiar type of e-commerce (e.g. Amazon.com).
- Business-to-business (B2B) – economically the most intensive, representing more than twice the size of the B2C market.[6]
- Business-to-government (B2G) – highly important in the area of public procurement policy.
- Consumer-to-consumer (C2C) – for example, eBay auctions.

Many countries are developing regulatory frameworks for e-commerce. Laws have been adopted in various fields of relevance, such as digital signatures, online dispute resolution, cybercrime, consumer protection, and taxation of electronic services. At international level, an increasing number of initiatives and regimes are related to e-commerce.

The WTO and e-commerce

As the key policy player in modern global trade, the WTO has established a system of agreements regulating international trade. The major treaties are the General Agreement on Tariffs and Trade (GATT)[7] dealing with the trade in goods, the General Agreement on Trade in Services (GATS),[8] and TRIPS.[9] Within this framework, the WTO regulates many relevant e-commerce issues, including telecommunications liberalisation, IPR, and some aspects of ICT development. E-commerce figures in the following WTO activities and initiatives:

- A temporary moratorium on custom duties on electronic transmissions, introduced in 1998, has rendered all e-transmissions free of custom duties among WTO member states.[10]

- The WTO Work Programme on Electronic Commerce, established in 1998, sets out responsibilities for WTO bodies in e-commerce-related areas.[11]

- A dispute resolution mechanism which addresses, among others, cases involving electronic transactions. (One example is the USA/Antigua Online Gambling case, where e-commerce was particularly relevant.[12])

Although e-commerce has been on the WTO's diplomatic back-burner, various initiatives have arisen and several key issues have been identified, including the ones discussed next.

Should e-commerce transactions be categorised under services (regulated by GATS) or goods (regulated by GATT)?

Many e-commerce transactions have a dual nature. In the early digital days, the main dilemma was whether music should be categorised as a good or a service, depending on whether it is delivered on a CD (tangible) or via the Internet (intangible)? Ultimately, the same song could have different trade status (and be subject to different customs and taxes) depending on the medium of delivery. The question of categorisation emerges also in the context of mixed transactions involving intangible elements (online conclusion of contract, distribution of software) and tangible ones (physical delivery of a printer or other digital devices). This type of transaction will become even more prominent with advancements in the field of IoT. The issue of categorisation has considerable implications because of the different regulatory mechanisms for goods and services.

What should be the connection between TRIPS and the protection of IPR on the Internet?

Since the WTO's TRIPS agreement provides much stronger enforcement mechanisms for IPR than the WIPO treaties, developed countries have been trying to extend TRIPS coverage to e-commerce and to the Internet through using two approaches. First, citing the principle of technological neutrality, they argue that TRIPS, like other WTO rules, should be extended to any telecommunications medium, including the Internet. Second, some

developed countries have requested the closer integration of WIPO's 'digital treaties' into the TRIPS system. Both issues remain open and are likely to become increasingly important in future WTO negotiations. The lack of global e-commerce arrangements will be partially compensated by some specific initiatives (e.g. regarding contracts and signatures) and various regional agreements, mainly in the EU and the Asia-Pacific region.

WTO's future role in e-commerce

There are ongoing discussions on whether the WTO should play an increasing role in e-commerce. During the WTO Public Forum in September 2016, it was argued that the organisation could more strongly incorporate e-commerce and the overall digital economy in its agenda.[13] However, member states do not seem to agree on the matter. Some show willingness to focus more of their attention on e-commerce, and consider multilateral frameworks in this field, while others are of the view that there are other priorities the WTO should be focusing on (such as access to infrastructure and digital skills) before discussing regulatory frameworks.[14]

E-commerce and other digital policy issues

Making a clear distinction between e-commerce and other Internet governance issues is increasingly challenging. For example, the trade dimension of the data economy is inevitably affected by human rights regulations on privacy and freedom of information (issues tackled, for example, within the UNHRC), standards for data transactions (developed by ISO, IETF, ITU), cybersecurity – where data play an increasingly important role in the fight against terrorism and crime (UN GGE, UNODC). While the WTO cannot (and should not) deal with the full complexity of digital policy beyond trade, the organisation has to develop mechanisms to synchronise its work on e-commerce with the work of other international bodies, which will inevitably impact the WTO's regulations on e-commerce.

Other global e-commerce initiatives

There are several international organisations that deal with e-commerce-related issues. UNCITRAL has done significant work in this area. In 1992, UNCITRAL formed a Working Group on Electronic Data Interchange (which later became the Working Group on Electronic Commerce), whose work led, among others, to the adoption of the UNCITRAL Model Law on Electronic Commerce[15] and the United Nations Convention on the Use of Electronic Communications in International Contracts.[16] The Model Law has been one of the most successful and widely supported international initiatives in the field; it focuses on mechanisms for the integration of e-commerce with traditional commercial law (e.g. recognising the validity of electronic documents). The Model Law has been used as the basis for e-commerce regulation in many countries.

Another initiative in the field of e-commerce is the Electronic Business XML (ebXML) Initiative, launched by the UN Centre for Trade Facilitation and Electronic Business (CEFACT) and the Organization for the Advancement of Structured Information Standards (OASIS). The aim of the initiative is to develop relevant and open technical specifications in support of domestic and international electronic business exchanges.[17] While new specifications are being developed, the previous set – the Electronic Data Interchange (EDI) – is still widely deployed. It remains to be seen if and how they will be adjusted to cope with new trends and technological developments.

UNCTAD is particularly active in research and capacity-building, focusing on the relevance of e-commerce to development. Every year it monitors the evolution of the information economy and publishes the Information Economy Report, which assesses the role of new technologies in trade and development.[18] In 2016, UNCTAD launched the eTrade for All Initiative, a multistakeholder initiative aimed at improving the ability of developing countries to use and benefit from e-commerce.[19]

The OECD's activities touch on various aspects related to e-commerce, including consumer protection and digital signatures. Its involvement in e-commerce issues started with the 1998 Action Plan for Electronic Commerce, structured around four main issues: building trust for users and consumers, establishing ground rules for the digital marketplace, enhancing the information infrastructure for electronic commerce, and maximising its benefits.[20] Such issues have since been tackled in OECD recommendations and guidelines.

The G20 has also paid increased attention to e-commerce-related issues in recent years. At the G20 Leaders' Summit in Hangzhou, China (September 2016), e-commerce cooperation was highlighted as one of the priorities for G20 members.[21] The leaders also took note of an initiative to create an Electronic World Trade Platform, mainly aimed at assisting small and medium-sized enterprises (SMEs) to engage with the global e-commerce market.

In the business sector, one of the most active international organisations is the International Chamber of Commerce (ICC), which produces a wide range of recommendations and analyses in the field of e-commerce.

Another initiative that is worthwhile mentioning is the UN Global Compact. Although not specifically aimed at tackling e-commerce-related issues, the initiative is oriented towards creating stronger connections between businesses and human rights, and supporting companies to do business responsibly, by aligning their strategies and operations with universal principles on human rights. Since aspects related to the protection of human rights in the digital environment are increasingly influencing the way in which Internet companies conduct their businesses, this initiative is expected to have a significant impact on the Internet industry, including in the area of e-commerce.

Regional initiatives

The EU developed its first e-commerce strategy at the so-called Dot Com Summit of EU leaders in Lisbon (March 2000). Although it embraced a private and market-centred approach to e-commerce, the EU also introduced a few corrective measures aimed at protecting public and social interests (the promotion of universal access, a competition policy involving consideration of the public interest, and a restriction in the distribution of harmful content). Later on, in 2015, the Digital Single Market Strategy was adopted. It has a strong focus on e-commerce, with its objectives to facilitate better online access to digital goods and services, and strengthen the digital economy as a driver for growth.

The EU also has an E-commerce Directive (aimed at introducing a uniform and comprehensive legal framework for electronic commerce across EU member states), as well as a set of other legal instruments dealing with electronic signatures, data protection, and electronic financial transactions.

In the Asia-Pacific region, the focal point of e-commerce cooperation is APEC. One of the first APEC e-commerce-related programmes was the 1998 APEC Blueprint for Action on

Electronic Commerce, which aimed to consolidate and reinforce the various APEC initiatives in this area. To implement this plan, an E-Commerce Steering Group was established to address various e-commerce issues, including consumer protection, data protection, spam, and cybersecurity. The most prominent initiative is APEC's Paperless Trading Individual Action Plan,[22] which aims to create paperless systems in cross-border trade.

Within ASEAN, a Working Group on E-commerce and ICT Trade Facilitations was established, with the aim of contributing to the development of e-commerce regulatory and legislative frameworks that create trust and confidence for consumers. In this regard, the group has initiated the E-commerce Legal Infrastructure Project, which aims to formulate guidelines for an e-commerce legal infrastructure, and facilitate the development and growth of trusted e-commerce and e-business within and among ASEAN countries.

The Common Market for Eastern and Southern Africa (COMESA) is also undertaking work in the area of e-commerce. The COMESA Strategy outlines the organisation's commitment to actively promote e-commerce to enhance the digital integration of the common market. In 2010, the COMESA Council adopted a Model Law on Electronic Transactions, which contains provisions on electronic signatures, e-commerce, consumer protection, unsolicited commercial communications, and online dispute resolution.[23]

Plurilateral initiatives

Plurilateral initiatives bring together countries from different regions interested in the same issues. The plurilateral approach is increasingly used in the WTO context. Several trans-regional trade agreements have been negotiated lately, and they are likely to have a significant impact on digital policy. Two of the most visible agreements are the Trans-Pacific Partnership (TPP), signed in February 2016, and the Transatlantic Trade and Investment Partnership (TTIP), still under negotiation as of October 2016. These trade agreements would affect not only e-commerce, but also data regulation and dispute resolution in the Internet matters.

www.igbook.info/ecommerce

Internet DATA economy

The new business model (Figure 19) of the Internet industry, developed mainly by companies based in Silicon Valley, started to emerge in the late 1990s and took full shape in the 2010s. The growth of the Internet in the 1990s could not be sustained on public funding, as it had been in the past; it required a more robust business model. A few attempts to charge for access to Internet services and content failed. The new Internet business model does not charge users for the use of Internet services; it generates income from sophisticated advertising.

In this new business model, user data is the core economic resource. When searching for information and interacting on the Internet, users give away significant amounts of data, including personal data and the information they generate - their 'electronic footprint'. Internet companies collect and analyse this data to extract bits of information about user preferences, tastes, and habits. They also mine the data to extract information about a group; for instance, the behaviour of teenagers in a particular city or region. Internet

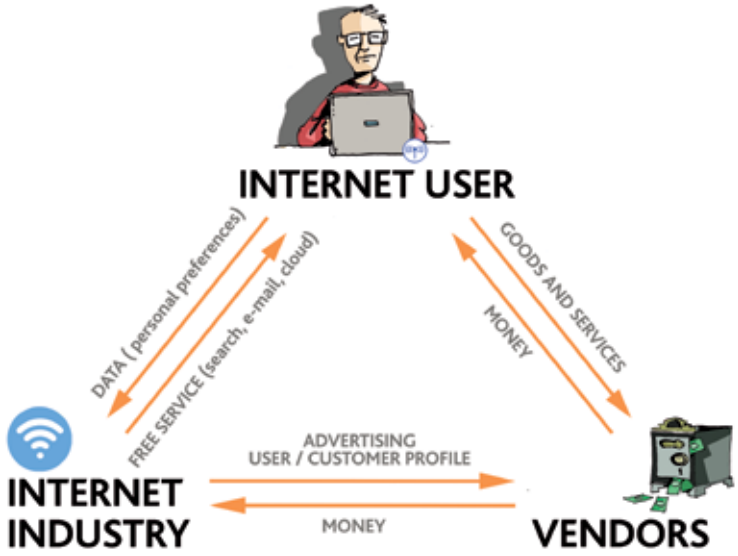

Figure 19. Internet business model

companies can predict with high certainty what a person with a certain profile is going to buy or do. This valuable block of data about Internet users has different commercial uses, but it mainly serves vendors, who use it for their marketing activities.

The issues

Protection of users and transparency

Formally speaking, by clicking 'I agree' to usually long and fine-print contracts or terms of service, users accept the conditions set by the service provider. The question remains whether users are making informed decisions, especially in view of the potential use of their data for commercial purposes. It is very likely that – in many cases – users accept the 'deal' of exchanging their data for valuable Internet services without serious consideration. The more transparent and easier to comprehend Internet arrangements are, the more beneficial it is, not only for users but also for Internet companies who can ensure a more sustainable business model, based on informed choices of Internet users.

Risk of abuse of dominant market positions

The Internet industry is prone to the establishment of market monopolies. As an example, in August 2016, Google's share of the search engine market was at 70% for desktop searches, and at more than 90% for mobile/tablet searches.[24]

When companies have monopolistic (or dominant) market positions, they sometimes tend to abuse such positions and introduce barriers that prevent or make it difficult for new companies to enter the market. To address such issues, relevant national and/or regional authorities need to have efficient and effective monitoring mechanisms at their disposal, as well as the ability to develop and enforce adequate competition and antitrust policies and legislation. Although such policies and legislation are country or region specific, they can be used to efficiently address the anti-competitive behaviour of global Internet companies

operating at local or regional level. The EU, for example, due to its advanced market regulations in this area, has undertaken several initiatives aimed at preventing or addressing unlawful practices, and forcing Internet companies to follow regulations. In recent years, the European Commission has become very active in monitoring competition on the EU digital market. As a consequence, it has initiated several actions against Internet companies' alleged abuse of dominant market positions. Google has been the target of some of these actions, which focused, among others, on the company's advertising-related practices.

Internet ACCESS economy

Internet users and companies pay ISPs for Internet-access-related services. Typically, ISPs have to cover the following expenses from the fees collected:

- Cost of telecommunications expenses and Internet bandwidth to the next major Internet hub.
- Cost of IP addresses obtained from RIRs or local LIRs. Each device accessing the Internet needs an IP address.
- Cost of acquiring, installing, and maintaining equipment and software (Figure 20).

Increasingly, the Internet access business is complicated by government regulatory requirements in areas such as data-retention. More regulation leads to more expenses, which are either passed to Internet users through subscription fees, or buffered by reduced profit for the ISPs.

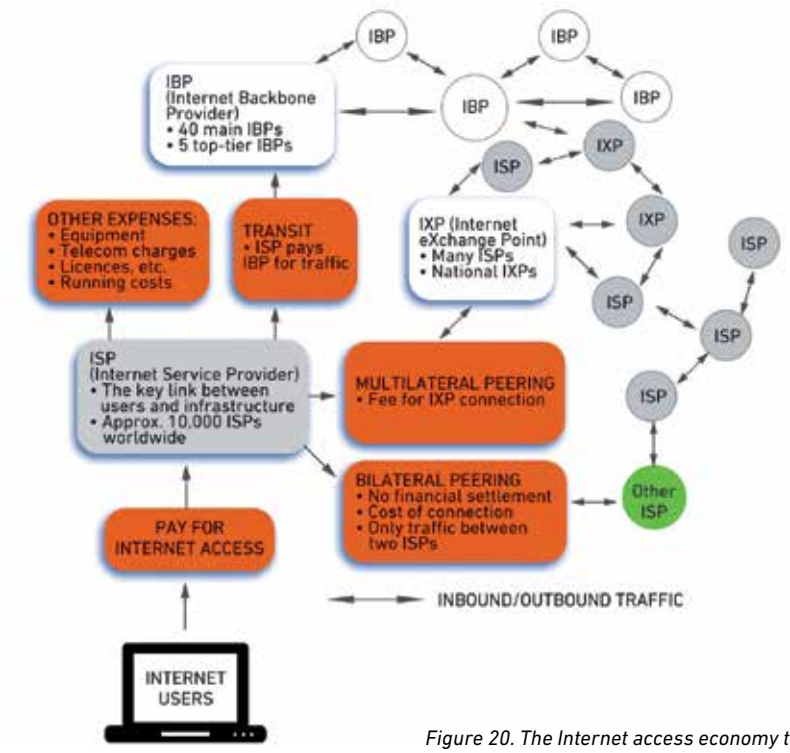

Figure 20. The Internet access economy traffic flow

The issues

Redistribution of revenue between telecommunications and Internet companies

Telecommunications operators have raised the question of redistribution of the revenue generated by the Internet. They are trying to increase their share of the 'revenue pie' generated by the Internet boom. So far, the main business beneficiaries of the Internet boom are Internet content companies due to their innovative business model based on online advertising. Telecommunications companies argue that they should also benefit because *they* facilitate access to Internet content through *their* telecommunications infrastructure.

The telecommunications industry usually justifies requests for a higher income from Internet-generated revenue by the need to invest in upgrading the telecommunications infrastructure. Content companies, on the other hand, argue that access providers already charge end-users for Internet access, and that the main reason for their alleged lower incomes is their obsolete business model ('all-you-can-eat' charges such as flat rates). European telecommunications operators, through ETNO, raised controversy during preparations for WCIT-12 in Dubai, when they proposed that content providers (e.g. Facebook, Google) pay for access to their services. The proposal did not gain support at that time, but it is likely to remain an open issue in future Internet governance negotiations.

This discussion on the redistribution of Internet revenue strongly underpins the net neutrality debate – for example, should all Internet traffic be treated equally, or should it be segregated into different tiers, depending on the quality of services, payment, and reliability (e.g. a range of options from VIP Internet to an Internet for the poor).

Flat rate vs pay per package

The discussion on Internet flat rates is often framed in terms of striking a proper and optimal balance between three aspects: technical efficiency, economic efficiency, and social effects.[25] Some authors highlight the challenges of replacing the existing, simple, flat-rate pricing structure with a more complex one, such as accounting based on the traffic of packets.[26] Regarding practical changes, some believe that changing the current Internet rate policies could open a Pandora's box, by triggering more problems than solutions.

Sharing telecommunications revenue with developing countries

Many developing countries have raised questions about the equity of the economic conditions of the Internet economy. Compared to the traditional telephony system, where the price of each international call is shared between two countries, the Internet model puts the entire burden on one side: users from developing countries may have to finance connection to Internet backbones located mainly in developed countries. As a result, paradoxically, small and poor countries may end up subsidising the Internet in developed countries.

The problem of financial settlement is particularly relevant for the poorest countries, which rely on income from international telecommunications as an important budgetary source. The situation has been further complicated with the introduction of VoIP – Internet telephony – which shifts telephone traffic from national telecommunications operators to the Internet.

Developing countries have raised the question of fairer Internet access business models in multiple contexts, including during WSIS, within ITU working groups, and at WCIT-12.

Emerging trends: Internet of Things, artificial intelligence, sharing economy

The IoT is an emerging trend which is having a major impact on the Internet economy. The integration of the IoT into business models reduces costs and increases efficiency. Many new businesses are now utilising 'smart buildings' to optimise energy costs and preserve the environment. The application of ICT solutions into business processes provides businesses with a competitive advantage, which helps them develop faster than in traditional surroundings. Businesses are therefore demanding new, tailor-made and innovative approaches from the IT industry, which is contributing significantly to the general economic welfare.

Advances in the field of AI are also expected to have significant economic effects. On the one side, the new wave of automation brought by AI is likely to generate considerable productivity growth. On the other hand, concerns have been raised regarding the impact that this automation could have on jobs and employment.

The latest model in the Internet economy is the so-called sharing economy, which has catapulted new players – such as Uber and Airbnb – into the global market. Such businesses have taken full advantage of the opportunities offered by the Internet economy, through integrating digital solutions into their business processes, thus leveraging reduced business costs, and through more direct access to consumers. At the same time, such models have found opposition from traditional businesses such as taxi and hotel services. There is ongoing controversy as to whether there is a need for specific regulations for the sharing economy (i.e., to cover issues such as liability, consumer protection, taxation, etc.), and even as to whether governments should ban services falling within this category. The EU has, for now, chosen a 'wait and see' approach. The European Commission published, in June 2016, a Communication on a European Agenda for the collaborative economy, aimed at providing member states with guidance on ways in which existing EU legislation should be applied to the collaborative economy. The Commission also suggested that absolute bans of sharing economy activities should only constitute a measure of last resort.[27]

A by-product of e-commerce is the emerging freelance market. On the one hand, this has given rise to a vibrant start-up community of freelancers and has contributed to strengthening SMEs and to reducing unemployment. On the other, it requires a new approach to labour, not least due to the treatment of income arising from online freelance work.

Another area that has significantly contributed to the Internet economy – and at the same time raised numerous debates – is e-gambling. Different regulatory approaches have been applied to e-gambling, due to its unique characteristics. The EU, for example, leaves it up to member states to regulate. The sensitivity of this area and its interrelation with public policy, morals, the protection of minors, and cybersecurity criminal matters made an argument that the regulation of e-gambling is more suitable to be conducted on national level according to each country's political and social background.

www.igbook.info/othereconomic

E-banking, e-money, and virtual currencies

Digital cash is a threat to every government on the planet that wants to manage its currency.

David Saxton, co-founder of Net1[28]

E-banking

E-banking involves the use of the Internet to conduct conventional banking operations, such as card payments or fund transfers. The novelty is only in the medium; the banking service remains essentially the same. E-banking provides advantages to customers by offering online access and paperless options, and by reducing the costs of transactions. For example, it is estimated that customer transactions which cost US$ 4 in traditional banking cost only US$ 0.17 in e-banking.[29]

E-money

Electronic money or e-money is the money balance recorded electronically on a stored-value card or remotely on a server. The Bank for International Settlements (BIS) defines e-money as 'stored value or prepaid payment mechanisms for executing payments via point-of-sale terminals, direct transfers between two devices, or over open computer networks such as the Internet'.[30] E-money is anchored in the existing banking and monetary system (financial legal tender supervised by national banks). It is usually associated with so-called smart cards issued by companies such as Mondex and Visa Cash.

Digital currency, virtual currency, and cryptocurrency

Unlike traditional e-money that represents fiat currency (such as EUR and USD) without changing its value, digital currency is not equivalent to any fiat currency (and is not part of a national financial system, and therefore is not regulated by state authorities).

Digital currencies can either be centralised or decentralised. In a centralised model, operations such as the issuance of the currency, and the mechanisms to implement and enforce rules on the use and circulation of the currency are managed by a central party. In a decentralised model, such operations are managed by various parties across the network.

Both virtual currencies and cryptocurrencies are types of digital currencies. While virtual currencies are based on a centralised model, cryptocurrencies (digital currencies that use cryptography for security, making them difficult to counterfeit) can be either centralised or decentralised. Bitcoin is one example of decentralised cryptocurrency.[31]

In 2012, the European Central Bank defined virtual money (virtual currencies) as a 'type of unregulated, digital money which is issued and usually controlled by its developers, and

used and accepted among the members of a specific virtual community'.[32] In 2014, the European Banking Authority defined virtual currency as 'a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically'.[33]

Cryptocurrencies are set to take the online world by storm, as their popularity and use increases. Large companies like Apple, Dell, and PayPal have already indicated their plans to integrate cryptocurrencies as a payment method, and more are likely to follow.

In recent years, Bitcoin has emerged as one of the most popular cryptocurrencies, and the number of services that allow the use of Bitcoin has increased drastically.

Bitcoin

The use of Bitcoin is based on blockchain technology, meaning that there is a central ledger of all transactions: a distributed database shared in a computer network (P2P network). This open source software allows all peers in a network to verify every transaction ever made in Bitcoin, and therefore serve as guardians of this central ledger. Nodes (as peers in networks are known) work collaboratively, with little or no interaction between them, adopting mutual verification as proof of transaction chronology. This 'ledger' is secure as long as all the computing (processor) power of honest nodes is higher than that of dishonest nodes.

The number of bitcoins to be produced is limited to 21 million, meaning that the value of the digital currency increases over time (early adopters are thus rewarded). Anyone can create ('mine') Bitcoin by transmitting the solution for a previously unsolved mathematical-computational problem (using the proof-of-work system). All nodes work on this 'problem' and once the solution is found, that block is closed and all of the nodes move forward to the next problem (the next block in this chain). Nodes, or 'miners' as they are called, are rewarded for dedicating their computer power to the safety of network. This reward is in the form of a specific number of bitcoins and transaction fees paid by others.

The main advantages of cryptocurrencies are low fees compared to the traditional banking system, quick and transparent payments, and mobile access. These advantages can boost the activities of start-ups and help developing countries stand on an equal footing with developed countries in the global market.

Many worldwide services now accept Bitcoin as payment and such transactions have been exempted from value added tax (VAT) in several countries. In July 2015, the CJEU ruled that exchanging traditional currency for Bitcoin online should be exempt from consumption taxes just like other transactions of banknotes and coins.

There are also signs that central banks are paying more and more attention to virtual currencies. As an example, in early 2016, the People's Bank of China announced that it was looking into the possibility of launching its own virtual currency, considering that this would contribute to making economic activities more transparent, while also reducing money laundering and tax evasion.[34]

In 2016, the International Monetary Fund (IMF) published the report Virtual Currencies and Beyond: Initial Considerations. The report points at different challenges related to the regulation and policy-making of virtual currencies, including consumer protection, taxation, and financial stability. According to the report, proper policy responses 'will need to calibrate regulation in a manner that appropriately addresses the risks without stifling innovation'. At international level, best practices and international standards should guide regulatory responses and promote harmonisation across jurisdictions.[35]

The issues

Changes to the worldwide banking system

The further use of both e-banking and e-money could bring about changes to the worldwide banking system, providing customers with additional possibilities while simultaneously reducing banking charges. Bricks-and-mortar banking methods will be seriously challenged by more cost-effective e-banking. It should be noted that most traditional banks have already adopted e-banking. In 2002, there were only 30 banks providing online services in the USA. Today it is difficult to find a bank without e-banking services.

Mobile commerce

E-payments and e-money are currently undergoing fast changes, as technology and devices evolve and develop. Mobile payments have already surpassed the simple orders placed via SMS, as mobile phones become more sophisticated and 'intelligent' (like smart phones and iPhones) allowing for diverse applications, including for mobile commerce.

Cybersecurity

Cybersecurity is one of the main challenges to the wider deployment of e-payments. How can the safety of financial transactions via the Internet be ensured? It is important to stress the responsibility of banks and other financial institutions for the security of online transactions. The main development in this respect was the Sarbanes-Oxley Act (SOXA),[36] adopted by the US Congress as a reaction to the Enron, Arthur Andersen, and WorldCom financial scandals. This act tightens financial control and increases the responsibility of financial institutions for the security of online transactions. It also shares the burden of security responsibility between customers – who have to demonstrate certain prudence – and financial institutions.

Unavailability of e-payment methods

The unavailability of e-payment methods is often viewed as one of the main impediments to the faster development of e-commerce. Currently, e-commerce is conducted primarily by credit card. This is a significant obstacle for developing countries that do not have a developed credit card market. The governments in those countries would have to enact the necessary legal changes to enable the faster introduction of card payments.

National and regional initiatives

To foster the development of e-commerce, governments worldwide need to encourage all forms of cash-free payments, including credit cards and e-money. The faster introduction of e-money will require additional governmental regulatory activities.

After Hong Kong, the first to introduce comprehensive e-money legislation, the EU adopted the Electronic Money Directive in 2000 (it was revised in 2009).[37] Unlike e-money, there is no regulation of digital and/or virtual currency in the EU yet. Currently, it is left to member states to regulate currencies such as Bitcoin. Germany considers Bitcoin as 'private money' exchanged between two persons or entities. In the UK, it is a considered a means of exchange but not money. Most countries have chosen a 'wait and see' approach. Other countries, such as Russia and Thailand, have taken more radical steps to ban Bitcoin transactions on a national level.

International initiatives

Due to the nature of the Internet, it is likely that e-money and virtual currencies will become global phenomena, thus providing a reason to address this issue at international level. One potential player in the field of e-banking is the Basel Committee E-Banking Group. This group has already started addressing authorisation, prudential standards, transparency, privacy, money laundering, and cross-border supervision, which are key issues for the introduction of e-money.[38]

The main international initiative in relation to virtual currency has been taken in the Financial Action Task Force (FATF), which addresses the questions of money laundering and the financing of terrorism. The USA has initiated discussions in the FATF on how to apply rules against money laundering and the financing of terrorism in the field of virtual currencies.

The law enforcement link

The 2002 request from the New York State Attorney General to PayPal and Citibank not to execute payments to Internet casinos is an example of how law enforcement agencies have started to make use of e-payment systems to perform their tasks.[39] What law enforcement could not achieve through legal mechanisms, it accomplished through the control of electronic payments.

Privacy

Every e-payment transaction leaves a trace, which is recorded by the issuers of the e-payment instrument (credit card companies, banks). While the keeping of such records is needed and justifiable for clearing purposes and as evidence of payments, the aggregation of such data may pose serious threats to users' privacy, if data mining is used to track purchasing and spending habits or score clients for the provision of future financial services.

Risks and misuse of virtual currencies

The risks of virtual currency became clear after the closure of Mt Gox, one of the biggest Bitcoin online exchange markets, in February 2014.[40] The many investors lost close to US$ 500 million in a case of user account credentials theft.

There are many warnings that virtual currencies could potentially be misused for illegal goods and services, fraud, and money laundering. The anonymity of cryptographic Bit-

coin transactions increases the potential for possible misuse. Moreover, Bitcoin wallets (where bitcoins can be stored offline) can also be encrypted.

In 2014, the FBI closed the Silk Road website which was used to trade in stolen card data, drugs, and other illegal products; the website used Bitcoin as its payment method.[41]

A US government-funded report on the National Security Implications of Virtual Currencies, published at the end of 2015, noted that 'non-state actors', including terrorist and insurgent groups, may exploit virtual currency by using it for regular economic transactions.[42]

The EU is trying to address such problems through legislative measures. In July 2016, the European Commission published a proposal for amending the Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. The proposal intends, among others, to bring virtual currency exchange platforms under the scope of the Directive, requiring them to introduce due diligence control measures that would help in the detection of suspicious virtual currency transactions. The proposal also aims at introducing a legal definition for virtual currencies, and it uses, to this end, the definition provided by the European Banking Authority in 2014.[43]

www.igbook.info/emoney

Consumer protection

Consumer trust is one of the main preconditions for the success of e-commerce. E-commerce is still relatively new and consumers are not as confident with it as with real-world shopping. Consumer protection is an important legal method for developing trust in e-commerce. E-commerce regulation should protect customers in several areas, such as:

- Online handling of payment card information.
- Misleading advertising.
- Delivery of defective products.

A new and specific feature of e-commerce is the internationalisation of consumer protection, which is not a vital issue in traditional commerce. In the past, consumers rarely needed international protection. They were buying locally and therefore needed local customer protection. With e-commerce, an increasing number of transactions take place across international borders.

Jurisdiction is a significant issue surrounding consumer protection. It involves two main approaches. The first favours the seller (mainly e-business) and is a country-of-origin/prescribed-by-seller approach. In this scenario, e-commerce companies have the advantage of relying on their own legal environment, which is predictable and well-known. The other approach, which favours the customer, is a country-of-destination approach.

The main disadvantage for e-commerce companies is the potential for exposure to a wide variety of legal jurisdictions. One possible solution to this dilemma is a better harmonisation of consumer protection rules, making the question of jurisdiction less relevant. As with other e-commerce issues, the OECD assumed the lead by adopting the 1999 Guide-

lines for Consumer Protection in the Context of E-commerce[44] and the 2003 Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders.[45] The main principles established by the OECD are still valid and have been adopted by other business associations, including the ICC.

The EU offers a high level of e-commerce consumer protection and promotes awareness campaigns on online shopping issues. The problem of jurisdiction has been addressed via the Brussels I Regulation,[46] which stipulates that consumers will always have recourse to local legal protection. The recast Brussels I Regulation,[47] applicable as of January 2015, further harmonises the rules of jurisdiction by extending the situations under which individuals not domiciled in the EU can be sued by consumers in the courts of EU member states.

A number of private associations and NGOs also focus on consumer protection in the area of e-commerce, including Consumers International, the International Consumer Protection and Enforcement Network, and the ICC.

The future development of e-commerce will require either the (further) harmonisation of national laws or a new international regime for e-commerce customer protection.

www.igbook.info/consumers

Taxation

The spirit of discussion on the Internet and taxation can be likened to Faraday's response to a sceptical politician who asked him about the purpose of his invention (electromagnetic induction): 'Sir, I do not know what it is good for. But of one thing I am quite certain, some day you will tax it.'[48]

The more the Internet becomes the core of modern economy, the more the question of taxation has come into focus. It has become even more important since the financial crisis in 2008. Many governments have been trying to increase fiscal income to reduce growing public debt. The taxation of economic activities on the Internet became one of the first possibilities for increasing fiscal income.

One of the first comprehensive reports on Internet taxation was presented by the French Ministry of Economy and Finance in January 2013,[49] and was later followed by other reports dealing with the issue of taxation in the digital economy.[50]

The Internet governance dilemma of whether cyber issues should be treated differently from real-life issues is clearly mirrored in the question of taxation. Since the early days, the USA has been attempting to declare the Internet a tax-free zone. In 1998, the US Congress adopted the Internet Tax Freedom Act. After the applicability of this act was extended several times, in 2016 the US Congress passed legislation that permanently bans states and local governments from taxing Internet access. In addition to the permanent extension of the Internet Tax Freedom Act, the measure also bans some taxes on digital goods and services.[51]

The OECD and the EU have promoted the view that the Internet should not have special taxation treatment. The OECD's 1998 Ottawa Principles specify that the taxation of e-commerce should be based on the same principles as taxation for traditional commercial

activities: neutrality, efficiency, certainty and simplicity, effectiveness and fairness, and flexibility.[52] In a report from 2014, the European Commission reiterates that 'there should not be a special tax regime for digital companies. Rather the general rules should be applied or adapted so that 'digital' companies are treated in the same way as others.'[53]

Following the view that the Internet should not have special taxation treatment, the EU introduced a regulation in 2003 requesting non-EU e-commerce companies to pay VAT if they sold goods within the EU. The main motivation for the EU's decision was that non-EU (mainly US) companies had an edge over European companies, which had to pay VAT on all transactions, including electronic ones. Currently, non-EU countries have started to adopt the same strategy. With the rapid increase in the number of Internet users and the increased centrality of Internet companies – mostly from the USA – in their economies, many countries have started to tax Internet services that are offered by companies not registered within their borders. Examples range from Russia[54] and India[55] to Israel[56] and Indonesia.[57]

Another e-taxation issue that remains unresolved is the question of the location of taxation. The Ottawa Principles introduced a 'destination' instead of 'origin' principle of taxation. The US government, however, has a strong interest in having taxation remain at the origin of transactions, since most e-commerce companies are based in the USA. In contrast, the EU, for example, is interested in destination taxation, as it has more e-commerce consumers than sellers.

In the context of the Internet, taxation is not only discussed as an object of revised legislation, but also in the context of tax avoidance by large Internet companies. In January 2016, the European Commission presented an Anti Tax Avoidance Package, which aims to prevent companies in the EU from shifting their profits to low-tax countries. The publication came in the midst of rising discussions concerning Google's tax practices. According to Italian authorities, Google has evaded €227 million in taxes between 2009 and 2013.[58] On top of that, controversy has arisen in the UK concerning the revelation of a £130 million tax deal between Google and national tax authorities.[59] In May 2016, the French government even organised a search of Google's Paris headquarters as part of an investigation into tax fraud, as France accused the company of owing €1.6 billion in unpaid taxes.[60] A recent study by the US Public Interest Research Group Education Fund and Citizens for Tax Justice showed that among the top 30 tax-withholding businesses, 10 were tech companies, with Apple as the record holder.[61]

Some countries are introducing tax reliefs for Internet infrastructure providers and/or providers of online services, with the aim of encouraging investments in the deployment of infrastructure, and boosting local e-commerce companies. In India, for example, the telecom ministry has proposed a ten-year tax 'holiday' for big projects in the IT sector to draw investment.[62] In China, the State Council is offering tax concessions to Chinese hi-tech companies, lowering their corporate tax from 25 to 15%.[63] The UK government included a provision in its 2016 budget introducing a tax relief for micro-entrepreneurs who sell their services online or rent their home through the Internet.[64]

www.igbook.info/taxation

Endnotes

[1] Andrew Odlyzko views the question of pricing and architecture on the Internet from a historical perspective. Based on the pricing for transportation systems since the ancient world, he draws conclusions on the current Internet pricing policy. For more information, consult: Odlyzko A (2004) Pricing and Architecture of the Internet: Historical Perspectives from Telecommunications and Transportation. Available at http://www.dtc.umn.edu/~odlyzko/doc/pricing.architecture.pdf [accessed 25 October 2016].

[2] World Bank (2016) World Development Report 2016: Digital Dividends. Available at http://www.worldbank.org/en/publication/wdr2016 [accessed 29 October 2016].

[3] The White House (1997) Framework for Global Electronic Commerce. Available at http://clinton4.nara.gov/WH/New/Commerce/ [accessed 25 October 2016].

[4] WTO (1998) Work programme on electronic commerce. Available at http://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm [accessed 25 October 2016].

[5] European Union (2000) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Available at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32000L0031 [accessed 25 October 2016].

[6] PFSweb (2015) B2B eCommerce. Available at http://www.pfsweb.com/PDF/whitepapers/PFSweb-B2B-eCommerce-Whitepaper.pdf [accessed 16 August 2016].

[7] WTO (no date) GATT and the Goods Council. Available at http://www.wto.org/english/tratop_e/gatt_e/gatt_e.htm [accessed 25 October 2016].

[8] WTO (no date) Services trade. Available at https://www.wto.org/english/tratop_e/serv_e/serv_e.htm [accessed 2 November 2016].

[9] WTO (1994) Agreement on Trade-related Aspects of Intellectual Property Rights. Available at http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm [accessed 25 October 2016].

[10] Although 'temporary', the moratorium has been subsequently extended by the WTO Ministerial Conference. The most recent such decision was taken at the Nairobi Ministerial Conference in December 2015, and it to be reviewed at the 2017 conference. WTO Ministerial Conference (2015) Ministerial Decision of 19 December 2015: WT/MIN(15)42 – WT/l/977. Available at https://www.wto.org/english/thewto_e/minist_e/mc10_e/l977_e.htm [accessed 25 October 2016].

[11] For details on the WTO's e-commerce-related activities, refer to WTO (no date) Electronic commerce. Available at http://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm [accessed 25 October 2016].

[12] For more information about the USA/Antigua Online Gambling Case, refer to http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm [accessed 25 October 2016].

[13] Geneva Internet Platform (2016) Report from WTO Public Forum 2016. Available at http://digitalwatch.giplatform.org/events/wto-public-forum [accessed 27 October 2016].

[14] For a more comprehensive overview on e-commerce discussions within the WTO, refer to Maciel M (2016) E-commerce in the WTO: the next arena of Internet policy discussions. Available at https://www.diplomacy.edu/blog/e-commerce-wto-next-arena-internet-policy-discussions [accessed 27 October 2016].

[15] UNCITRAL (1996) Model Law on Electronic Commerce. Available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html [accessed 25 October 2016].

[16] United Nations General Assembly (2005) Resolution A/60/20. United Nations Convention on the Use of Electronic Communications in International Contracts. Available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html [accessed 2 November 2016].

[17] ebXML website. Available at http://www.ebxml.org/ [accessed 25 October 2016].

[18] UNCTAD (no date) Information Economy Report (series). Available at http://unctad.org/en/Pages/Publications/InformationEconomyReportSeries.aspx [accessed 25 October 2016].

[19] UNCTAD (no date) eTrade for All: Unlocking the Potential of E-Commerce in Developing Countries. Available at http://unctad.org/en/Pages/DTL/STI_and_ICTs/eTrade-for-All.aspx [accessed 27 October 2016].

[20] OECD (1998) Action Plan for Electronic Commerce. Available at http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=SG/EC(98)9/FINAL&docLanguage=En [accessed 27 October 2016].

[21] Teleanu S (2016) Digital policy issues emphasised at the G20 Leaders' Summit. Available at https://www.diplomacy.edu/blog/digital-policy-issues-emphasised-g20-leaders'-summit [accessed 27 October 2016].

[22] APEC (no date) Paperless Trading Individual Action Plan. Available at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Paperless-Trading-Individual-Action-Plan.aspx [accessed 25 October 2016].

[23] COMESA (2010) Model Law on Electronic Transactions and Guide to enactment. Available at http://programmes.comesa.int/attachments/article/166/COMESA%20Model%20Law%20and%20%20Guide%20to%20Enactment%20(fin).pdf [accessed 25 October 2016].

[24] Net Market Share (2016) Market Share Statistics for Internet Technologies. Available at https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0 [accessed 1 September 2016].

[25] Thuy T, Nguyen T and Armitage GJ (2005) Evaluating Internet Pricing Schemes: A Three-Dimensional Visual Model. *ETRI Journal* 27(1) pp. 64–74. Available at http://etrij.etri.re.kr/etrij/journal/article/article.do?volume=27&issue=1&page=64 [accessed 25 October 2016].

[26] Hayel Y, Maille P and Tuffin B (2005) Modelling and analysis of Internet pricing: introduction and challenges. In Proceedings of the International Symposium on Applied Stochastic Models and Data Analysis (ASMDA), Brest, France. Available at http://conferences.telecom-bretagne.eu/asmda2005/IMG/pdf/proceedings/1389.pdf [accessed 26 October 2016].

[27] European Commission (2016) A European agenda for the collaborative economy. Available at http://ec.europa.eu/DocsRoom/documents/16881 [accessed 1 September 2016].

[28] As quoted in Holland K and Cortese A (1995) The future of money: e-cash could transform the world's financial life. *Business Week,* 12 June, p. 66.

[29] As reported in Olson T (2012) Higher costs, new laws mean no more free rides on some bank services, accounts. *Pittsburgh Tribune-Review*, 1 April. Available at http://triblive.com/x/pittsburghtrib/business/s_789300.html [accessed 1 November 2016].

[30] Basel Committee on Banking Supervision (1998) Risk Management for Electronic Banking and Electronic Money Activities. Basel March 1998 Available at http://www.bis.org/publ/bcbs35.pdf [accessed 25 October 2016]. Final version published in 2003 and available at http://www.bis.org/publ/bcbs98.htm [accessed 25 October 2016].

[31] Kamberi A (2014) Cryptocurrencies and Bitcoin. Available at https://www.diplomacy.edu/blog/cryptocurrencies-and-bitcoin [accessed 25 August 2016].

[32] European Central Bank (2012) Virtual currency schemes. Available at https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf [accessed 17 August 2016].

[33] European Banking Authority (2014) EBA Opinion on 'virtual currencies'. Available at https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf [accessed 17 August 2016].

[34] *The Register* (2016) China to set up its own virtual currency. 22 January. Available at http://www.theregister.co.uk/2016/01/22/china-virtual-currency-risks/ [accessed 29 October 2016].

[35] He D *et al.* (2016) Virtual Currencies and Beyond: Initial Considerations. International Monetary Fund Staff Discussion Note 16/03. Available at https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf [accessed 21 February 2016].

[36] *Soxlaw* (no date) A guide to the Sarbanes Oxley Act. Available at http://www.soxlaw.com/ [accessed 26 October 2016].

[37] European Union (2009) Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF [accessed 26 October 2016].

[38] The Basel Group is based at the Bank for International Settlements. It provides a *Survey of Developments in Electronic Money and Internet and Mobile Payments.* Available at http://www.bis.org/publ/cpss62.pdf [accessed 26 October 2016].

[39] Richtel M (2002) PayPal and New York in Accord on Gambling. *The New York Times*, August 22. Available at http://www.nytimes.com/2002/08/22/business/technology-paypal-and-new-york-in-accord-on-gambling.html?src=pm [accessed 26 October 2016].

[40] Takemoto Y and Knight S (2014) Mt. Gox file for bankruptcy, hit with lawsuit. *Reuters*, 28 February. Available at http://www.reuters.com/article/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228 [accessed 26 October 2016].

[41] Federal Bureau of Investigation (2014) Press Release: Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court. Available at https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court [accessed 26 October 2016].

[42] Baron J *et al.* (2015) National Security Implications of Virtual Currency. Examining the Potential for Non-state Actor Deployment. Rand Corporation. Available at http://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1231/RAND_RR1231.pdf [accessed 17 August 2016].

[43] European Commission (2016) Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC. Available at http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf [accessed 17 August 2016].

[44] OECD (1999) Guidelines for Consumer Protection in the Context of Economic Commerce. Available at http://www.oecd.org/internet/consumer/oecdguidelinesforconsumerprotectioninthecontextofelectroniccommerce1999.htm [accessed 26 October 2016].

[45] OECD (2003) Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices. Available at http://www.oecd-ilibrary.org/industry-and-services/oecd-guidelines-for-protecting-consumers-from-fraudulent-and-deceptive-commercial-practices-across-borders_9789264103573-en-fr [accessed 1 November 2016].

[46] European Union (2001) Regulation (EC) No 44/2001 (Brussels I Regulation). Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0044:en:HTML [accessed 26 October 2016].

[47] European Union (2012) Regulation (EU) No 1215/2012 (Recast Brussels I Regulation). Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:en:PDF [accessed 26 October 2016].

[48] Soete L and Weel B (1999) Cybertax. Maastricht Economic Research Institute on Innovation and Technology (MERIT), Maastricht University. Available at http://www.merit.unu.edu/publications/rmpdf/1998/rm1998-020.pdf [accessed 27 October 2016].

[49] Collin P and Colin N (2013) Mission d'expertise sur la fiscalité de l'économie numérique. Available at http://www.economie.gouv.fr/files/rapport-fiscalite-du-numerique_2013.pdf [accessed 27 October 2016].

[50] Examples of publications dealing with the issue of Internet taxation include: EY (2015) The dawning of digital economy taxation. Available at http://www.ey.com/Publication/vwLUAssets/ey-the-dawning-of-digital-economy-taxation/$FILE/ey-the-dawning-of-digital-economy-taxation.pdf [accessed 17 August 2016]; Andes S and Atkinson R (2013) A Policymakers' Guide to Internet Tax. Available at http://www2.itif.org/2013-policymakers-guide-internet-tax.pdf [accessed 17 August 2016]; OECD (2015) Addressing the Tax Challenges of the Digital Economy. Available at http://www.oecd-ilibrary.org/taxation/addressing-the-tax-challenges-of-the-digital-economy_9789264218789-en [accessed 17 August 2016]. For more resources on this issue,

consult GIP Digital Watch observatory (no date). Taxation. Available at http://digitalwatch.giplatform.org/issues/taxation [accessed 17 August 2016].

[51] Phillips Erb K (2016) Congress Makes Internet Access Tax Ban Permanent. *Forbes*, 11 February. Available at http://www.forbes.com/sites/kellyphillipserb/2016/02/11/congress-makes-internet-access-tax-ban-permanent/#a403c12380a3 [accessed 26 October 2016].

[52] The Ottawa Taxation Principles are: Neutrality, Efficiency, Certainty and simplicity, Effectiveness and fairness, Flexibility. OECD (2003) Implementation of the Ottawa Taxation Framework Conditions. The 2003 Report. Available at http://www.oecd.org/tax/administration/20499630.pdf [accessed 26 October 2016].

[53] European Commission (2014) Commission Expert Group on Taxation of the Digital Economy. Brussels: European Commission, p. 5. Available at http://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/taxation/gen_info/good_governance_matters/digital/report_digital_economy.pdf [accessed 4 July 2016].

[54] *The Moscow Times* (2016) Russia State Duma passes Google Tax Law. 15 June. Available at https://themoscowtimes.com/articles/russia-state-duma-passes-google-tax-law-53310 [accessed 4 July 2016].

[55] Revanna H (2016) Govt notifies 6% equalization tax on online advertisements. *IBT*, 31 May. Available at http://www.ibtimes.co.in/govt-notifies-6-equalisation-tax-digital-ads-take-effect-june-1-680785 [accessed 4 July 2016].

[56] *The Guardian* (2016) Google, Facebook, eBay and other tech firms targeted by new Israeli tax rules. 12 April. Available at https://www.theguardian.com/technology/2016/apr/11/google-facebook-ebay-tech-firms-israel-tax [accessed 4 July 2016].

[57] *Reuters* (2016) Indonesia says Internet giants need to pay tax or face blockages. 29 February. Available at http://www.reuters.com/article/us-indonesia-tax-internet-idUSKCN0W20QM [accessed 4 July 2016].

[58] *Reuters* (2016) Italian tax police believe Google evaded 227 million euros in taxes: sources. 28 January. Available at http://www.reuters.com/article/us-google-italy-tax-idUSKCN0V614L [accessed 4 July 2016].

[59] Robertson J (2016) Google tax row: what's behind the deal. *BBC News*, 28 January. Available at http://www.bbc.com/news/business-35428966 [accessed 4 July 2016].

[60] *BBC* (2016) Google's Paris HQ raided in tax probe. 24 May. Available at http://www.bbc.com/news/business-36370628 [accessed 4 July 2016].

[61] McIntyre RS *et al*. (2015) Offshore Shell Games 2015. Available at http://www.uspirg.org/sites/pirg/files/reports/USP%20ShellGames%20Oct15%201.3.pdf [accessed 4 July 2016].

[62] Aulakh G (2016) Budget 2016: Telecom Ministry seeks 10-year tax holiday for Make in India drive. *Economic Times*, 15 February. Available at http://economictimes.indiatimes.com/industry/telecom/budget-2016-telecom-ministry-seeks-10-year-tax-holiday-for-make-in-india-drive/articleshow/50988028.cms [accessed 4 July 2016].

[63] Ren (2016) Beijing offers tax concessions to hi-tech companies. *South China Morning Pos*t, 14 February. Available at http://www.scmp.com/news/china/policies-politics/article/1913172/beijing-offers-tax-concessions-high-tech-companies [accessed 4 July 2016].

[64] Rampen J (2016) Airbnb hosts get first £1,000 tax free after Budget 2016 shake up. *Mirror,* 16 March. Available at http://www.mirror.co.uk/money/airbnb-hosts-first-1000-tax-7568083 [accessed 17 August 2016].

Section 6

THE DEVELOPMENT BASKET

The development basket

Technology has been the main driver of societal changes throughout history (the wheel, agricultural tools, the printing press, the telegraph, etc.). Technological advancements are expected to bring improvements in society. The current thinking on development and technology can be traced back to the enlightenment period and the growth of science and technology, between the sixteenth and the twentieth centuries. At the core of this thinking lies the link between technology and progress, as well as the idea that technology can solve most social problems: in its simplest form, more technology should lead towards more development.

Technology has also shaped the UN development agenda, which was first promoted after the Second World War, in a move to support the development of newly independent states, former colonies. While technology has contributed to alleviating poverty and improving the wellbeing of many, it has also faced limitations. Social and economic developments are much more complex than technological ones. They require, for example, education and capacity development to empower individuals to make use of the new technologies, as well as policies and institutions that reflect both local cultures and the need to adapt to modern developments. In addition, social adjustments require time, as society changes slower than technology develops.

Communism and the failure of technologically driven development

The major historical failure of the technologically driven development was the failure of the Communist system at the end of the twentieth century. Science and technology were the highest priority areas of the Soviet Union and the Eastern bloc. Despite a later start and limited resources, the Soviet Union managed to match the achievements of the Western world in many areas of scientific and technological development. In particular, it did very well in satellite and military technologies. However, technology was not enough to address socio-economic issues, and the system collapsed. There are many reasons for the collapse, including ideological and structural ones; however, one reason which is still under-researched is the heavy dependence on technological solutions and techno-engineering.

The digital era has reiterated the enabling power of technology. There are numerous examples of how the Internet has enabled many, from the individual to the global level. Yet, the link between technological and social progress is not automatic, as has been clearly outlined by numerous studies and reports.[1] The complex interplay between technology and society will be addressed in this section. Some of the underlying questions include:

- Will the Internet reduce or broaden the existing divide between the developed and developing worlds?
- How and when will developing nations be able to reach the digital levels of more industrially developed countries?
- How can the Internet and digital technologies enable sustainable development, in its different dimensions?

This section addresses the main development issues *per se*. However, development appears horizontally in many digital policy discussions. Almost every Internet governance issue has a developmental aspect, as outlined in the few examples below:

- Access to the Internet – the first precondition for overcoming the digital divide – mainly depends on the existence of a telecommunications infrastructure.
- The current economic model for Internet access continues to place a disproportionate burden on those developing countries that have to finance access to backbones based in developed countries.
- E-commerce offers opportunities to companies in developing countries to access the global market, but such companies first need to have access to the Internet.

Digital technologies and development: policy framing

Digital development issues were put on the global agenda during the WSIS process in the early 2000s. The first UNGA resolution on WSIS stressed the role of WSIS in 'promoting development, in particular with respect to access to and transfer of technology'.[2] As such, the overall objective of the summit was to contribute to bridging the digital divide between the developed and developing countries, and to facilitate the implementation of the millennium development goals (MDGs). The WSIS Geneva Declaration and Plan of Action highlighted development as a priority and linked it to the UN Millennium Declaration[3] and its promotion of access of all countries to information, knowledge, and communication technologies for development. With the link to the MDGs,[4] WSIS was strongly positioned in the development context. The Tunis Agenda for the Information Society also tackled issues related to ICT for development, with a significant part of the document being dedicated to financial mechanisms for meeting the related challenges. More than ten years later, the outcome document of the UNGA high-level meeting on the overall review of the implementation of the WSIS outcomes (WSIS+10 outcome document) established a link between WSIS and the SDGs[5] in its Article 5:

> *We recognize that increased connectivity, innovation, and access have played a critical role in enabling progress on the Millennium Development Goals, and we call for close alignment between the World Summit on the Information Society process and the 2030 Agenda for Sustainable Development, highlighting the crosscutting contribution of information and communications technology to the Sustainable Development Goals and poverty eradication, and noting that access to information and communications technologies has also become a development indicator and aspiration in and of itself.*[6]

The SDGs make a direct reference to the Internet in Goal 9.c., which is to 'significantly increase access to ICT and strive to provide universal and affordable access to the Internet in LDCs by 2020'. Furthermore, in the framework of the SDGs, the Technology Facilitation Mechanism was established, which looks at how science, technology, and innovation can facilitate achievement of the SDGs.[7]

The development theme was also highlighted within the IGF, starting with the first meeting in Athens (2006), through to the latest IGF in 2015, where the overarching theme was 'Evolution of Internet Governance: Empowering Sustainable Development'.

How does ICT affect the development of society?

Following the adoption of the SDGs, there have been many initiatives aimed at looking into this question, and exploring ways in which ICTs could catalyse development.

Some examples include UNCTAD's ICT for Development programme;[8] the WSIS Action Lines-SDG Matrix, which summarises the ways in which ICT can contribute to the different SDGs;[9] and the 2015 and 2016 editions of the WSIS Forum, which were aimed at linking the SDGs to ICT solutions.[10] Finally, the CSTD focused its 2015–2016 intersessional activity on the theme 'Foresight for digital development', examining the potential long-term effects of the latest digital applications (including the IoT, online education, 3D printing, digital automation, etc.) on the economy, society, and the environment. The Commission made several recommendations to governments, encouraging them to, inter alia, adopt appropriate policies to support the development of emerging technologies and take advantage of the opportunities they create, and to promote an enabling environment for digital development, with a focus on areas such as human capital, ICT and complementary infrastructure, and legal frameworks.

The World Bank's World Development Report 2016: Digital Dividends[11] brought a cautionary approach to the discussion of the link between ICT and development, questioning the simplistic view that more technology will lead to more development. The report draws attention to the fact that, while the Internet (and digital technologies, more broadly) has the potential to enable growth and development, inequalities and gaps continue to exist and even widen both at global level and within countries.

Digital technologies bring benefits to people (easier access to information, jobs, and other opportunities), businesses (more productivity and trade, greater competition and innovation), and governments (better public services and enhanced interaction with citizens). But these benefits are not spreading evenly enough and rapidly enough to allow true global economic growth. To overcome this challenge, the World Bank report recommends two main directions: closing the digital divide; and adopting complementary policies that would allow individual users, business, and the public sector to take full advantage of digital technologies. Such policies (collectively called analogue complements) would cover regulations that encourage market competition and give companies the incentive to continuously innovate, policies focused on education and training programmes in the area of digital literacy, and more capable and accountable public institutions that effectively employ technologies in policy-making processes and provision of public services. Moreover, even if all these ingredients are present, the key challenge lies in how and when they should be used and combined.

The report reconfirms the old wisdom that technology is never neutral. The history of human society provides many examples of technology empowering some individuals, groups, or nations, while excluding others. The Internet is no different in this respect: from the individual to the global level, digital opportunities are seized in different ways, and a profound change has occurred in the distribution of wealth and power.

In short, the effects of ICTs on socio-economic development are complex and wide-ranging. Nevertheless, the growing interest in these social and economic dimensions of ICTs provides possibilities to better measure and untangle the web of ICT's impact on society, and to find out how to best utilise ICT applications for socio-economic development.

www.igbook.info/development

The digital divide

The digital divide can be defined as a rift between those who have access and capabilities to use ICT/Internet, and those who, for technical, political, social, or economic reasons, do not. The OECD refers to the digital divide as 'the gap between individuals, households, businesses and geographic areas at different socioeconomic levels with regard both to their opportunities to access information and communication technologies (ICTs) and to their use of the Internet for a wide variety of activities'.[12]

The digital divide is not an independent phenomenon. It reflects existing broad socio--economic inequalities in education, healthcare, capital, shelter, employment, clean water, and food.

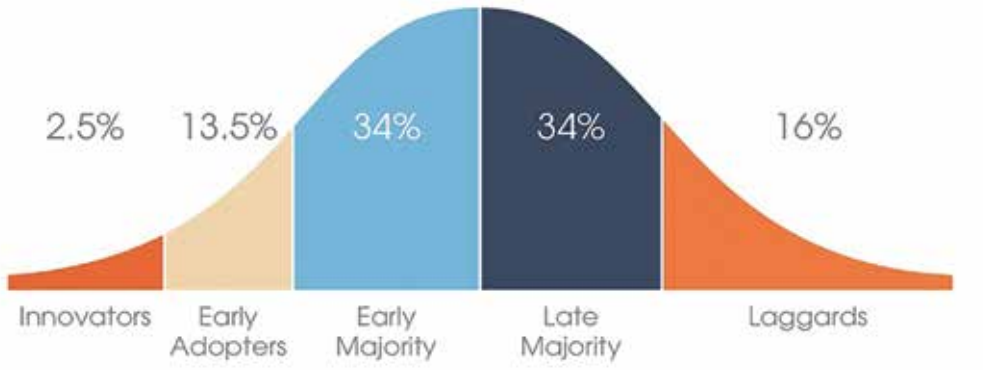

Figure 21. Rogers's diffusion of innovations curve

Rogers's diffusion of innovations curve (Figure 21) helps explain the crucial interplay between the possibilities that are offered by technological tools, and the realities of technology perception and adoption. It classifies adopters of technologies into several categories, ranging from innovators to laggards.

Rogers's curve also explains the digital divides that exist at different levels: within countries and between countries, between rural and urban populations, between old and young, between men and women, between educated and less educated, etc.

Is the digital divide widening?

ICT/Internet developments leave the developing world behind at a much faster rate than advances in other fields (e.g. agricultural or medical techniques) and, as the developed world has the necessary tools to successfully take advantage of these technological advances, the digital divide appears to be continuously and rapidly widening. This view is frequently expressed in various highly regarded documents, such as the United Nations Development Programme (UNDP) Human Development Reports and the International Labour Organization (ILO) Global Employment Reports.

Some opposing views argue that statistics on the digital divide are often misleading and that the digital divide is in fact not widening at all, but is even narrowing.[13] According to this view, the traditional focus on the number of computers, the number of Internet websites, or the available bandwidth should be replaced with a focus on the broader impact of ICT/Internet on societies in developing countries. Frequently quoted examples are the digital successes of Brazil, China, and India.

In fact, the criteria for assessing the gaps in the digital divide are changing and becoming more complex to better capture the development realities. Current assessments consider aspects such as ICT readiness and overall ICT impact on society. WEF has developed the Networked Readiness Index (NRI) as a new approach in measuring the Internet-level of countries worldwide.[14] It also provides new perspectives on how the digital divide is addressed.

Universal access

In addition to the digital divide, another frequently mentioned concept in the development debate is universal access, i.e., Internet access for all. Although it should be the cornerstone of any digital development policy, differing perceptions and conceptions of the nature and scope of universal access remain. The question of universal access at the global level remains largely an open issue, and depends mainly on the readiness of developed countries to invest in the realisation of this goal, as well as on the policy environment in developing countries. Still, the importance of universal access is agreed on in many international documents, such as the WSIS+10 outcome document.

Unlike universal access at the global level, in some countries universal access is a well-developed economic and legal concept. Providing telecommunication access to all citizens is the basis of US telecommunications policy. The result is a well-developed system of different policy and financial mechanisms to subsidise access costs in remote areas and regions with high connection costs. The subsidy is financed by regions with low connection costs, primarily the big cities. The EU has also taken a number of concrete steps towards achieving universal access by promoting policies to ensure every citizen has access to basic communications services, including an Internet connection, and enacting specific regulations thereof.[15] A proposal for a European Electronic Communications Code, put forward by the European Commission in September 2016, plans to redefine the notion of universal service at EU level, by removing legacy service (such as public payphones) from the scope and focusing on broadband.[16]

Recently, many Internet companies have taken initiatives to increase Internet access. They are trying to harvest the enormous business potential of regions that are not yet connected. These initiatives either focus on the traditional means of constructing cables or rely on less traditional methods, such as using Internet-disseminating drones (Facebook) and balloons (Google).

Refer to Section 2 for further discussion on Internet infrastructure, including innovative solutions.

Strategies for overcoming the digital divide

Since access involves different dimensions – from access to infrastructure to access to content – as a UNHRC report points out,[17] overcoming the digital divide, at global, regional, and national level, is a complex and long-term process, which requires a mix of measures and policies, as well as the involvement of a multitude of actors (governments, intergovernmental organisations, the private sector, etc.).

Developing telecommunications and Internet infrastructures

Access to Internet infrastructure is one of the main challenges to overcoming the digital divide. There are two main aspects related to access to the Internet in developing countries. The first is access to international Internet backbones. The second is connectivity within developing countries.

Access to international Internet backbones depends mainly on the availability of submarine fibre optic cables, which play a major role in connecting continents. Due to geography, but also due to the relatively smaller costs of deployment, major intercontinental backbone links are submerged under the oceans. These cables currently provide the medium through which more than 90% of all global Internet traffic flows.

Refer to Section 2 for further discussion on Internet backbone cables.

In addition to submarine cables, there are emerging plans for additional strategic terrestrial intercontinental cable. The Chinese One Belt, One Road project, for instance, looks at deploying a fibre optic terrestrial cable to connect Asia and Europe. More terrestrial link cables are in the planning phase.

In the long term, the shift towards overland Internet communication could have far-reaching developmental impact on landlocked Eurasian countries. They could be provided with easier and cheaper access to the Internet, compared to the current situation where they have to finance an expensive access via Internet submarine cables.

Another solution for improved access is the introduction of IXPs, which help to keep local traffic within a country. Without IXPs, for example, e-mail exchanges between customers of two operators in the same country would often be routed via international connection and returned to the same country. IXPs are technical facilities through which different ISPs exchange Internet traffic through peering (without paying). IXPs are usually established to keep Internet traffic within smaller areas (e.g. city, region, country).

Still, many developing countries do not have IXPs, which means a considerable part of traffic between the clients within the country is routed through another country. This increases the volume of long-distance international data traffic from the developing country, and the cost of providing Internet service to the country. Different initiatives seek to establish IXPs in developing countries.[18] One that has achieved considerable success is that of the AU's African Internet eXchange System (AXIS) Project, which has supported the establishment of IXPs in Africa.

Connectivity in developing countries is another major challenge. Formerly, the majority of Internet users were concentrated in major cities. Rural areas usually had no access to the

Internet. The situation started changing with the rapid growth of mobile telephony and wireless communication.

Wireless communication might be a viable alternative to the often-challenging development of traditional terrestrial communications infrastructures (which involves laying cables over very long distances throughout many Asian and African countries). In this context, radio spectrum policies are of utmost importance in ensuring spectrum availability and efficient use. In this way, the problem of the last mile or local loop, one of the key obstacles to faster Internet development, could be overcome. However, there are also views according to which mobile technologies are not a comprehensive solution, but rather an intermediary one when it comes to covering large areas that lack connectivity. It is argued that the radio spectrum has physical limits, for example regarding the number of devices that can be connected over wireless networks.[19]

Traditionally, the infrastructural aspect of the digital divide has been the focus of the ITU through its ITU-D.

Who should cover the cost of links between developing and developed countries?

When an end-user in Africa sends an e-mail to a correspondent in Europe, the USA, or China, the African ISP bears the cost of international connectivity from Africa to the main backbones located in the main Internet hubs in Europe, North America, and Asia. However, when a European end-user sends an e-mail to Africa, the African ISP still bears the cost of international connectivity, and ultimately the African end-user bears the brunt by paying higher subscription fees covering the flow of digital traffic both ways. This is mainly because ISPs in developing countries have difficulties in entering into shared-cost peering agreements with large international providers, due to their small customer bases. These ISPs end up acting like resellers, in that they buy connectivity from international providers and resell to their domestic clients, with the resulting higher costs.[20]

The main argument in discussions about changes to the current system of Internet charges uses the analogy of the telephone financial settlement system, which shares costs and income between communication end-points. However, Geoff Huston, Chief Scientist at APNIC, argues that this analogy is not sustainable.[21] In the telephony system, only one clearly identifiable commodity– a phone call establishing human conversation between two telephone sets – has a price. The Internet does not have an equivalent, single commodity; it has packets, which take different routes through the network. This fundamental difference makes the analogy with telephony inappropriate. It is also the main reason why the telephone financial settlement model cannot be applied to the Internet.

The ITU initiated discussions on possible improvements to the current system for the settlement of Internet expenses, aiming for more balanced distribution of costs for Internet access. In 2008, ITU Recommendation D. 50 was adopted, which included recommendations for commercial agreements on international Internet connections that would take into account the need for compensation between parties for the value of elements such as traffic flow, number of route, cost of international transmission, etc. Due to opposition from developed countries and telecom operators, the recommendation is practically ineffective. One of the limitations of negotiating this issue between governments is that most interconnection agreements are concluded between private telecommunications operators, and are often confidential. This led the ITU to adopt, in 2013, a Supplement to Recommendation D.50, which put emphasis on alternative modalities for reducing the cost of international Internet connectivity, such as IXPs, rollout of submarine cables, and the development of local content.[22]

Financial support

During the WSIS process, the importance of financial support for bridging the digital divide was clearly recognised. One idea proposed at WSIS was the establishment of a UN-administered Digital Solidarity Fund to help technologically disadvantaged countries build telecommunications infrastructures. Although a Global Digital Solidarity Fund was officially inaugurated in March 2005, it did not garner broad support from developed countries, which favoured direct investment instead of the establishment of a centralised development fund.

Developing countries receive financial support through various channels, including bilateral or multilateral development agencies, such as the UNDP or the World Bank, as well as regional development initiatives and banks. The ITU has also launched an ICT Development Fund, a seed-funding initiative aimed to contribute to promoting sustainable development through the implementation of ICT development-related projects at national, regional, and global level. Looking forward, the Addis Ababa Action Agenda, adopted at the Third International Conference on Financing for Development, and endorsed by the UNGA in July 2015, provides a global framework for financing sustainable development, across all SDGs, and, as such, could help further incentivise financial support for countries to bridge the various dimensions of the digital divide.[23]

With increased liberalisation of the telecommunications market, the tendency for developing telecommunications infrastructures through foreign direct investment has grown. Since telecommunications markets of developed countries are oversaturated, many international telecommunications companies see the markets of developing countries as the area for future growth.

Skills and competences for effective access

The basic ability to connect to the Internet is a precondition for access. Still, the definition of access is believed by some to be significantly broader and should take into account the quality of access. The WSIS+10 outcome document pleads in this regard for 'an evolving understanding of what constitutes access, emphasizing the quality of that access. [...] speed, stability, affordability, language, local content and accessibility for persons with disability are now core elements of quality'.

The existence of communications infrastructure is useless unless people possess the means (devices) and the knowledge (ICT literacy) to access and benefit from the Internet. Developing countries, in particular those in Africa, still make a limited contribution to global online knowledge. The gap between the developed and the developing world is more significant in the area of knowledge-contribution than, for example, access to the Internet. For example, Hong Kong (SAR China) provides more content to Wikipedia than all of Africa combined, although Africa has 50 times more Internet users.[24]

Many initiatives and organisations have aimed to build skills and address sociocultural aspects of digital divides. For example, international initiatives and organisations such as One Laptop per Child, Close the Gap, and Computer Aid International aim to provide refurbished and low-cost equipment to underserved communities in developing countries. Local initiatives to provide affordable devices have taken off as well. Singapore, for example, has a programme through which students and persons with disabilities from low-income families are given the opportunity to acquire a computer at an affordable price.[25]

For developing countries, one of the main issues has been brain drain – the movement of highly skilled labour from developing to developed countries. Through brain drain, developing countries lose skilled labour, as well as their investment in the training and education of the migrating skilled labour.

Brain drain will likely continue, given the various employment and emigration schemes that have been introduced in the USA and other developed countries to attract skilled, mainly ICT-trained, labour.

On the other hand, one development that may stop or, in some cases, even reverse brain drain, is the increase in the outsourcing of ICT tasks to developing countries. The most successful example is the development of India's software industry centres, such as Bangalore and Hyderabad.

Policy and institutional aspects

Telecommunications policy issues are closely linked with overcoming the digital divide in many respects:

- Neither private investors nor, increasingly, public donors, are ready to invest in countries without a proper institutional and legal environment for Internet development.
- The development of national ICT sectors depends on the creation of necessary regulatory frameworks.
- Telecommunications policy should facilitate the establishment of an efficient telecommunications market with more competition, lower cost, and a wider range of services provided.

The creation of an enabling environment is a demanding task, entailing the gradual de-monopolisation of the telecommunications market; the introduction of Internet-related laws (covering copyright, privacy, e-commerce, etc.); and the availability of Internet access to all without political, religious, or other restrictions.

One of the first steps is to establish independent and professional telecommunications regulatory authorities. Experience from developed countries shows that solid regulatory strategies are a precondition for rapid growth in telecommunications infrastructure. Developing countries have started to follow this approach, but some of them still face problems with regulatory authorities that are generally weak, lack independence, or are often part of a system in which state-owned telecom operators are influential in regulatory and political processes.

Another major challenge has been the liberalisation of the telecommunications market. India and Brazil are usually held up as examples of developing countries where such liberalisation facilitated fast growth of the Internet and the ICT sector and benefited overall economic growth. Some other countries, in particular least developed ones, have found liberalisation of the telecommunications market to be a major challenge. With the loss of telecommunications monopolies, governments in those countries lost an important source of budgetary income. The lower budgets affected all the other sectors of social and economic life.

In some cases, at the same time as losing telecom revenues, these countries failed to harvest the benefits of liberalisation through lower costs and better telecom services, mainly because the privatisation of telecommunications companies was not supplemented by the establishment of effective markets and competition. Such practices led the World Bank to emphasise that countries should open major market segments to competition prior to, or at the same time as, privatising government-owned operators; in this way, they will reduce costs faster than those countries that privatise first and introduce competition later.

www.igbook.info/digitaldivide

Capacity development

The effectiveness and legitimacy of Internet governance depend on the capacity of nations, organisations, and individuals to participate fully in Internet governance policy processes. Capacities refer to their abilities 'to define and solve problems, make informed choices, order their priorities, plan their futures, and to implement programmes and projects to sustain them'.[26]

About capacity development

While there is agreement about the importance of capacity development, there is little understanding about what it includes. Moreover, capacity development is a popular buzzword. In diplomatic negotiations, capacity development is often used as the least common denominator when there is a little agreement on other aspects of the negotiations.

Typically, capacity development is understood as training. This interpretation of the term can be traced back to the 1950s and 1960s, when training was at the core of the technical assistance programmes provided by developed countries to developing ones. Later, in the 1970s, the concept of technical cooperation moved beyond the simple transfer of skills and knowledge, towards contextualisation within national policies and priorities. More recently (in the 1990s), capacity development started focusing on empowering and strengthening endogenous capacities in developing countries.

Capacity development or capacity building

Capacity development and capacity building are two terms often heard in development discussions. The former refers to developing existing endogenous capacities and skills that are present in all countries, while the latter is used more in reference to a process of starting from scratch and building something that has not existed previously. Capacity development is more widely used in current development parlance.

Capacity development could be defined by reference to types of capacities and the levels at which they are developed.

Types of capacities:

- Hard capacities that include technical and specialised knowledge and know how (e.g. engineering knowledge).

- Soft capacities that are often divided in two sub-groups:
  - Operational capacities: intercultural communication, leadership, organisational culture and values, problem-solving skills.
  - Adaptive capacities: ability to analyse and adapt, change readiness and management, confidence.

Hard capacities are often referred to as being technical and visible, while soft capacities are described as rational and invisible.

The various levels where capacities are developed and needed are visualised through the capacity development butterfly (Figure 22, based on the methodology used by the Swiss Agency for Development and Cooperation).[27]

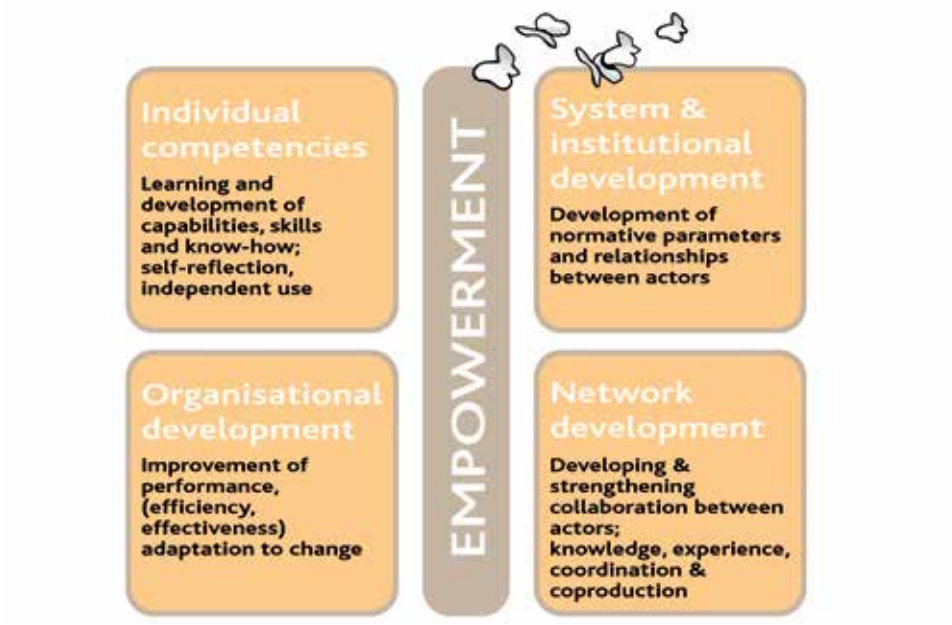

Figure 22. Capacity development butterfly

Capacity development in Internet governance and digital policy

The need for capacity development has been an underlying feature in Internet governance since the WSIS 2003–2005 outcome documents, which underscored capacity development as a priority for developing countries. Likewise, the 2015 WSIS+10 outcome document calls for further investment in capacity development.

Given the novel nature of Internet governance, the main focus has been on individual training and policy immersion.

Many organisations, including the ITU, DiploFoundation, and the Geneva Internet Platform (GIP),[28] APC, the Internet Society, and ICANN have dedicated capacity development programmes. Various regional summer schools on Internet governance also contribute to strengthening capacity, in particular for developing countries. Many of the available programmes focus on telecommunications infrastructure, technical standards, cybersecurity, spam, ICT regulation, freedom of expression, e-commerce, labour law, access, and overcoming the digital divide.

Hundreds of individuals have been trained in Internet governance and digital policy. The shift towards a more mature phase would require a stronger focus on organisational development, by ensuring sustained participation in policy processes. This includes developing the organisational capacities of governments, civil society, business associations, and academia in developing countries. Organisational and system-level capacity development are becoming particularly relevant in dealing with issues such as cybersecurity.

Research on capacity development in general and experience from the Internet governance field lead towards the following highlights:

- While the Internet is a global facility, Internet policy is often very local. It is shaped by local cultural and social specificities (e.g. cultural sensitivity for content, relevance of privacy protection). Thus, capacity development should follow local dynamics, taking into consideration local political, social, cultural, and other specific conditions in developing and implementing capacity development programmes and activities.

- The urgency for capacity development could be addressed by providing just-in-time learning as a part of policy processes. Some elements of this approach are used by DiploFoundation and the GIP, in just-in-time training programmes for diplomats, as well as by ICANN, in its Fellowship Programme,[29] and the Internet Society, in its IGF Ambassadors Programme.[30]

- The growing need for capacity in the digital policy field has to be addressed at a more systemic level, by including Internet governance and related topics in the curriculum of academic postgraduate studies.

- Genuine and sustainable empowerment can be achieved through holistic capacity development on individual, organisational, system, and network levels, as visualised in the capacity development butterfly (Figure 22).

www.igbook.info/capacitydevelopment

Endnotes

[1] Two such studies are World Bank (2016) World Development Report 2016: Digital Dividends. Available at http://www.worldbank.org/en/publication/wdr2016 [accessed 29 October 2016], and Alliance for Affordable Internet (2016) The 2015-2016 Affordability Report. Available at http://a4ai.org/affordability-report/report/2015/ [accessed 5 November 2016].

[2] United Nations General Assembly (2002) Resolution A/56/183. World Summit on the Information Society. Available at http://www.itu.int/net/wsis/docs/background/resolutions/56_183_unga_2002.pdf [accessed 27 October 2016].

[3] United Nations General Assembly (2000) Resolution A/55/L.2. United Nations Millennium Declaration. Available at http://www.un.org/millennium/declaration/ares552e.htm [accessed 27 October 2016].

[4] United Nations (no date) Millennium Development Goals. Available at http://www.un.org/millenniumgoals/ [accessed 27 October 2016].

[5] United Nations General Assembly (2015) Resolution A/70/1. Transforming our world: the 2030 Agenda for Sustainable Development. Available at http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E [accessed 27 October 2016].

[6] United Nations General Assembly (2015) Resolution A/70/125. Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society. Available at http://workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf [accessed 27 October 2016].

[7] For more information on the connections between the SDGs and the Internet, refer to *GIP Digital Watch* observatory (no date) Sustainable Development Goals and the Internet. Available at http://digitalwatch.giplatform.org/processes/sustainable-development-goals [accessed 11 August 2016].

[8] UNCTAD (no date) Information and Communication Technology for Development. Available at http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D.aspx [accessed 27 October 2016].

[9] WSIS Forum (2015) WSIS-SDG Matrix: Linking WSIS Action Lines with Sustainable Development Goals. Geneva: International Telecommunications Union. Available at https://www.itu.int/net4/wsis/sdg/Content/wsis-sdg_matrix_document.pdf [accessed 27 October 2016].

[10] For more details on the discussions held at the 2015 and 2016 editions of the WSIS Forum, refer to *GIP Digital Watch* observatory (no date) WSIS Forum 2015. Available at http://digitalwatch.giplatform.org/events/wsis-forum-2015 [accessed 28 October 2016]; and *GIP Digital Watch* observatory (no date) WSIS Forum 2016. Available at http://digitalwatch.giplatform.org/events/wsis-forum-2016 [accessed 28 October 2016].

[11] World Bank (2016) World Development Report 2016: Digital Dividends. Available at http://www.worldbank.org/en/publication/wdr2016 [accessed 29 October 2016].

[12] OECD (2001) Understanding the Digital Divide. p. 5. Available at http://www.oecd.org/internet/ieconomy/1888451.pdf [accessed 27 October 2016].

[13] Internet World Stats (2016) Digital Divide Gap is Getting Smaller. Available at http://internetworldstats.com/wp/digital-divide-gap-is-getting-smaller/ [accessed 30 October 2016].

[14] WEF (2016) Global Information Technology Report. Available at https://www.weforum.org/reports/the-global-information-technology-report-2016 [accessed 27 October 2016].

[15] European Union (2014) Universal Service. Available at https://ec.europa.eu/digital-single-market/universal-service [accessed 27 October 2016].

[16] European Commission (2016) Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code. Available at https://ec.europa.eu/digital-single-market/en/news/proposed-directive-establishing-european-electronic-communications-code [accessed 28 October 2016].

[17] United Nations (2011) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. Available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf [accessed 28 October 2016]. For a discussion on the UN report, refer to Wagner A (2012) Is Internet access a human right? *The Guardian*, 11 January. Available at https://www.theguardian.com/law/2012/jan/11/is-internet-access-a-human-right [accessed 28 October 2016].

[18] Internet Society (2012) Promoting the Use of Internet Exchange Points (IXPs): A Guide to Policy, Management and Technical Issues. Available at https://www.internetsociety.org/sites/default/files/Promoting%20the%20use%20of%20IXPs.pdf [accessed 5 November 2016].

[19] South Eastern European Dialogue on Internet Governance (2016) SEEDIG's contribution to the IGF 2016 Inter-sessional Programme on Policy Options for Connecting and Enabling the Next Billion – Phase II. Available at http://www.seedig.net/wp-content/uploads/2016/09/SEEDIG-contribution-to-IGF-CENB-II.pdf [accessed 28 October 2016].

[20] Berkman Center for Internet & Society, Harvard Law School (2003) BOLD 2003: Development and the Internet, Part 4: Solutions in the Architecture. Available at http://cyber.law.harvard.edu/bold/devel03/modules/modIC.html [accessed 28 October 2016].

[21] Huston G (2005) Where's the Money? Internet Interconnection and Financial Settlement. *The ISP Column*, January 2005, Internet Society, pp. 7–9. Available at http://www.potaroo.net/isp-col/2005-01/interconn.pdf [accessed 27 October 2016].

[22] The ITU-D Recommendation D.50, as well as its supplements, are available at http://www.itu.int/rec/T-REC-D.50/e [accessed 11 August 2016].

[23] United Nations (2015) Addis Ababa Action Agenda of the Third International Conference on Financing for Development. Available at http://www.un.org/esa/ffd/publications/aaaa-outcome.html [accessed 28 October 2016].

[24] World Bank (2016) World Development Report 2016: Digital Dividends. Available at http://www.worldbank.org/en/publication/wdr2016 [accessed 29 October 2016].

[25] Infocomm Development Authority of Singapore (no date) NEU PC Plus Programme. Available at https://www.imda.gov.sg/community/consumer-education/digital-inclusion/neu-pc-plus-programme [accessed 15 August 2016].

[26] Swiss Agency for Development and Cooperation (2006) Glossary Knowledge Management and Capacity Development. Available at https://www.eda.admin.ch/dam/deza/en/documents/publikationen/glossar/157990-glossar-wissensmanagement_EN.pdf [accessed 5 November 2016].

[27] Swiss Agency for Development and Cooperation (2006) Capacity Development in SDC. Available at https://www.eda.admin.ch/content/dam/deza/en/documents/die-deza/strategie/202114-capacity-development-sdc_EN.pdf [accessed 5 November 2016].

[28] Diplo's capacity development activities include Internet Governance Capacity Building Programme; online courses on Internet governance, cybersecurity, and technical infrastructure; MA in Contemporary Diplomacy with a specialisation in Internet Governance. More recently, as operator of the GIP, Diplo provides just-in-time training for permanent missions.

[29] ICANN (no date) ICANN Meeting Fellowships. Available at https://www.icann.org/fellowship-program [accessed 7 November 2016].

[30] Internet Society (no date) IGF Ambassadors Programme. Available at http://www.internetsociety.org/what-we-do/education-and-leadership-programmes/next-generation-leaders/igf-ambassadors-programme [accessed 7 November 2016].

Section 7

THE SOCIOCULTURAL BASKET

The sociocultural basket

The Internet has had a considerable impact on the social and cultural fabric of modern society. It is difficult to identify any segment of our social life that is not affected by the Internet. It introduces new patterns of social communication, breaks down language barriers, and creates new forms of creative expressions – to name but a few of its effects. Today, the Internet is as much a social phenomenon as it is a technological one.

Content policy

One of the main sociocultural issues is content policy, often addressed from the standpoints of government policies (content control measures imposed by various considerations, ranging from national security and morality and public order, to politically motivated forms of censorship), human rights (the impact of content policies on rights such as freedom of expression and the right to communicate), and technology (tools for content control). Discussions usually focus on three groups of content.

- Content that has a global consensus for its control. Included here are child sexual abuse-related content, justification of genocide, and incitement to or organisation of terrorist acts.

- Content that is sensitive for certain countries, regions, or ethnic groups due to their particular religious and cultural values. Globalised online communication poses challenges for local, cultural, and religious values in many societies. Most content control in Middle Eastern and Asian countries, for example, is officially justified by the protection of specific cultural values. This often means that access to pornographic and gambling websites is blocked.

- Political censorship on the Internet, often to silence political dissent and usually under the claim of protecting national security and stability.[1]

How content policy is conducted

An à la carte menu for content policy contains the following legal and technical options, which are used in different combinations.

Governmental filtering of content

Governments that filter access to content usually create an Internet Index of websites blocked for citizen access. Technically speaking, filtering utilises mainly router-based IP blocking, proxy servers, and DNS redirection. Filtering of content occurs in many countries. In addition to the countries usually associated with these practices, such as China, Saudi Arabia, and Singapore, other countries are increasingly implementing filtering measures as well.[2]

Private rating and filtering systems

Faced with the potential risk of the disintegration of the Internet through the development of various national barriers (filtering systems), W3C and other like-minded institutions made proactive moves proposing the implementation of user-controlled rating and filtering systems. In these systems, filtering mechanisms can be implemented by software on personal computers or at server level controlling Internet access.

This possibility allows users in different countries and cultures to implement their own filtering systems, obviating the need for national intervention which could provoke fragmenting of the Internet into national or culturally filtered blocks. It remains to be seen whether governments will trust their citizens to carry out the filtering states deem necessary. This is likely to be an additional user-customised resource, rather than replace systematic government filtering.

Government content control on religious grounds in specific countries is well known, but filtering on religious grounds may also be applied or advocated by specific organisations. For example, in 1998, a software package was reportedly distributed by the Scientology movement to its members. Critics dubbed the software 'Scieno sitter' and claimed that it prevented access to websites critical of Scientology.[3] Other examples could potentially affect entire populations: for example, the Australian Christian Lobby lobbied the Australian government to impose an opt-out filtering system which would block 'adult content' content in Australian homes and on mobile devices.[4]

Content filtering based on geographical location

Another technical solution related to content is geo-location software, which filters access to particular web content according to the geographic or national origin of users. The Yahoo! case was important in this respect, since the group of experts involved, including Vint Cerf, indicated that in 70–90% of cases, Yahoo! could determine whether sections of one of its websites hosting Nazi memorabilia were accessed from France.[5] This assessment helped the court come to a final decision, which requested Yahoo! to filter access from France to Nazi memorabilia. Since the 2000 Yahoo! case, the precision of geo-location has increased further through the development of highly sophisticated geo-location software.

Content control through search engines

The bridge between the end-user and web content is usually a search engine. Filtering of search results is therefore also used as a tool to prevent access to specific content. Such filtering is often implemented by search engines to comply with governmental policies. One notable example is that of Google in China. In 2006, Google decided to launch a local version of its search engine (google.cn) that was intended to comply with Chinese government policies regarding the filtering of online content deemed objectionable. In 2010, the company changed its approach by redirecting searches performed on Google.cn to its Hong Kong-based servers (which were free from filtering). This led to tension with the government, which, in the end, determined Google to close its operations in China.[6]

Filtering of search results is not implemented only from the governmental sphere; commercial interests may interfere as well, more or less obviously or pervasively. Commentators have started to question the role of search engines in mediating user access to information and to warn about their power of influencing users' knowledge and preferences.[7] This issue is increasingly attracting the attention of governments, which call for more transparency

from Internet companies regarding their practices. As an example, in a speech made in October 2016, German chancellor Angela Merkel called on Internet companies to make publicly available information regarding the algorithms they employ in their search engines. Such information, Merkel said, would allow users to better understand how and on what basis the information they receive via search engines is presented to them. The chancellor concluded: 'Algorithms, when they are not transparent, can lead to a distortion of our perception, they can shrink our expanse of information.'[8]

Web 2.0 challenge: user-generated content

With the development of Web 2.0 platforms – blogs, forums, document-sharing websites, and social media – the difference between the user and the creator has blurred. Internet users have become creators of large portions of web content, such as blog posts, videos, and photo galleries. Identifying, filtering, and labelling 'improper' websites is becoming a complex activity. While automatic filtering techniques for texts are advanced, automatic recognition, filtering, and labelling of visual content are still in the development phase.

One approach sometimes taken by governments in their attempts to deal with user-generated content that they deem objectionable is to completely block access to platforms such as YouTube and Twitter throughout the country. This maximalist approach, however, results in unobjectionable content, including educational material, being blocked. A more extreme measure is that of cutting Internet access completely to hinder communication via social network platforms (as was the case, for example, during the Arab Spring events[9]).

As the debate of what can and cannot be published online is becoming increasingly mature, social media platforms themselves have started to formalise their policies of where they draw the border between content that should or should not be tolerated. For example, Facebook's Statement of Rights and Responsibilities specifies: 'We can remove any content or information you post on Facebook if we believe that it violates this statement or our policies.'[10] However, the implementation of such policies sometimes leads to unintended consequences, with platforms removing legitimate content.

Automated content control

For Internet social media companies, it is difficult to identify illegal content among millions of video, sound, and textual content inputs. One possible solution to this challenge could be based on the use of AI mechanisms. One example of the potential of AI in this field is Conversation AI – a tool developed by Google-initiated start-up Jigsaw, with the aim of detecting hate speech and other forms of verbal abuse and harassment online.[11] As of October 2016, the software, which relies on Google's powerful data technology, is in the testing phase. However, relying on machine learning to make decisions as to what constitutes hate speech opens many questions, such as whether such systems would be able to differentiate between hate speech and irony and sarcasm.

Legal and policy instruments in content control

Content, in the form of writing and verbal expression, has always been in the focus of public policy. Societies decide what is acceptable and unacceptable content based on political, security, and religious considerations. Policies range from encouraging freedom of expression to imposing censorship. The Internet has entered this sensitive policy field

by making dissemination of information and content much easier than before. Thus, we are confronted with a paradoxical situation characterised, on the one hand, by a heavily regulated content policy field and, on the other hand, by a legal vacuum regarding the applicability of traditional content policy to the Internet.

National level

The legal vacuum in the field of online content policy provides legal uncertainty. National regulation in this field could bring a more predictable legal situation, and ensure better protection of human rights such as freedom of expression and freedom of information. In addition, legal rules could reduce the high level of discretion that governments enjoy in content policy. The business sector, in particular ISPs and Internet companies, could also benefit by avoiding ambiguous situations when they have to decide on content policy issues.

As the border between justified content control and censorship is very vague and thus difficult to enshrine in legislation, the tension is increasingly being resolved in the courtroom. For example, several social media outlets were sued in May 2016 for allowing racist and homophobic content on their platforms.[12] Furthermore, following attacks in Paris in November 2015 and in Israel between 2014 and 2016, social media outlets have been accused of providing a platform for terrorists 'to communicate, recruit members, plan and carry out attacks, and strike fear in their enemies',[13] in addition to facilitating the spread of terrorist propaganda.[14]

International initiatives

In response to terrorist threats, and the increased sophistication with which terrorists manage their activities and promote their ideologies online, multilateral forums have started addressing ways to limit harmful content. For example, the G7 leaders agreed to 'enhance efforts to counter the threat posed by terrorist groups exploiting the Internet and social media for terrorist purposes'.[15] Furthermore, the UN Security Council has requested its Counter-Terrorism Committee to propose guidelines and good practices to counter terrorists' use of the Internet to promote their narratives and recruit others.[16] More concretely, the UNODC published a report on the use of the Internet for terrorist purposes.[17]

Refer to Section 3 for further discussion on countering the distribution of terrorist propaganda and violent extremism materials online.

At regional level, the main regulatory initiatives have arisen in European countries with strong legislation in the field of hate speech, including anti-racism and anti-Semitism. European regional institutions have attempted to impose these rules on cyberspace. The primary legal instrument addressing the issue of content is the CoE 2003 Additional Protocol to the Convention on Cybercrime,[18] concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. On a more practical level, in 2012, the EU adopted the European Strategy to Make the Internet a Better Place for Children. Under this strategy, several activities and programmes have been implemented, targeted at awareness raising, fighting illegal content, introducing filtering and content labelling, working with civil society on child online safety issues, and creating a database of information on the use of technology by children.[19]

The OSCE is also active in this field. Since 2003, it has organised a number of conferences and meetings with a particular focus on freedom of expression and the potential misuses

of the Internet (e.g. racist, xenophobic, and anti-Semitic propaganda, and content related to violent extremism and radicalisation that lead to terrorism).

The issues

Content control and freedom of expression

Content control is often seen as a possible restriction of freedom of expression. Many societies worldwide are trying to address this sensitive area by promoting freedom of expression, while allowing exceptional and publicly justified content control. This is especially important in the USA, where the First Amendment guarantees broad freedom of expression, even the right to publish Nazi-related and similar materials.

Freedom of expression largely shapes the US position in the international debate on content-related issues on the Internet. For example, while the USA has signed the Cybercrime Convention, it cannot sign the Additional Protocol to this convention, dealing with hate speech and content control. The question of freedom of expression was also brought up in the context of the Yahoo! court case. In its international initiatives, the USA will not step beyond the line which may endanger freedom of expression as stipulated in the First Amendment.

Illegal offline – illegal online

As with human rights, the dominant view is that rules of the offline world apply to the Internet when it comes to content policy.

One of the arguments of the cyber approach to Internet regulation is that quantity (intensity of communication, number of messages) makes a qualitative difference. In this view, the problem of hate speech is not that no regulation against it has been enacted, but that the sharing and spreading through the Internet makes it a different kind of legal problem. More individuals are exposed and it is difficult to enforce existing rules. Therefore, the difference that the Internet brings mainly relates to problems of enforcement, not to the rules themselves.

Refer to Section 4 for further discussion on the cyberlaw approach to Internet regulation.

The effectiveness of content control

In discussions on Internet policy, one of the key arguments is that the decentralised nature of the Internet can bypass censorship. In countries with government-directed content control, technically gifted users have found ways around such control (e.g. accessing filtered content through VPNs, or making the content available at a different location than the one to which access is blocked). Moreover, experts have warned that filtering measures can also have negative consequences at a technical level. Blocking at the DNS level can, for example, conflict with the adoption of DNSSEC, and it could also promote the fragmentation of the Internet.[20]

Who should be responsible for content policy?

The main players in the area of content control are parliaments and governments. Most often, they apply core constitutional principles to what content should be controlled and

how. ISPs, as Internet gateways, are commonly held responsible for implementation of content filtering, either according to government prescriptions or to self-regulation (at least regarding issues of broad consensus, such as child pornography). Some groups of users, such as parents, are keen to introduce a more efficient content policy to protect children. Various rating initiatives help parents to find child-friendly content. New versions of Internet browser software usually include many filtering options.

Internet companies (such as Facebook, Google, and Twitter) are becoming *de facto* content regulators. Google, for example, has had to decide on more than half million requests for removal of links from search results, based on the right to be forgotten.

Refer to Section 4 for further discussion on online content-related dispute resolution mechanisms implemented by Internet companies.

Such companies are also increasingly involved in cooperative efforts with public authorities in an attempt to combat illegal online content. In an illustration of this trend, technology companies in Silicon Valley had several meetings with US authorities over the course of 2016, discussing opportunities of cooperation on matters related to online content control, especially in relation to terrorism-related content.[21] In the EU, IT companies have worked together with the European Commission on a Code of Conduct on illegal online hate speech, which includes a series of commitments to fight the dissemination of online hate speech in Europe.[22]

www.igbook.info/contentpolicy

Online education

The Internet has opened new possibilities for education. Online/e-learning initiatives use the Internet as a medium for the delivery of courses to participants around the world. At the same time, e-learning is used to support the delivery of face-to-face learning in traditional settings such as universities, leading to blended learning. While it cannot replace traditional education, e-learning provides new possibilities, especially when constraints of time and space impede physical attendance in class. Recently, online education has been linked to higher-education reform, as well as institutional and organisational changes.[23]

Traditionally, education has been governed by national institutions. The accreditation of educational institutions, the recognition of qualifications, and quality assurance are all governed at national level. However, cross-border education requires the development of new governance regimes. Many international initiatives aim to fill the governance gap, especially in areas such as quality assurance and the recognition of academic degrees.

The issues

WTO and education

One controversial issue in the WTO negotiations is the interpretation of Articles I (3)(b) and 3(c) of the GATS, which specify exceptions from the free trade regime for government-provided services. According to one view, supported mainly by the USA and the

UK, these exceptions should be treated narrowly, *de facto* enabling free trade in higher education. This view is predominantly governed by interests of the English-speaking educational sector to gain global market coverage in education, and has received considerable opposition from many countries.[24]

One of the key aspects of the debate focuses on the question of whether education should be considered a commodity or a public good. If education is considered a commodity, the WTO's free trade rules will be implemented in this field as well. A public goods approach, on the other hand, would preserve the current model of education in which public universities receive special status as institutions of importance for national culture. Online education could also be affected by trade liberalisation. Some commentators have warned about a possible 'trade creep' in education policy.[25]

Quality assurance and standardisation

The availability of online learning delivery systems and easy entry into this market has opened the question of quality assurance. A focus on the technical aspects of online delivery can overlook the importance of the quality of materials and didactics. A variety of possible difficulties can endanger the quality of education. One is the easy market entry of new, mainly commercially driven educational institutions, which frequently have few of the necessary academic and didactical capabilities. Another problem of quality assurance is that the simple transfer of existing paper-based educational materials to an online medium does not take advantage of the specific didactic potential of the new medium. This aspect has prompted education organisations to start to develop standards and guidelines for evaluating the design and the content of courses delivered online.[26]

The recognition of academic degrees and the transfer of credits

Recognition of degrees has become particularly relevant within the online learning environment. When it comes to online learning, the main challenge is the recognition of degrees at regional and global level.

The EU has developed a regulatory framework with the European Credit Transfer and Accumulation System (ECTS).[27] The Asia-Pacific region has introduced its own regional model for the exchange of students and a related credit system – the University Mobility in Asia and the Pacific (UMAP) programme.[28]

In the evolving implementation of online learning, there is a tendency towards recognition and transfer of credits following traditional strategies for bricks-and-mortar universities.

The innovation of Massive Open Online Courses (MOOCs) is also evolving, as the initial pervasive acceptance and hype cycle have run their course, and resources are being developed to provide the same or better personal interactions that are provided in traditional or blended learning educational systems.

The standardisation of online learning

The early phase of online learning development was characterised by rapid development and high diversity of platforms, content, and didactics. However, there is a need to develop common standards to facilitate the recognition of credits or other qualifications, and to ensure minimal quality. Most standardisation is performed by private and professional institutions.

ICT, education, and development

The SDGs include an ambitious goal which calls for inclusive and equitable quality education and ensuring lifelong learning opportunities for all (Goal 4). Achieving this goal can be linked to several WSIS action lines, as shown in the WSIS-SDGs matrix.[29] This further underscores the importance of ICT for education.

www.igbook.info/onlineeducation

Cultural diversity

Cultural diversity is a broad concept, and can include diversity of language, national identities, traditions, and religions. The relation between the Internet and cultural diversity, in its various forms, is two-fold. On the one hand, the Internet can contribute to the promotion of cultural diversity at a global level, through its ability to facilitate both exchanges between individuals with different cultural backgrounds, and access to vast resources of information and knowledge. The Internet also offers individuals new possibilities to express themselves in ways that reflect their national and cultural identities. On the other hand, and as underlined during WSIS, cultural diversity is essential to the development of an inclusive information society that is based on dialogue and respect among cultures.

In the online environment, the preservation, enhancement, and promotion of cultural diversity can be achieved, among others, through encouraging the development of local content. As local content has the potential to reflect national identities and cultural specificities, having more local content online translates into additional opportunities for making the Internet a more diverse and inclusive space, and for promoting these exact identities and specificities at a global level.

The translation, adaptation, and online distribution of existing local content, and the preservation of varied information reflecting indigenous knowledge and traditions through digital means represent other forms of promoting cultural diversity. Digital archives can also contribute to strengthening local communities, and documenting and preserving local heritage. This is particularly relevant for communities that are isolated or nomadic, whose technological needs might require approaches that are entirely localised. The production and distribution of software in local languages also has the potential to increase the rates of Internet adoption.

www.igbook.info/culturaldiversity

Multilingualism

Since its early days, the Internet has been a predominantly English-language medium. According to some statistics, a little over 50% of web content is in English,[30] whereas 75% of the world's population does not speak English.[31] At the same time, Chinese – which is the world's most spoken language – only accounts for about 2% of all content. A report released by the UN Broadband Commission in 2015 reveals that only about 5% of the world's estimated 7100 languages are currently represented on the Internet. It also notes that the use of the Latin script remains a challenge for many Internet users, in particular for reading domain names.[32]

Figure 23. Multilingualism

This situation has prompted many countries to take concerted action to promote multilingualism and to protect cultural diversity. The promotion of multilingualism (Figure 23) is not only a cultural issue; it is directly related to the need for the further development of the Internet. If the Internet is to be used by wider parts of society, content must be accessible in more languages.

Although the English language is still over-represented on the web, this is slowly starting to change. As increasingly more people are getting online, some languages are becoming increasingly prominent. For example, between 2011 and 2015, Russian-language content has reportedly grown with 41.5%, Spanish with 15.5%, and Portuguese with 56%.[33] The rapid increase in Indian and Chinese users might similarly lead to a growing Hindi and Chinese online language base.

The issues

Non-Latin alphabets

The promotion of multilingualism requires technical standards that facilitate the use of the various alphabets, scripts, and characters. One of the early initiatives related to the multilingual use of computers was undertaken by the Unicode Consortium – a non-profit institution that develops standards to facilitate the use of character sets for different languages. ICANN and the IETF took an important step by introducing IDN TLDs (both for ccTLDs and gTLDs).

IDNs facilitate the use of domain names written in non-Latin alphabets (such as Chinese, Arabic, Cyrillic), as well as with Latin-alphabet-based characters with diacritics or ligatures (present in languages such as French, German, Hungarian, Romanian, etc.).[34]

Refer to Section 2 for further discussion on IDNs.

IDNs contribute to making the Internet more inclusive, as the possibility of accessing and registering domain names in more languages and scripts empowers more people to use the Internet. Domain names are not only about addressing and naming, but also about content. They are therefore relevant for local communities, and they have the potential to encourage the use and the development of local content, in local languages and scripts.

Machine translation

Many efforts have been made to improve machine translation. Given its policy of translating all official activities into the languages of all member states, the EU has supported various development activities in the field of machine translation. Although major breakthroughs (involving, for example, the use of AI systems) have been made, limitations remain.

With growing market opportunities in non-English-speaking countries, Internet companies have also started to provide machine translation tools on their platforms. For example, Facebook and Instagram provide automatic translations of user-generated content.

Appropriate governance frameworks

The promotion of multilingualism requires appropriate governance frameworks. The first element of governance regimes has been provided by organisations such as UNESCO, which has instigated many initiatives focusing on multilingualism, including the adoption of important documents, such as the 2001 Universal Declaration of Cultural Diversity.[35] Another key promoter of multilingualism is the EU, since it embodies multilingualism as one of its basic political and working principles.[36]

The evolution and wide usage of Web 2.0 tools, allowing ordinary users to become contributors and content developers, offers an opportunity for greater availability of local content in a wide variety of languages. Nevertheless, without a broader framework for the promotion of multilingualism, this opportunity might result in an even greater gap, since users feel the pressure to use a common language (usually English) to reach a bigger audience.

Meaningful access

The need for linguistic and cultural diversity on the Internet is also an important topic connected to access and development. The availability of local content, provided in local languages, gives people an incentive to get online. At the same time, it allows people to express themselves online in their own languages and generate content. As a result, local content can make the Internet more inclusive and help bridge the digital divide.

www.igbook.info/multilingualism

Global public goods

There have been numerous efforts to define and protect the Internet as global and public facility. Global public good is the most frequently used concept in addition to *res communis omnium*, global commons, and the common heritage of mankind. These concepts are used interchangeably or with considerable overlapping. The Internet as a global public good is defined by two approaches: economic – as a resource that is non-rivalrous and non-excludable in its use; security – as a global infrastructure beyond national sovereignty.

Economic approach

The economic approach to the Internet as a global public good is based on two characteristics: non-rivalrous (consumption by one does not detract from that of another) and non-excludable (it is difficult, if not impossible, to exclude an individual from enjoying the good). Following these criteria, the World Bank[37] argues that the Internet is an imperfect public good since it has just one of the characteristics of a public good. Namely, the Internet is non-rivalrous, as its use by one person does not reduce its availability to others. The Internet does not fulfil the other main characteristic – non-excludability – as the use of Internet is typically subject to a fee, in one form or another.

However, the Internet is not a unified entity. It has many aspects. Thus, the status of global public good could be applied to overall access to Internet, use of knowledge and data on the Internet, use of Internet standards, access to online education, etc.

One of the key features of the Internet is that through the worldwide interaction of users, new knowledge and information are produced. Considerable knowledge has been generated through exchanges on mailing lists, social networks, and blogs. Except for Creative Commons,[38] there is no mechanism to facilitate the legal use of such knowledge. Left in a legal uncertainty, it is made available for modification and commercialisation. This common pool of knowledge, an important basis of creativity, is at risk of being depleted. The more Internet content is commercialised, the less spontaneous exchanges may become. This could lead to reduced creative interaction.

The concept of global public goods, combined with initiatives such as Creative Commons, could provide solutions that would both protect the current Internet creative environment and preserve Internet-generated knowledge for future generations.

Security approach

The security approach aims to protect the global Internet infrastructure, by considering it a global public good. According to this approach, the Internet as a global public good should be – in particular – protected from the intervention of national governments. Proponents of this approach often make an analogy between the open sea and the Internet.

Refer to Section 1 for further discussion on analogies.

Typically, the security approach covers the DNS, routing, and Internet protocols as global public goods.[39] Internet standards (mainly TCP/IP) are open and public. The Internet governance regime, it is argued, should ensure protection for the main Internet standards as global public goods.

The balance between private and public interests

One of the underlying challenges of the future development of the Internet is to strike a balance between private and public interests. The question is how to provide the private sector with a proper commercial environment while ensuring the development of the Internet as a global public good. In many cases, it is not a zero-sum game but a win-win situation. Many Internet companies have tried to develop business models which provide income and enable the creative development of the Internet.

Private companies predominate in running the Internet infrastructure. One of the resulting challenges is the harmonisation of the private ownership of the Internet infrastructure with the status of the Internet as a global public good. National laws provide the possibility of private ownership being restricted by certain public requirements, including providing equal rights to all potential users and not interfering with the transported content.

www.igbook.info/publicgoods

Endnotes

1 Freedom House publishes annual *Freedom on the Net* reports, which look, among other issues, at whether/how governments around the world implement censorship policies. Freedom House (no date) About Freedom on the Net. Available at https://freedomhouse.org/report-types/freedom-net [accessed 2 November 2016].

2 The OpenNet Initiative collects, analyses, and publishes data on Internet filtering and surveillance practices performed in countries around the world. It provides country profiles, regional overviews, and interactive maps, accessible via its website https://opennet.net/ [accessed 2 September 2016].

3 Operation Clambake (no date) Church of Scientology Censors Net Access for Members. Available at http://www.xenu.net/archive/events/censorship/ [accessed 29 October 2016].

4 Taylor J (2013) Australian Christian Lobby urges Coalition rethink on Internet filtering. *ZDNet*, 6 September. Available at http://www.zdnet.com/article/australian-christian-lobby-urges-coalition-rethink-on-internet-filtering/ [accessed 29 October 2016].

5 Although Vint Cerf participated in the panel, he objected to the final report, which he said 'did not focus on the flaws or the larger implications of installing online gates'. Source: Guernsey L (2001) Welcome to the world wide web, passport, please? *New York Times,* 15 March 2001. Available at http://www.nytimes.com/2001/03/15/technology/welcome-to-the-web-passport-please.html?pagewanted=all&src=pm [accessed 29 October 2016].

6 Waddell K (2016) Why Google Quit China – and Why It's Heading Back. *The Atlantic*, 19 January. Available at http://www.theatlantic.com/technology/archive/2016/01/why-google-quit-china-and-why-its-heading-back/424482/ [accessed 5 September 2016].

7 A good starting point to this debate is Mary Murphy's blog post on DiploFoundation's Internet Governance blog channel and the comments raised upon: *Google...stop thinking for me!* Available at https://www.diplomacy.edu/blog/googlestop-thinking-me [accessed 29 October 2016].

8 Connolly K (2016) Angela Merkel: Internet search engines are distorting perception. *The Guardian*, 27 October. Available at https://www.theguardian.com/world/2016/oct/27/angela-merkel-internet-search-engines-are-distorting-our-perception [accessed 30 October 2016].

9 Crete-Nishihata M and York J (2011) Egypt's Internet Blackout: Extreme Example of Just-in-time Blocking. OpenNet Initiative. Available at https://opennet.net/blog/2011/01/egypt's-internet-blackout-extreme-example-just-time-blocking [accessed 29 October 2016].

10 Facebook (2015) Statement of Rights and Responsibilities. Available at https://www.facebook.com/terms [accessed 14 July 2016].

11 Greenberg A (2016) Inside Google's Internet justice league and its AI-powered war on trolls. *Wired*, 9 September. Available at https://www.wired.com/2016/09/inside-googles-internet-justice-league-ai-powered-war-trolls/ [accessed 30 October 2016].

12 Chazan D (2016) Facebook, YouTube and Twitter sued for 'failure to remove homophobic content'. *The Telegraph*, 15 May. Available at http://www.telegraph.co.uk/news/2016/05/15/facebook-youtube-and-twitter-sued-for-failure-to-remove-homophob/ [accessed 14 July 2016].

13 Williams D (2016) Relatives of Palestinian attack victims sue Facebook for $1 billion in U.S. *Reuters*, 11 July. Available at http://www.reuters.com/article/us-israel-palestinians-facebook-idUSKCN0ZR1G0 [accessed 14 July 2016].

14 *BBC* (2016) Twitter, Facebook and Google 'aided Paris attacks'. 16 June 2016. Available at http://http://www.bbc.com/news/technology-36548798 [accessed 14 July 2016].

15 G7 (2016) G7 Action Plan on Countering Terrorism and Violent Extremism. Available at http://www.mofa.go.jp/files/000160278.pdf [accessed 18 August 2016].

[16] UN News Centre (2016) Security Council requests UN panel to propose global framework on countering terrorist propaganda. 11 May. Available at http://www.un.org/apps/news/story.asp?NewsID=53909#.V7VzGWW5oQF [accessed 18 August 2016].

[17] UNODC (2012) *The use of the Internet for terrorist purposes*. Vienna: United Nations Office at Vienna. Available at https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf [accessed 18 August 2016].

[18] Council of Europe (2003) Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Available at http://conventions.coe.int/Treaty/en/Treaties/html/189.htm [accessed 29 October 2016].

[19] European Commission (2015) From a Safer Internet to a Better Internet for Kids. Available at https://ec.europa.eu/digital-single-market/safer-internet-better-internet-kids [accessed 29 October 2016].

[20] For details on the various implications of content filtering, consult: ICANN Security and Stability Advisory Committee (2012) SSAC Advisory on Impacts of Content Blocking via the Domain Name System. Available at https://www.icann.org/en/system/files/files/sac-056-en.pdf [accessed 5 September 2016], and Barnes A *et al*. (2016) Technical Considerations for Internet Services Blocking and Filtering (Internet Architecture Board RFC 7754). Available at https://tools.ietf.org/html/rfc7754 [accessed 5 September 2016].

[21] Yadron D and Wong JC (2016) Silicon Valley appears open to helping US spy agencies after terrorism summit. *The Guardian*, 8 January. Available at https://www.theguardian.com/technology/2016/jan/08/technology-executives-white-house-isis-terrorism-meeting-silicon-valley-facebook-apple-twitter-microsoft [accessed 18 August 2016].

[22] European Commission (2016) European Commission and IT companies announce Code of Conduct on illegal online hate speech. Available at http://europa.eu/rapid/press-release_IP-16-1937_en.htm [accessed 18 August 2016].

[23] Willcox K *et al*. (2016) Online Education: A Catalyst for Higher Education Reform. Massachusetts Institute of Technology. Available at https://professional.mit.edu/sites/default/files/MIT%20Online%20Education%20Policy%20Initiative%20April%202016.pdf [accessed 18 August 2016].

[24] For a comprehensive study of the interpretation of GATS related to higher education, refer to Tilak J (2011) *Trade in higher education: The role of the General Agreement on Trade in Services (GATS)*. Paris: UNESCO, International Institute for Educational Planning. Available at http://unesdoc.unesco.org/images/0021/002149/214997e.pdf [accessed 29 October 2016].

[25] Knight J (2015) Trade creep: Implications of GATS for higher education policy. *International Higher Education* 28, pp. 5–7. Available at http://ejournals.bc.edu/ojs/index.php/ihe/article/view/6658 [accessed 29 October 2016].

[26] For a sample list of organisations and works dealing with recommendations and standards for e-learning, refer to WBTIC (no date) Overview of E-learning Standards. Available at http://wbtic.com/primer_standards.aspx [accessed 29 October 2016].

[27] European Commission (no date) ECTS. Available at http://ec.europa.eu/education/tools/ects_en.htm [accessed 29 October 2016].

[28] UMAP (no date) UMAP. Available at http://umap.org/about/ [accessed 29 October 2016].

[29] WSIS Forum (2015) WSIS-SDG Matrix: Linking WSIS Action Lines with Sustainable Development Goals. Geneva: International Telecommunication Union. Available at https://www.itu.int/net4/wsis/sdg/Content/wsis-sdg_matrix_document.pdf [accessed 27 October 2016].

[30] W3Techs (2016) Usage of content languages for websites. Available at https://w3techs.com/technologies/overview/content_language/all [accessed 29 October 2016].

[31] British Academy Policy Centre (2011) Language Matters More and More. Available at http://www.ucml.ac.uk/sites/default/files/pages/160/Language%20Matters%20more%20and%20more.pdf [accessed 29 February 2016].

[32] The Broadband Commission for Digital Development (2015) The State of Broadband 2015: Broadband as a Foundation for Sustainable Development. Available at http://www.broadbandcommission.org/Documents/reports/bb-annualreport2015.pdf [accessed 18 August 2016].

[33] Wood J (2015) Top languages of the Internet, today and tomorrow. *Unbabel*, 10 June. Available at https://unbabel.com/blog/top-languages-of-the-internet/ [accessed 15 July 2016].

[34] For an overview of the IDN programme, as well as updates regarding its implementation, consult ICANN (no date) Internationalized Domain Names. Available at https://www.icann.org/resources/pages/idn-2012-02-25-en [accessed 29 October 2016].

[35] UNESCO (2001) Universal Declaration on Cultural Diversity. Available at http://portal.unesco.org/en/ev.php-URL_ID=13179&URL_DO=DO_TOPIC&URL_SECTION=201.html [accessed 29 October 2016].

[36] European Commission (no date) Multilingualism. Available at http://ec.europa.eu/languages/index_en.htm [accessed 29 October 2016].

[37] World Bank (2016) World Development Report 2016: Digital Dividends. Available at http://www.worldbank.org/en/publication/wdr2016 [accessed 29 February 2016].

[38] Creative Commons is a non-profit organisation that develops, supports, and stewards legal and technical infrastructure that maximizes digital creativity, sharing, and innovation. Available at http://creativecommons.org/ [accessed 29 October 2016].

[39] Broeders D (2015) *The Public Core of the Internet*. Amsterdam: Amsterdam University Press. Available at http://www.wrr.nl/fileadmin/en/publicaties/PDF-Rapporten/The_public_core_of_the_internet_Web.pdf [accessed 31 October 2016].

Section 8

THE HUMAN RIGHTS BASKET

The human rights basket

The basic set of Internet-related human rights includes privacy; freedom of expression; the right to seek, receive, and impart information; various rights protecting cultural, linguistic, and minority diversity; and the right to education. Other human rights come into place in the realm of digital policy, such as children's rights, and those rights afforded to journalists and the press.

While human rights are usually explicitly addressed (e.g. freedom of expression and online privacy), they are also involved in cross-cutting issues that appear when dealing with net neutrality (the right to access, freedom of expression, anonymity), cybersecurity (observing human rights while carrying out cybersecurity and protection activities), content control, etc.

Online vs offline human rights

UNGA and UNHRC resolutions, as well as similar documents adopted within regional organisations such as the CoE and the EU, have firmly established the principle that the same human rights that people enjoy offline must also be protected online. The Association for Progressive Communications (APC) underlines, in the Internet Rights Charter, that Internet-related human rights are embedded in the UN human rights system based on the UDHR and other related instruments.[1]

While the question of offline vs online rights has been settled in principle, the implementation of offline regulation in the online space raises further challenges. Those who suggest that online rights require a specific approach argue that the sheer quantity of communication facilitated by the Internet (i.e., intensity of communication, number of messages) makes a qualitative difference. For example, the issue with hate speech is not the question of whether or not regulation against it has been enacted, but that the ease of sharing and spreading hate speech through the Internet makes it a different kind of legal problem. As more individuals are exposed to hate speech via numerous online platforms, it becomes increasingly difficult to enforce existing rules against hate speech. Therefore, while the existing rules are appropriate, the Internet brings challenges related to enforcement.

Technology and human rights

Technical standards and protocols affect the exercise of human rights. Infrastructure providers, device manufacturers, and standards bodies all have a role to play in defining the protections embedded in the technical layer of the Internet. Encryption mechanisms and protocols such as 'Do Not Track' can set the protection of privacy and freedom of expression as a default.

At the DNS level, controversies arose, for example, with the release of the .sucks top-level domain, approved by ICANN in February 2015. Some have criticised this development for its extortionary potential (paying premiums to acquire a second-level domain name of the type [brand].sucks), while others have regarded it as a space for the exercise of freedom of expression.[2] This and other similar concerns have led to intensive discussions within the

ICANN community on whether ICANN, as a technical organisation *per se,* should have human-rights-related obligations. The 2016 ICANN bylaws incorporate human rights among the core values that should guide ICANN's decisions and actions: ICANN is to respect 'internationally recognised human rights as required by applicable law'. It is, however, underlined that this core value does not create any obligation on ICANN outside its mission (which is 'to ensure the stable and secure operation of the Internet's unique identifier systems') or beyond obligations found in applicable law.[3]

'New' human rights enabled by the Internet

The right to access

Estonia was the first country to legally guarantee the right to access the Internet through a universal service legislation, in 2000. In July 2010, Finland gave its citizens a legal right to a 1Mbps broadband connection (the speed was doubled to 2 Mbps from November 2015). Other countries have taken similar steps towards guaranteeing their citizen's right to access the Internet.[4] Opinions still differ regarding a firm worldwide recognition of access to the Internet as a human right. Some argue that access to the Internet cannot have the same relevance as access to clean water, food, and other basic needs. Others argue that this is a false dilemma, since access to the Internet is often crucial for ensuring fulfilment of other basic human rights.

Net neutrality and zero-rating have brought the right to access into public focus worldwide. What type of Internet access do we mean, when we speak of a right to access? Should access to a limited number of websites and platforms, such as that provided by toll-free applications, be considered access to the Internet? The Indian government response to this question was negative, when it banned zero-rating services. Other countries are debating this issue. It remains to be seen which of the following angles will dominate the discussion on zero-rating: human rights (right to access), economic (emerging business model), or development (assistance to underserved communities).

The right to be forgotten

The right to be forgotten, or more precisely the right to be de-indexed, was introduced by the CJEU landmark case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. The case regarded a notice of auction published by the Spanish newspaper *La Vanguardia* for Mr Costeja's property due to unpaid debts in 1998. Although Mr Costeja had settled his debts many years before, once the newspaper digitised its archives, any Google search on his name would point to that notice of auction among its first results. The Spanish court of first instance decided that the newspaper archive should not be altered to no longer display this information: it was considered an issue of freedom of the media. However, the Spanish Data Protection Authority (*Agencia Española de Protección de Datos*) required that Google should remove the link to this information. Google challenged this in front of the highest national court (*Audiencia Nacional*), which referred the case to the CJEU.

On 13 May 2014, the CJEU ruling against Google proceeded as follows: First, it asserted its jurisdictional competence by establishing that the search engine activities of the Spanish subsidiary of Google Inc. – headquartered in the USA and owning the search algorithm – were 'economically profitable' and they fell under the territorial scope of application of EU Data Protection Directive 95/46. Second, it determined that Google was a data controller (an entity processing

data) as its activity consisted of 'finding information published or placed on the Internet by third parties, indexing it automatically, storing it temporarily and finally, making it available to Internet users according to a particular order of preference.' Third, it required Google to comply with the Data Protection Directive as controller in the territory of an EU member state, in order to 'remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful'.[5] The Court also recognised that when the public interest is at stake, the data controller needs to assess whether to continue to make available a particular link.

Through this process, the CJEU introduced a new approach which relies on the processing of data according to the location of the user, independent of server location or company headquarters.[6] This was a bone of contention in the months following the CJEU judgement, coming into sharper focus with an order of the Paris *Tribunal de Grande Instance* in favour of global applicability, forcing Google to move from de-indexing results from its sub-domains within the EU (google.it, google.fr) to removing links from google.com when accessed from Europe.[7]

Moreover, the EU went one step further, enshrining the right to be forgotten in legislation, with the adoption of the General Data Protection Regulation (replacing the 1996 Directive).[8] The Regulation, which is to become applicable starting May 2018, contains specific provisions on the 'right to erasure (right to be forgotten)', saying that individuals have the right to obtain the erasure of their personal data on several grounds, and that the controller has the obligation to erase such data without undue delay. In addition, if the controller has made the personal data public, it is also required to take 'reasonable steps' to inform controllers processing the respective data that the data subject has requested the erasure of any links to, or copy or replication of, those personal data.

The regulation of the right to be forgotten has given rise to two opposing views: some see it as an enhancement of the right to privacy and data protection, in that it defines a process through which users can ask for the erasure of the data collected and stored by Internet companies. Others see it as a possible threat to freedom of expression, if the legal provisions are implemented in such a way that they allow content to be erased even if it does not violate someone else's rights.[9] It remains to be seen how the legal provisions will be implemented and which of the two views will prevail.

www.igbook.info/hr

The Internet and existing human rights

Freedom of expression and the right to seek, receive, and impart information

Online freedom of expression has featured high on the diplomatic agenda in the last few years; it is, for example, on the agenda of the UNHRC, as well as of regional intergovernmental bodies such as the CoE. Freedom of expression on the Internet has also been discussed at numerous international conferences and processes, including the IGF.

One of the most comprehensive approaches is provided by the Freedom Online Coalition (a group of 30 governments, as of November 2016), which hosts annual meetings and undertakes research and awareness raising activities on freedom of expression on the Internet.

The discussion on online freedom of expression has been a contentious policy area. It is one of the fundamental human rights, usually appearing in the context of discussions on governmental content control, censorship, and surveillance. In addition, the issue of freedom of expression is complicated by some current approaches towards the proliferation of hate speech and extreme views on the Internet, with arguments being brought both in favour and against measures aimed at limiting free speech in such instances.[10] Nonetheless, there seems to be a trend towards limiting free speech in favour of social responsibility.[11]

Online freedom of expression also spans several other Internet-governance-related issues such as encryption and anonymity, net neutrality, and IPR. Some of these aspects have been analysed in reports issued by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, who has emphasised on numerous occasions that the right to freedom of expression online deserves strong protection. Freedom of expression also appears in broader discussions on human rights and access to Internet.

Freedom of expression is protected by global instruments, such as the UDHR (Article 19) and the UN International Covenant on Civil and Political Rights (Article 19), and regional instruments such as the European Convention on Human Rights (Article 10) and the American Convention of Human Rights (Article 13).

In the UDHR, freedom of expression is counterbalanced by the right of the state to limit freedom of expression for the sake of morality, public order, and general welfare (Article 29). Thus, both the discussion and implementation of Article 19 must be viewed in the context of establishing a proper balance between two needs.[12] This ambiguous situation opens many possibilities for different interpretations of norms and ultimately different implementations. The controversy around the right balance between Articles 19 and 29 in the real world is mirrored in discussions about achieving this balance on the Internet.

The main governance mechanism for addressing online freedom of expression is the UNHRC Resolution on Protection of Freedom of Expression on the Internet (2012).

Freedom of expression is the focus of human rights NGOs such as Human Rights Watch, Amnesty International, and Freedom House. Freedom House, for example, evaluates the level of Internet freedom experienced by average users in sample countries around the world. Its Freedom on the Net 2016 study noted that Internet freedom worldwide has declined for the sixth consecutive year, and over half of the 65 countries assessed were on a negative trajectory, driven by actions such as censorship and restrictions on the use of certain Internet services, arrests of social media users, broad surveillance, and shutting down of all Internet access in particular instances.[13]

www.igbook.info/foe

Privacy and data protection[14]

Privacy and data protection are relevant to several Internet governance baskets: human rights, infrastructure (developing standards for data management), security (access to data for protection of national security and the fight against crime), and economy (processing data as a basis for a business model).

Privacy and data protection are two interrelated Internet governance issues. Privacy is usually defined as the right of citizens to control their own personal information and to decide whether or not to disclose it. Data protection is a legal mechanism that ensures privacy. Privacy is a fundamental human right. It is recognised in the UDHR, the International Covenant on Civil and Political Rights, and in many other international and regional human rights conventions.

National cultures and different ways of life influence the practice of privacy. Privacy is particularly important in Western societies, with Germans, for example, assigning high relevance to privacy. Modern practices of privacy focus on communication privacy (no surveillance of communication) and information privacy (no handling of information about individuals). Traditionally, privacy concerns related to government surveillance. Increasingly, however, privacy issues relate to infringements by the business sector as well.

The issues

The main privacy issues can be analysed using a triangle among individuals, states, and businesses, as presented in Figure 24.

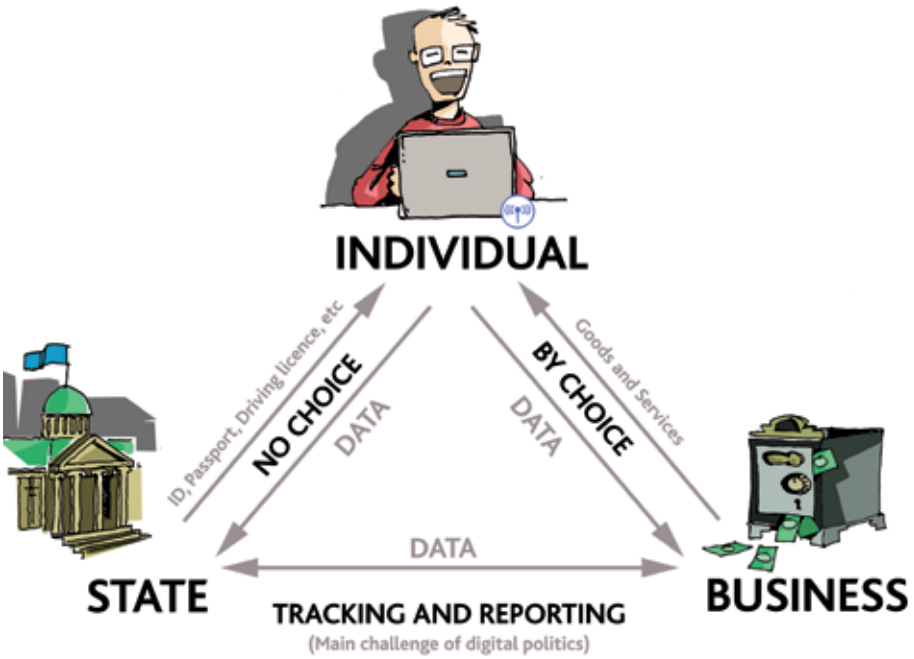

Figure 24. Privacy in the digital age

Privacy protection: individuals and states

Information has always been an essential tool for states to exercise authority over their territories and populations. Governments collect vast amounts of personal information (birth and marriage records, social security numbers, voting registration, criminal records, tax information, housing records, car ownership, etc.). It is not possible for an individual to opt out of providing personal data to the state, short of emigrating to another country, where they would confront the same request for data. Information technology, such as that used in data mining,[15] aids in the aggregation and correlation of data from many specialised systems (e.g. taxation, housing records, car ownership) to conduct sophisticated analyses, searching for usual and unusual patterns and inconsistencies (Figure 25).

One of the main challenges of e-government initiatives is to ensure a proper balance between the modernisation of government functions and the guarantee of citizens' privacy rights, including restricting the collection of information to what is strictly necessary to perform the government's legitimate functions and to provide public services. However, recent years have witnessed an increased appetite of governments for collecting data, and the association of more personal data for compulsory identification (such as biometric data).

After the events of 11 September 2001 in the USA, the US Patriot Act,[16] and comparable legislation in other countries, broadened government authority to collect information, including a provision for lawful interception of information. The concept of lawful interception in gathering evidence is also included in the CoE Convention on Cybercrime (Articles 20 and 21).

Privacy protection: individuals and businesses

As depicted in the privacy triangle (Figure 24), the second, and increasingly important relationship is that between individuals and the business sector. Individuals disclose personal data when opening a bank account, booking a flight or hotel, paying online with a credit card, or even browsing or searching the Internet: each of these activities may leave multiple traces of data.

Figure 25. Data mining

The success and sustainability of electronic commerce, both business-to-customer and business-to-business, depend on the establishment of trust in both business privacy policies and the security measures they establish to protect clients' confidential information from theft and misuse. With the expansion of social network platforms (e.g. Facebook, Twitter), concerns arise over the eventual misuse of personal data – not only by the owner or administrator of a social network platform, but also by other individuals using it.[17] Moreover, Internet companies tend to change their privacy policies often, and not leave users much choice besides the usual 'take it or leave it approach' (when users can either accept the privacy policy as such, or choose not to use the service).[18]

In an information economy, data about customers, including their preferences and purchase profiles, become an important market commodity. For some companies, such as Facebook, Google, and Amazon, information about customers' preferences constitutes a cornerstone of their business model. Basically, the currency that users pay for (online) services rendered 'for free' is personal data, whether in the form of a browser cookie indicating their online behaviour or specific information requested in filling in a webform or making a payment. As users reveal more information about themselves, privacy violations become more frequent and more sophisticated.[19]

Privacy protection: states and businesses

The third side of the privacy triangle is the least publicised, yet perhaps the most significant privacy issue.

Both states and businesses collect considerable amounts of data about individuals. States put a lot of pressure on Internet business companies (e.g. Facebook, Google) to grant access to data to support their anti-terrorist and anti-criminal activities. As an example, after the Paris terrorist attacks in November 2015, the French government relied heavily on data provided by the Internet industry. Similarly, governments are increasingly concerned about stronger encryption used by the Internet industry, which makes the surveillance of Internet traffic more difficult.

The business sector is trying to resist governmental pressure and limit access by state authorities to their data. If government authorities gain access to business data, this can reduce the level of trust among Internet users and affect the business model of Internet companies. This tension between state authorities and the business sector will continue be one of the underlying issues in global digital policy in the forthcoming period.

Privacy protection: individuals and individuals

The last aspect of privacy protection, not visualised in the privacy triangle, is the potential risk to privacy coming from individuals. Today, anyone with sufficient funds may own powerful surveillance tools. Even a simple mobile phone equipped with a camera can become such a tool. Technology has 'democratised surveillance', to quote *The Economist*.[20] Many instances of the invasion of privacy have occurred, from voyeurism to the sophisticated use of cameras for recording card numbers in banks and for economic espionage.

The main problem for protection from this type of privacy violation is that most legislation focuses on the privacy risks stemming from the state or from private companies. Faced with this new reality, a few governments have taken some initial steps. US Congress adopted the Video Voyeurism Prevention Act, prohibiting the taking of photos of unclothed people without their permission.[21] Germany and a few other countries have adopted similar privacy laws, aimed at preventing individual surveillance.

The international regulation of privacy and data protection

One of the main international instruments on privacy and data protection is the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981.[22] Although it was adopted by a regional organisation (CoE), it is open for accession by non-European states. Since the Convention is technology neutral, it has withstood the test of time.

The 1995 EU Data Protection Directive[23] has also formed an important legislative framework for the processing of personal data in the EU and has had a huge impact on the development of national legislation not only in Europe but also globally. Following a reform process to cope with new developments and to ensure effective privacy protection in the current technological environment, a new General Data Protection Regulation was adopted in 2016, which will become applicable from May 2018, thus replacing the 1995 Directive.[24]

Another key international – but non-binding – document on privacy and data protection is that of the OECD Guidelines on Protection of Privacy and Transborder Flows of Personal Data from 1980, updated in 2013.[25] These guidelines, and the OECD's subsequent work, have inspired many international, regional, and national regulations on privacy and data protection. Today, virtually all OECD countries have enacted privacy laws and empowered authorities to enforce those laws.

While the principles of the OECD guidelines have been widely accepted, there are differences in how they are implemented, notably between Europe and the USA. In Europe, there is comprehensive data protection legislation, while in the USA, privacy regulation has been developed for each sector of the economy including financial privacy (the Graham-Leach-Bliley Act), children's privacy (the Children's Online Privacy Protection Act), and medical privacy (under the Health Insurance Portability and Accountability Act).

Another major difference is that, in Europe, privacy legislation is enforced by public authorities, while in the USA, enforcement principally rests on the private sector and self-regulation. Businesses set their own privacy policies, and other businesses and individuals are responsible for informing themselves and acting accordingly. The main criticism of the US approach is that individuals are placed in a comparatively weak position, as they are seldom aware of the importance of options offered by privacy policies and commonly agree to them without informing themselves.

Privacy Shield between the USA and the EU

The different US and EU approaches to privacy protection have raised questions mainly related to the processing of personal data by private companies. How can the EU ensure that data about its citizens are protected according to the rules specified in its data protection regulations? Do EU or US rules apply when handling data transferred through a company's network from the EU to the USA? The EU threatened to block the transfer of data to any country that could not ensure the same level of privacy protection as spelled out in its legal framework. This request inevitably led to a clash with the US self-regulation approach to privacy protection.

This deep-seated difference made any possible agreement more difficult to achieve. Moreover, adjusting US law to EU data protection law would not have been possible since it would have required changing a few important principles of the US legal system. The

breakthrough in the stalemate occurred in 1998 when US Ambassador David L. Aaron suggested a 'Safe Harbour' formula. This reframed the whole issue and provided a way out of the impasse in the negotiations.

The Safe Harbour provided a legal framework for exchange of data across the Atlantic Ocean. It attempted to ensure that EU citizens' data were protected according to EU rules even if the data were located on servers based in the USA. The agreement allowed EU regulations to be applied to US companies inside a legal 'safe harbour'. US companies handling EU citizens' data could voluntarily sign up to observe the EU's privacy protection requirements. Once subject to the agreement, they had to observe the formal enforcement mechanisms agreed on between the EU and the USA. Under the Safe Harbour Framework, over 4400 companies legally transferred data from the EU to the USA for 15 years.

However, in October 2015, the CJEU invalidated the Safe Harbour Framework, considering that the European Commission had not appropriately evaluated whether the USA maintains 'essentially equivalent' protection of EU citizens' data.[26] This decision triggered negotiations between EU and US diplomats in search for a new mechanism. These negotiations resulted in the Privacy Shield, approved by EU member states in July 2016, with four countries abstaining – Austria, Bulgaria, Croatia, and Slovenia. Later that month, the European Commission formally adopted a decision confirming the adequacy of the EU-USA Privacy Shield.[27]

The Shield imposes stronger obligations on US companies to protect EU citizens' personal data, and requires the US government to more robustly enforce the new provisions and monitor their implementation. In addition, the Privacy Shield also addresses one issue that has presented a major area of concern: the US government's access to the personal data of EU citizens. The Shield brought in written assurances from the USA that any such access would be subject to appropriate limitations, safeguards, and oversight mechanisms. The US government has also committed to cooperating with data protection authorities in the EU, as well as to creating an Ombudsperson mechanism for receiving and responding to complaints from individuals regarding US government access to their personal data.

www.igbook.info/privacy

Children's rights in the digital world

The Internet brings many benefits for children, and at the same time, many risks. Promoting such benefits while fostering a safe and secure online environment requires a careful balance between safeguarding children against the risks, and respecting children's digital rights, including the right to access information and freedom of speech.

Refer to Section 3 for further discussion on the security aspects of children's use of the Internet.

The United Nations Convention on the Rights of the Child (CRC)[28] is considered the cornerstone of children's rights. The CRC is one of the most widely ratified international human rights treaties: to date, every UN member state has ratified the CRC, with the notable exception of the USA.

The CRC recognised for the first time that children are people who have human rights. The Convention is based on four foundation principles:

- Children should be free from discrimination.
- Policies should be based on the best interests of children.
- Children should be allowed and encouraged to develop to their full potential.
- Children's views and perspectives are important and need to be heard.

It also tackles the rights of children according to three broad spheres – provision, protection, and promotion (or participation) – commonly referred to as the '3 Ps'.

The challenges

Protectionist approaches

Child online protection tends to focus on the protective aspect of children's use of technology. In fact, many argue that the Internet and technology have increased the risks for children, and therefore children can reap the benefits only if the risks are mitigated. However, policies which focus exclusively on online risks can sideline the Internet's potential to empower children.

A rights-based approach, based on children's rights as enshrined in legal instruments such as the CRC, aims to maximise the opportunities of the digital world for children and young people while protecting them from risks. Since this approach strikes a more careful balance between children's digital rights and their need for protection, it is increasingly favoured by experts.

Applicability of the CRC to the online world

The CRC, which was unanimously adopted in 1989, was formulated before the mass adoption of the Internet. Does the CRC apply to the online world, and how?

The 2012 UNHRC's Resolution on the promotion, protection and enjoyment of human rights on the Internet[29] ended the debate on whether existing human rights apply online or whether a new set of rights is needed for the online environment. Experts agree that while this was a significant achievement, greater steps were needed regarding children's rights, which require special protection.[30]

In particular, the CRC offers a consensual guide to the principles and ideals of meeting children's rights offline, and can also offer the same protection online, if it is appropriately developed. The CRC therefore needs to be translated into a clear set of guidelines.[31]

While the CRC carries the mandate for governments to act in the best interests of children, it also provides the point of departure from which a range of policies and measures can be formulated.

www.igbook.info/children

Rights of persons with disabilities[32]

According to World Health Organization (WHO), around 1 billion people in the world live with disabilities.[33] This number is increasing due to population aging; emergence of new diseases; chronic health conditions; armed conflict and violence; poverty and unhealthy living conditions; and the absence of knowledge about disability, its causes, prevention, and treatment.[34]

The Internet provides new possibilities for the social inclusion of people with disabilities. To maximise technological possibilities for people with disabilities, there is a need to develop the necessary Internet governance and policy framework. The main international instrument in this field is the Convention on the Rights of Persons with Disabilities (UNCRPD), adopted by the UN in 2006, which establishes rights that are now in the process of being included in national legislation, which will make them enforceable.[35]

Awareness of the need for technological solutions that include people with disabilities is increasing with the work of organisations that teach and foster support for the disabled community, such as the IGF Dynamic Coalition on Accessibility and Disability,[36] the Internet Society Disability and Special Needs Chapter, and the International Center for Disability Resources on the Internet.

Accessibility challenges for people with disabilities arise from the gap between the abilities required to use hardware, software, and content, and the available resources and abilities of a person with a disability. To narrow this gap, policy actions take two directions:

- Include accessibility standards in the requirements for the design and development of equipment, software, and online content.
- Foster the availability of accessories in hardware and software that increase or substitute the functional capabilities of the person with disabilities.

In the field of Internet governance, the main focus is on online content and applications and their suitability for being accessed and used by people with disabilities. International standards in web accessibility are developed by W3C within its Web Accessibility Initiative. Despite the existence of such standards, many online applications still do not comply with them, due to various reasons, such as lack of awareness or perceived complexity and high costs.

www.igbook.info/disabilities

Gender and human rights online

Women's rights online include a wide-ranging set of issues related to both access to the Internet (e.g. online violence), and lack of access (e.g. loss of opportunity when it comes to access to information, education, business, and political activities).

Historically, girls and women have faced discrimination and major inequalities in education (including ICT specialisations), health, social welfare, political participation, and jus-

tice. Many of these disparities between men and women in the enjoyment of fundamental rights have been perpetuated online. Violence, migration, conflict, and crisis have also affected the wellbeing of women and their ability to fulfil their potential both offline and online, with important obstructions of their private sphere.

Women represent more than half of the world's population, yet their participation in technology-mediated processes is an area where progress is still needed. The protection of women's rights online is part of a broader sociocultural and professional shift focusing attention on reducing discrimination and diminishing bias in the exercise of rights, including for accessing educational and economic opportunities, holding office, and receiving equal pay.

While access to the Internet has increased over the last two decades, gendered patterns of use create uneven opportunities and generate important gaps in the empowerment of girls and women across the globe. ITU data for 2016 show that the global Internet user gender gap grew from 11% in 2013 to 12% in 2016 and remains largest (31%) where access is needed most: in the world's LDCs. The data also show that the regional gender gap is largest in Africa (23%) and smallest in the Americas (2%).[37]

According to a Web Foundation study, even improved access to mobile phones is not enough to get women online, or 'to achieve empowerment of women through technology'. The study showed that although most women and men own a phone, only 37% of the women are likely to access the Internet (about half the number of the men in the same communities), and women are 30–50% less likely to use the Internet for economic or political opportunities. Moreover, it showed that access is intrinsically linked to educational level, another factor to be considered in taking action for change.[38]

With strengthened online participation, women's involvement in public and political life has been on the rise, yet taking full advantage of the benefits of ICTs depends on eliminating a set of barriers such as inequality of access and technology-related violence against women. Among the acts of violence perpetrated via online means are cyberstalking, surveillance and privacy breaches, sexual harassment, and the unauthorised use and manipulation of personal information, including images and videos. In the era of ubiquitous connectivity, creating safer online spaces with the cooperation of Internet intermediaries comes into sharper focus as a first step towards the full realisation of women's human rights and development.

The 2016 report of the UN Special Rapporteur on violence against women, its causes and consequences, noted online violence against women as a new challenge. The report stated that 'while the use of information and communications technology has contributed to the empowerment of women and girls, its use has also generated online violence.' It called on states and non-state actors to 'fight online violence against women and girls while respecting freedom of expression and the prohibition of incitement to violence and hatred, in accordance with article 20 of the International Covenant on Civil and Political Rights'.[39]

The main international instruments for the protection of women's rights are the 1952 Convention on the Political Rights of Women and the 1979 Convention on the Elimination of All Forms of Discrimination against Women (CEDAW). Both UN Women and the UNHRC work actively on various dimensions of women's rights. However, mainstreaming the online facets of activities of existing women's rights bodies remains challenging. Groups such as APC and the IGF Dynamic Coalition on Gender and Internet Governance have been actively involved in advocacy for women's right online.

As the women's rights movement has matured, a move has been made to recognise that these are actually part of broader gender rights issues, which also cover the rights of other gender minorities. Human rights issues for women and other gender minorities, including the Lesbian, Gay, Bisexual, Trans and Queer (LGBTQ) community, comprise quality of access to information, professional opportunities, global policy processes, and other rights which are critical for human rights and Internet governance, and must be studied and addressed accordingly.

www.igbook.info/gender

Endnotes

[1] The APC Internet Rights Charter includes Internet access for all; freedom of expression and association; access to knowledge; shared learning and creation – free and open source software and technology development; privacy, surveillance, and encryption; governance of the Internet; awareness, protection, and realisation of rights. Available at http://www.apc.org/en/node/5677 [accessed 20 October 2016].

[2] Solon O (2015) Why the .sucks domain doesn't have to suck. *Bloomberg*, 19 August. Available at https://www.bloomberg.com/news/articles/2015-08-19/why-the-sucks-domain-doesn-t-have-to-suck [accessed 7 March 2016].

[3] ICANN (2016) Bylaws for Internet Corporation for Assigned Names and Numbers. Available at https://www.icann.org/resources/pages/governance/bylaws-en [accessed 7 October 2016].

[4] Borg-Psaila S (2011) Right to access the Internet: the countries and the laws that proclaim it. Available at https://www.diplomacy.edu/blog/right-access-internet-countries-and-laws-proclaim-it [accessed 20 October 2016].

[5] CJEU (2014) Judgement of the Court in Case C-131/12: Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Available at http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-131/12&td=ALL [accessed 20 October 2016].

[6] Radu R and Chenou JM (2015) Data control and digital regulatory space(s): towards a new European approach. *Internet Policy Review* 4(2). Available at http://policyreview.info/articles/analysis/data-control-and-digital-regulatory-spaces-towards-new-european-approach [accessed 20 October 2016].

[7] Bowcott O and Willsher K (2014) Google's French arm faces daily €1,000 fines over links to defamatory article. *The Guardian*, 13 November. Available at https://www.theguardian.com/media/2014/nov/13/google-french-arm-fines-right-to-be-forgotten [accessed 20 October 2016].

[8] European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Available at http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 [accessed 14 July 2016].

[9] For a more detailed overview of the possible implications of the right to be forgotten, read Keller D (2016) The new, worse 'right to be forgotten'. *Politico*, 27 January. Available at http://www.politico.eu/article/right-to-be-forgotten-google-defense-data-protection-privacy/ [accessed 14 July 2016].

[10] For an overview of reasons for restricting the expressions of extreme views, as well as arguments for allowing wider free speech, including outlying views, consult Heinze E (2014) Nineteen arguments for hate speech bans – and against them. Available at http://freespeechdebate.com/en/discuss/nineteen-arguments-for-hate-speech-bans-and-against-them/ [accessed 12 August 2016].

[11] Poushter J (2015) 40% of millennials OK with limiting speech offensive to minorities. Available at http://www.pewresearch.org/fact-tank/2015/11/20/40-of-millennials-ok-with-limiting-speech-offensive-to-minorities/ [accessed 12 August 2016].

[12] United Nations (1948) The Universal Declaration of Human Rights. Available at http://www.un.org/en/documents/udhr/ [accessed 20 October 2016].

[13] Freedom House (2016) Freedom on the Net 2016. Available at https://freedomhouse.org/report/freedom-net/freedom-net-2016 [accessed 16 November 2016].

[14] Valuable comments and input were provided by Katitza Rodriguez, International Rights Director at the Electronic Frontier Foundation (EFF).

[15] UCLA (no date) What is data mining? Available at http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm [accessed 20 October 2016].

[16] For details on the US Patriot Act, visit Electronic Privacy Information Centre (no date) USA Patriot Act. Available at http://epic.org/privacy/terrorism/hr3162.html [accessed 20 October 2016].

[17] The privacy focus and concern related to social networking sites are very well illustrated by the attentive monitoring and pressure exerted by media civil rights advocates on Facebook. For an overview of the wide range of privacy issues raised in relation to the use of this platform, refer to Wikipedia (2012) Criticism of Facebook. Available at http://en.wikipedia.org/wiki/Criticism_of_Facebook [accessed 20 October 2016].

[18] As an example, in August 2016, the Facebook-owned messaging service WhatsApp changed its privacy policy so that once the user accepts WhatsApp's Terms and Conditions, they automatically accept to share their data with Facebook directly – including for ad-targeting purposes. Opting out of the data-sharing entirely did not seem to be possible at the time the change was introduced, but WhatsApp offered a partial opt-out with regard to the use of data by Facebook for targeting purposes. For further details, consult Lamas N (2016) WhatsApp to share user data with Facebook for targeting – here's how to opt out. *Techcrunch*, 25 August. Available at https://techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out/ [accessed 20 October 2016].

[19] For an overview of the prominent privacy breaches over time, consult Lord N (2016) The History of Data Breaches. *Digital Guardian*, 12 October. Available at https://digitalguardian.com/blog/history-data-breaches [accessed 20 October 2016].

[20] *The Economist* (2004) Move over, Big Brother. 2 December. Available at http://www.economist.com/node/3422918 [accessed 30 October 2016].

[21] Gov.track.us (no date) Video Voyeurism Prevention Act. Available at https://www.govtrack.us/congress/bills/108/s1301/text [accessed 20 October 2016].

[22] Council of Europe (1981) Convention for the protection of individual with regard to automatic processing of personal data. Available at http://conventions.coe.int/treaty/en/treaties/html/108.htm [accessed 20 October 2016].

[23] European Union (1995) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046 [accessed 20 October 2016].

[24] European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Available at http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 [accessed 27 August 2016].

[25] OECD (2013) Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available at http://www.oecd.org/sti/ieconomy/privacy.htm [accessed 30 October 2016].

[26] CJEU (2015) Judgement of the Court in Case C-362/14: Maximilliam Schrems v Data Protection Commissioner. Available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2015 [accessed 21 October 2016].

[27] European Commission (2016) Commission Implementing Decision on the adequacy of the protection provided by the EU-U.S. Privacy Shield. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2016_207_R_0001 [accessed 21 October 2016].

[28] United Nations (1989) Convention on the Rights of the Child. Available at http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx [accessed 21 October 2016].

[29] UN Human Rights Council (2012) Resolution A/HRC/20/L.13. The promotion, protection and enjoyment of human rights on the Internet. Available at http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280 [accessed 21 October 2016].

[30] Livingstone S and Bulgar M (2014) A global research agenda for children's rights in the digital age. Journal of Children and Media 8(4). Available at http://www.lse.ac.uk/media@lse/WhosWho/AcademicStaff/SoniaLivingstone/pdf/Livingstone-&-Bulger-JOCAM-A-global-research-agenda-for-childrens-rights-in-the-digital-age.pdf [accessed 18 August 2016].

[31] For an analysis of how the CRC articles apply to the digital environment, refer to: Livingstone S and Bulgar M (2014), ibid, and Livingstone S and O'Neill B (2014). Children's rights online: Challenges, dilemmas and emerging directions. In S. van der Hof *et al.* (Eds) *Minding Minors Wandering the Web: Regulating Online Child Safety.* Berlin: Springer.

[32] Valuable comments and input were provided by Jorge Plano, professor at the National Technological University, Buenos Aires.

[33] World Health Organization (2015) Disability and Health. Fact sheet No. 352. Available at http://www.who.int/mediacentre/factsheets/fs352/en/ [accessed 21 October 2016].

[34] Disabled World (no date) Disability Statistics: Facts & Statistics on Disabilities & Disability Issues. Available at https://www.disabled-world.com/disability/statistics/ [accessed 21 October 2016].

[35] United Nations (2006) Convention on the Rights of Persons with Disabilities. Available at http://www.un.org/disabilities/convention/conventionfull.shtml [accessed 21 October 2016].

[36] The IGF Dynamic Coalition on Accessibility and Disability has developed a set of accessibility guidelines, which are available at http://www.intgovforum.org/cms/dynamiccoalitions/80-accessibility-and-disability#documents [accessed 10 August 2016].

[37] ITU (2016) ICT Facts and Figures 2016. Available at http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf [accessed 21 October 2016].

[38] Web Foundation (2015) Women's Rights Online: Translating Access into Empowerment. Available at http://webfoundation.org/about/research/womens-rights-online-2015/ [accessed 12 August 2016].

[39] United Nations (2016) Report of the Special Rapporteur on violence against women, its causes and consequences. Available at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/32/42 [accessed 7 November 2016].

Section 9

INTERNET GOVERNANCE ACTORS

Internet governance actors

Internet governance involves a wide variety of actors, or stakeholders, as they are often called, including national governments, international organisations, the business sector, civil society, and the academic and technical communities (as specified in paragraph 49 of the WSIS 2003 Declaration of Principles and in paragraphs 35 and 36 of the WSIS 2005 Tunis Agenda for the Information Society). While multistakeholderism is adopted as a governance principle in the WSIS documents, the main debate is on the specific roles and responsibilities of each actor, focusing mainly on the relationship between state and non-state actors in various areas of Internet governance.

Most Internet governance actors face a challenge in dealing with the high complexity of this field, characterised by the multidisciplinary nature of its issues, which involve technological, legal, economic, human rights, and sociocultural aspects, among others. In addition, Internet governance issues are addressed on different policy levels: local, national, regional, and global. This section provides a survey of the main Internet governance actors and a summary of their respective positions.

What is the conceptual difference between Internet governance and other global policy processes?

In Internet governance, governments had to enter an already existing non-governmental regime, built around the IETF, the Internet Society, and ICANN. In other policy areas (e.g. climate change, trade, migration), it has been the other way around. The intergovernmental policy space has been opening gradually to non-governmental actors. Since WSIS 2003, when many governments started entering the Internet governance scene, the main challenge has been to synchronise the existing non-governmental Internet governance regime and the traditional diplomatic one. This convergence has triggered the main controversies on the roles of governments and other actors in Internet governance, but also opportunities for creating more inclusive and effective policy-making.

Governments

The Internet, as the defining technology of the modern era, affects the geopolitics of states (centred on the question of national security), and, increasingly, their geoeconomics (defined as the promotion of national interests through economic means). The Internet also creates high levels of economic and social interdependence, which triggers the need for identifying policy solutions through negotiations and cooperation. Internet governance was introduced on the global diplomatic agenda in 2003–2005, during the WSIS process. Since then, many governments have been trying to grasp this complex policy field.

The critical relevance of the Internet for national societies worldwide has put additional pressure on governments to develop effective Internet governance at national level and to engage in Internet diplomacy efforts to protect their interests in the digital realm.

Governments' international efforts have been channeled in two main directions. Firstly, governments deal with the Internet, as a new policy issue, in a wide range of spaces, from multistakeholder ones, such as ICANN and the IGF, to multilateral ones, such as the ITU and the UN GGE (see, for example Table 3 showing governments' participation in the UN GGE). Secondly, governments have to deal with digital aspects of traditional policy issues such as trade (in the context of the WTO), health (WHO) and labour (ILO).

Even for large and wealthy countries, dealing with Internet governance issues has posed numerous challenges, such as management of the multidisciplinary nature of Internet governance (i.e., technological, economic, and social aspects) and the involvement of a wide variety of actors. Many governments have had to simultaneously train officials, develop policy, and actively participate in different international Internet-related meetings.

National coordination

In 2003, at the beginning of the WSIS process, most countries addressed Internet governance issues through telecommunications ministries and regulatory authorities – usually those that had been responsible for relations with the ITU, the main international organisation dealing with telecommunications issues. Gradually, with the growing impact of the Internet on the political, social, and economic fabric of modern society, other government departments have started being involved in Internet governance, including foreign affairs, culture, media, and justice.

The principal challenge for many governments has been to develop a strategy to gather and effectively coordinate support from non-state actors such as universities, private companies, and NGOs, that often have the necessary expertise to deal with Internet governance issues. In the years after WSIS 2003, most big and medium-sized G20 countries managed to develop sufficient institutional capacity to follow global Internet governance negotiations. Some of them, such as Brazil, have developed innovative national structures for following the Internet governance debate, involving telecommunications ministries, the diplomatic service, the business sector, civil society, and academia.[1] India, Indonesia, and Kenya are other examples of countries that have developed multistakeholder cooperation at national level. Many countries use national IGF initiatives as a way to engage the various stakeholder groups in Internet governance and digital policy processes. In October 2016, there were 47 national IGF initiatives recognised by the Secretariat of the global IGF.[2]

Policy coherence

Given the multidisciplinary nature of Internet governance and the great diversity of actors and policy forums, it is particularly challenging to achieve policy coherence. For example, the question of privacy and data protection is addressed from the human rights, trade, standardisation, and security perspectives, among others, but often with very little coordination among policy and expert groups dealing with each perspective (Figure 26). Achieving policy coherence in the field of Internet governance requires a flexible form of policy coordination, including horizontal communication between different ministries, the business sector, and other actors.

Apart from the management challenge, the achievement of policy coherence is usually limited by the existence of competing policy interests. This is especially true in countries with well-developed and diversified Internet economies. For example, at the beginning of

Cable geo-strategy and policy (in)coherence

The Anglo-French Entente[3] was established in 1904. In establishing close cooperation with Germany, however, the French Telegraph Ministry did not follow the country's foreign policy of preference for relations with Britain. The main reason for this was to reduce British dominance in the global cable geo-strategy while laying new telegraph cables in cooperation with Germany. In 1915, French historian Charles Lesage made the following comment on this policy (in)coherence: 'The prolonged disagreement between the general principles of French diplomacy and the procedures of the telegraphic policies come, I believe, from the fact that in this country, each ministry has its own foreign policy: the Ministry of Foreign Affairs has one, the Ministry of Finance has another... The Postal and Telegraph Administration also has, from time to time, a foreign policy; as it so happened, in these past few years, without being entirely hostile to England, it demonstrated a strong inclination to Germany.'[4]

the net neutrality debate, regulators in various countries tried to achieve a balance between the Internet industry, which supported net neutrality, and the telecommunication and entertainment sectors, which saw net neutrality as an obstacle to developing a new business model based on, for example, faster Internet(s) for delivery of multimedia content.

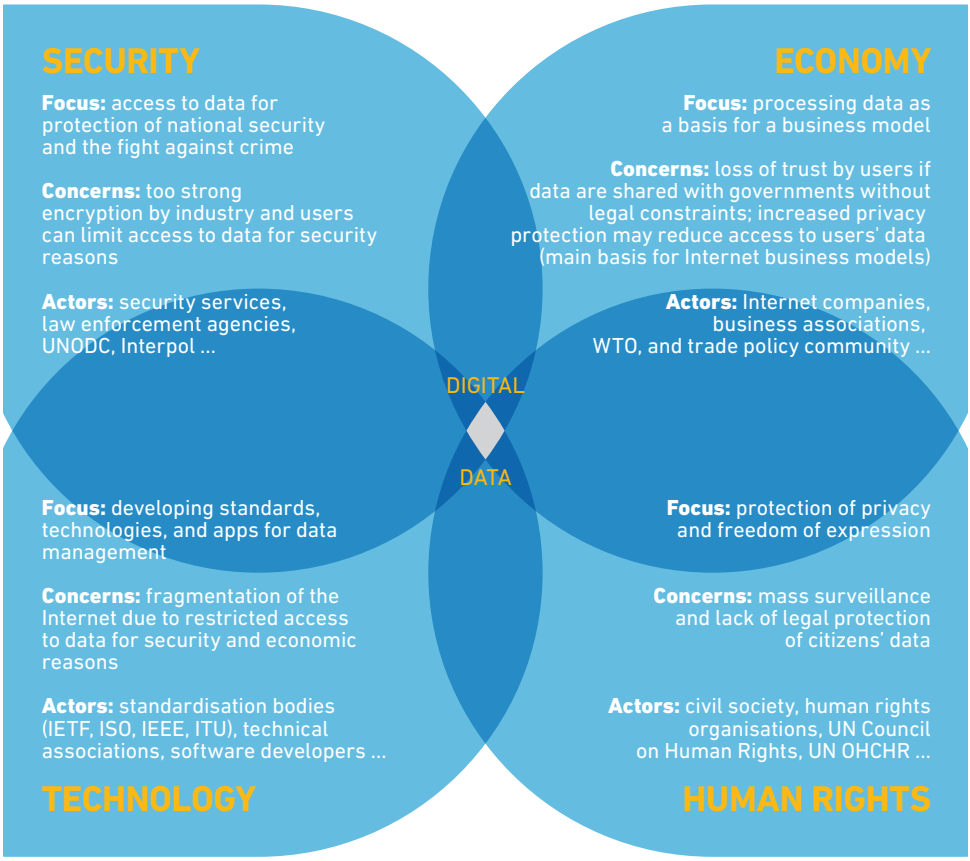

Figure 26. Bridging policy silos in the digital field

Role of Geneva-based permanent missions in Internet governance

For many governments, their permanent missions in Geneva have been important, if not vital, players in the WSIS and Internet governance processes. Many of the early Internet-governance-related activities were held in Geneva, home to the ITU, which took a leading role in the WSIS processes. The first WSIS phase took place in Geneva in 2003, where all but one of the preparatory meetings were held, keeping permanent missions based there directly involved. Currently, the IGF Secretariat is based in Geneva and many IGF preparatory meetings are organised there.

For large and developed countries, Geneva-based permanent missions have been part of the broad network of institutions and individuals that deal with the WSIS and Internet governance processes. For small and developing countries, permanent missions have been the primary and, in some cases, the only players in the processes. Internet governance issues have added to the agenda of the usually small and over-stretched missions of developing countries. In many cases, the same diplomat must undertake tasks associated with Internet governance processes, along with other issues such as human rights, health, trade, and labour.

Position of national governments

United States

The Internet was developed as part of a US-government-sponsored scientific project. From the origin of the Internet until today, the US government has been involved in Internet governance through different departments and agencies: initially, the Department of Defense, later the National Science Foundation, and most recently the Department of Commerce. The FCC has also played an important role in creating the Internet regulatory framework.

One constant of US government involvement has been its hands-off approach, usually described as a 'distant custodian'. It sets the framework, while leaving the governance of the Internet to those directly working with it, mainly the technical community. However, the US government has intervened more directly on a few occasions, as occurred in the mid-1990s when the non-profit Council of Registrars (CORE) project might have moved the root server and management of the core Internet infrastructure from the USA to Geneva.[5] This process was stopped by a famous (at least in the history of the Internet) diplomatic note sent by US Secretary of State Madeleine Albright to the ITU Secretary General.[6] In parallel to stopping the CORE initiative, the US government initiated consultations that resulted in the establishment of ICANN, in 1998. ICANN was entrusted, by the US government, with the role of performing the IANA functions, i.e., coordinate the Internet's systems of unique identifiers (mainly the DNS and IP numbers). The US government retained a stewardship role over the IANA functions up to October 2016, when this role was transitioned to the global Internet community.

Its well-developed online space and vibrant Internet industry make the USA particularly vulnerable to cybersecurity attacks. Thus, US diplomacy is very active in international cybersecurity negotiations. The USA supports the concept that existing security norms, such as the right to self-defence, should also be applied to the Internet. The country opposes the adoption of a global cybersecurity treaty. The USA is party to a wide range of regional and bilateral cybersecurity agreements. The USA deals with international cybercrime via the CoE Convention on Cybercrime, as well as via bilateral agreements, including MLATs. The USA also supports the development of cybersecurity structures, by, for example, establishing or strengthening existing CERTs.

On economic issues, the USA supports the free flow of data, as well as the free trade with digital services. Free online trade is promoted in the WTO and through various regional and bilateral trade agreements. The US Internet industry is the main beneficiary of free online trade, with the free flow of data as a critical aspect. The country opposes the taxation of online transactions.

European Union

The European Union has a unique mix of hard and soft digital power for forging future Internet governance compromise. The EU's hard digital power is based on the attraction of a 500-million-person market with both high Internet penetration (79.3% in 2015)[7] and purchasing power. As the concentration of the Internet industry lobby in Brussels shows, this type of hard power matters. By negotiating with the EU on anti-monopoly and data protection issues, Google and Facebook, among others, negotiate with the rest of the world (the EU's arrangements with the Internet industry often inspire other countries and regions to take similar action). In a situation where, for example, Google has a share of over 90% of the online search market in the European Economic Area, the EU is positioned as the main entity that could ensure that Google's high market penetration in Europe is not misused through practices involving abuse of the company's dominant market position.[8]

The EU's soft digital power is based on some sort of digital aikido diplomacy of turning weaknesses into strengths. While the EU does not have a strong Internet industry, this weakness could, paradoxically, be turned into a strength in Internet governance.

Namely, without the need to protect the economic interests of the Internet industry, the EU has more freedom to promote and protect public interests (user rights, inclusion, content diversity). In this way, the EU can become the guardian of 'Internet users', and the promoter of an enabling environment for the growth of the EU's Internet industry. The EU could achieve both ethical and strategic goals, which is not often the case in international politics.

An EU approach of developing different issue-based alliances has begun to emerge. At WCIT-12, Europe supported the USA. On data protection and privacy, the EU's position is close to the position of the Latin American countries. Switzerland and Norway have a similar position to the EU on most Internet governance issues.

In the forthcoming period, the EU's position in Internet governance will be further shaped by the development of the EU Digital Single Market, in particular in areas such as taxation, customer protection, and the free of flow of data.

EU member states have been putting emphasis on specific Internet governance issues, developing their niche areas. Germany and Austria are particularly concerned about privacy and data protection, hence their leading role in discussions on online privacy protection within both the EU and the UN system.

Estonia is a very dynamic digital policy actor. After the 2007 DDoS attack that seriously affected the Internet at national level, Estonia has become a very active player in the field of cybersecurity. It hosts NATO's Cooperative Cyber Defence Centre of Excellence, as well as the Conference on Cyber Conflict, a major cybersecurity event that has been held annually since 2010.

Romania has been specialising in the field of fighting against cybercrime. It hosts the CoE Cybercrime Programme Office, whose aim is to assist countries in strengthening their criminal justice systems and their capacity to respond to challenges posed by cybercrime, on the basis of the standards of the Convention on Cybercrime.

The Netherlands hosts the Global Forum on Cyber Expertise and numerous other initiatives in the field of cybersecurity.

China

China is an important player in Internet governance, as the country with the highest number of Internet users in the world (more than 700 million) and a fast growing Internet industry (four out of ten major Internet companies are from China). China has been balancing its position in digital policy between an economy-driven approach to unrestricted Internet communications beyond national borders and a politically driven cyber sovereignty approach for Internet activities at national level.

From an economic perspective, the global Internet is of vital interest for China's export-oriented economy. Chinese companies use the Internet as the information infrastructure for their business operations worldwide. Alibaba, the main Internet platform for Chinese businesses, currently has the highest volume of e-commerce transactions globally. Alibaba's owner Jack Ma has been calling for the establishment of an Electronic World Trade Platform aimed at assisting SMEs in engaging in global digital trade.[9] At the G20 meeting in Hangzhou, in September 2016, China strongly promoted digital economy and innovation.

From a political perspective, the protection of sovereignty as a cornerstone of the Chinese foreign policy is also mirrored in cyberspace. Chinese president Xi described cyber sovereignty at the 2015 World Internet Conference as 'the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing'.[10] According to the cyber sovereignty approach, the Internet must follow the laws, customs, and governance of the physical space demarcated by national borders.

China achieved a high level of cyber sovereignty by restricting access to the Chinese market for foreign Internet companies (Facebook, Google, Twitter) and, instead, encouraging the provision of similar services by Chinese companies: Baidu (equivalent of Google), Sina Weibo (equivalent of Twitter), Renren (equivalent of Facebook), Youku (equivalent of YouTube). Most of the data belonging to Chinese individuals and institutions are stored on servers in China. Critical views of China's cyber sovereignty are related to the filtering of online content that the government deems unfit for public dissemination.

In the global digital policy space, China generally supports a multilateral approach. However, it also actively participates in multistakeholder processes and bodies such as ICANN and the IETF. As part of its efforts to more actively participate in international digital policy, China has been hosting an annual World Internet Conference since 2014.

In the forthcoming period, China's foreign digital policy will support the development of the Digital Silk Road aimed at increasing digital connectivity between Asia and Europe. The Digital Silk Road will be part of a broader project – One Belt, One Road – linking China and Europe through numerous overland and maritime links.

Brazil

Brazil has been one of the most active countries in global digital politics and is the largest Internet market in Latin America. As a democratic and developing country with a vibrant digital space, Brazil has great potential to facilitate a compromise between the two

camps in the Internet governance debate (intergovernmental and non-governmental). This role became obvious in the aftermath of the Snowden revelations, when Brazil took strong diplomatic action. In her speech at the 68th Session of the UNGA, Brazilian president Dilma Rousseff made this request: 'The United Nations must play a leading role in the effort to regulate the conduct of States with regard to these technologies.' In addition, she described the surveillance as 'a breach of international law' and 'a case of disrespect to the national sovereignty' of Brazil.[11] When it seemed that Brazil was insisting on an intergovernmental approach, President Rousseff shifted back to the middle of the policy spectrum by proposing to co-organise the NETmundial meeting aimed at further developing the multistakeholder model of Internet governance. Brazil had a complex role to play where its main aim was to ensure a successful (yet non-binding) outcome of the meeting.[12]

Brazil is very active in numerous digital policy processes. The country hosted two out of 10 IGF meetings. It has played a leading role in the WSIS+10 negotiations. Together with Germany, Brazil has been a strong promoter of international protection of online privacy.

India

India is another important player in digital policy. The country has a wide Internet user base and an advanced Internet industry, but also faces challenges when it comes to providing access to its numerous population. India's complex Internet governance policy reflects the complexity of its national digital policy-making. It has one of the most diverse and vibrant civil society scenes in global Internet governance. In the past, the Indian government tended to lean towards an intergovernmental approach to Internet governance, while its business sector has been closer to a non-governmental approach. This dichotomy has created some surprising moves. For example, India proposed the establishment of the UN Committee for Internet-Related Policies as a way to achieve intergovernmental oversight of CIR. It shifted to the other side of the Internet policy spectrum at WCIT-12, when India sided with developed countries by not signing the amended ITRs, as most developing countries did. The current Indian administration is supportive of the multistakeholder model of Internet governance, as was reiterated during the ICANN 57 meeting, held in India in November 2016.[13]

Russia

Russia has been the most vocal and consistent promoter of a multilateral approach to Internet governance, with a leading role for governments in addressing Internet-related public policy issues. In particular, Russia has been promoting the ITU's role in the field of Internet governance. In cybersecurity, Russia made early steps in 1998, when it tabled a proposal for what became the first UNGA resolution pertaining to ICT and security.[14] Since 1998, this resolution has been repeated annually, paving the way for addressing cybersecurity through the work of the first committee of the UNGA and, lately, the UN GGE.[15] Together with China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan, Russia also pursues cyber-cooperation in other institutional venues. Notably, in the framework of the SCO, there is a 2009 agreement on international information security.

In September 2015, Russia introduced a data-localisation regulation, requiring Internet companies to store the data of Russian users within the Russian borders. This law can force major Internet companies (Facebook, Twitter, Google, LinkedIn) to either locate their servers in Russia, or risk having their services blocked within the Russian territory.

Table 3. Survey of membership of the five UN GGEs established since 2004

Year / Countries	2004-2005	2009-2010	2012-2013	2014-2015	2016-2017
Argentina			■		
Australia			■		■
Belarus	■	■	■	■	
Botswana					■
Brazil	■	■		■	■
Canada			■		■
China	■	■	■	■	■
Colombia				■	
Cuba					■
Egypt			■	■	■
Estonia		■	■	■	■
Finland					■
France	■	■	■	■	■
Germany	■	■	■	■	■
Ghana				■	
India	■	■	■		■
Indonesia			■		■
Israel		■		■	
Italy		■			
Japan			■	■	■
Jordan	■				
Kazakhstan					■
Kenya				■	■
Malaysia	■			■	
Mali	■				
Mexico	■			■	■
Netherlands					■
Pakistan				■	
Qatar		■			
Republic of Korea	■	■		■	■
Russian Federation	■	■	■	■	■
Senegal					■
Serbia					■
South Africa	■	■			
Spain				■	
Switzerland					■
United States of America	■	■	■	■	■
United Kingdom	■	■	■	■	■

Kenya

Kenya is among the most dynamic players in Internet governance. It has a very vibrant multistakeholder scene, with a national IGF, and active participation of civil society, the business community, and academia in government-led initiatives on Internet governance.

One of the main successes of Kenya has been the MPesa payment system, which has provided millions of individuals with the access to financial services. The system has given a major boost to the national Internet industry, while also being exported to other countries.

Kenya is very active in African and global digital policy processes. It hosted the annual IGF meeting in 2011. Moreover, representatives of Kenya's government, business community, and civil society are very active participants in the ITU, ICANN, the IGF, and the UN GGE, among others.

Indonesia

Indonesia has had a very fast growth of the Internet, reaching 53 million users in 2016. For Indonesia, as an archipelago country, the Internet is a critical infrastructure, connecting more than 6000 inhabited islands.

Indonesia has a national IGF, which gathers representatives of government institutions, business entities, academia, and civil society. In the security field, the country's main concern is related to the use of the Internet by terrorist groups. On the economic side, Indonesia has been considering a special tax for Google and other Internet companies. In the field of privacy and data protection, Indonesia adopted the right to be forgotten. In addition to the European understanding of the right to be forgotten (i.e., allowing the delisting of specific content from search engine results), Indonesia also allows the possibility of erasing irrelevant content from websites.

Indonesia has been an active participant in international digital policy. In 2013, it hosted the annual meeting of the IGF. The country also actively participates in activities of the ITU, ICANN, the IGF, and the UN GGE.

Switzerland

Switzerland has played a pioneering role in the development of the global Internet governance ecosystem, since the first major event – the 2003 WSIS phase, in Geneva. Swiss diplomat Markus Kummer led WGIG and, subsequently, the Secretariat of the IGF (until 2010). Since 2014, ICANN's GAC has been chaired by Thomas Schneider, official at the Swiss Federal Office of Communication.

In the field of cybersecurity, Switzerland has been an active contributor to the development of CBMs for cyberspace. Currently, Switzerland is a member of the UN GGE (2016–2017).

In the field of human rights, Switzerland is among the countries that actively support the protection of privacy in the online space, via UN and other international mechanisms.

Small states

The complexity of the issues and the dynamics of activities made it almost impossible for many small countries, in particular, small developing countries, to follow Internet governance policy processes. As a result, some small states have supported a one-stop-shop structure for Internet governance issues.[16] The sheer size of the agenda and the limited policy capacity of developing countries in both their home countries and in their diplomatic missions remains one of the main obstacles for their full participation in the process. The need for capacity building in the field of Internet governance and policy was recognised as one of the priorities for the WSIS Tunis Agenda for the Information Society.

Internet governance – a variable geometry approach

Internet governance requires the involvement of a variety of stakeholders who differ in many aspects, including international legal capacity, interest in particular Internet governance issues, and available expertise. Such variety may be accommodated by using the variable geometry approach implied in paragraph 49 of the WSIS Declaration of Principles,[17] which specifies the following roles for the main stakeholders:

- States – 'policy authority for Internet-related public policy issues' (including international aspects).
- The private sector – 'development of the Internet, both in the technical and economic fields'.
- Civil society – 'important role on Internet matters, especially at the community level'.
- Intergovernmental organisations – 'the coordination of Internet-related public policy issues'.
- International organisations – 'development of Internet-related technical standards and relevant policies'.

The variable geometry approach has started to emerge in practice. For example, states have a leading role in cybersecurity and e-commerce, while the technical and business communities have leading roles in standardisation and the management of Internet names and numbers.

The business sector[18]

In the early days of the Internet, the main concern of the business sector was related to the protection of trademarks, as companies were facing cybersquatting and the misuse of their trademarks by individuals who were fast enough to register them first as domain names. When ICANN was established in 1998, business circles clearly prioritised dealing with the protection of trademarks. The growth of the Internet and e-commerce has triggered the business sector's interest in other issue areas, such as privacy and data protection, and other online human rights, cybersecurity, e-banking, taxation, content policy, and mul-

tilingualism. Today, it is difficult to find any Internet governance issue not of direct relevance for the business community. However, the emphasis on a specific issue varies from industry to industry.

The International Chamber of Commerce

The ICC, well known as the main association representing business across sectors and geographic borders, has positioned itself as one of the main representatives of the business sector in the global Internet governance processes. The ICC was actively involved in the early WGIG negotiations and WSIS, and continues to be an active contributor in the current IGF processes.

With the continuous growth of the Internet, the interest of the business community in Internet governance has become wide and diverse. The following main groups of companies have been actively involved in Internet governance processes: domain name companies, ISPs, telecommunications companies, and Internet content companies.

Domain name companies

Domain name companies include registries, which manage TLDs (e.g. .com and .net), and registrars that facilitate the registration of domain names by end-users. Among the main actors are VeriSign and Afilias. The registries and registrars business is directly influenced by ICANN's policy decisions in areas such as the introduction of new TLDs and dispute resolution. This makes them some of the most important actors in the ICANN policy-making process. Several registries and registrars, either individually, or through associations, have also been involved in the broader Internet governance policy process (WSIS, WGIG, the IGF).

Internet service providers

The role of ISPs as key online intermediaries makes them particularly important for Internet governance. Their main involvement is at national level, in dealing with government and law enforcement authorities. At a global level, some ISPs, particularly from the USA and Europe, have been active in the WSIS, WGIG, IGF, and ICANN processes, either individually or through national, regional, or sector-specific business organisations (such as the Information Technology Association of America (ITAA), the European Internet Service Providers Association (EuroISPA), and others).

Telecommunications companies

Telecommunications companies facilitate Internet traffic and run the Internet infrastructure. The main actors include companies such as Verizon, AT&T, Vodafone, Deutsche Telekom, and Telefonica. Traditionally, telecommunications companies have been participating in international telecommunications policy through the ITU. They have been increasingly involved in the activities of ICANN and the IGF. Their primary interest in Internet governance is to ensure a business-friendly international environment for the further development of the Internet telecommunications infrastructure.

In addition, telecommunications operators have been raising the question of a redistribution of the revenue generated by the Internet. They argue that, as long as they provide access to Internet, they should receive a higher portion of the Internet-generated income (which now mainly benefits content companies, due to their advertising-based revenue generating model).

Refer to Section 5 for further discussion on redistribution of revenue between Internet and telecom companies.

Telecommunications companies have been trying to increase their income by introducing new services and requesting Internet content companies to pay more for faster services. Many of these proposals involve different treatment for different types of Internet traffic, which could represent a breach of the net neutrality principle. This makes telecommunications companies one of the main opponents of the net neutrality principle.

Refer to Section 2 for further discussion on net neutrality.

While trying to address the question of redistribution of Internet income, both telecommunications companies and the Internet industry have started to enter each other's domains. Telecommunications companies are providing Internet content and communication services, while the Internet industry is investing in telecommunications infrastructure. Google and Facebook, for example, are investing in trans-Atlantic and trans-Pacific seabed fibre optic cables.

Internet industry

The Internet industry is often referred to as OTT. It includes all industries whose business model is mainly based on the Internet. They are divided into three main segments: content, communications, and services. Most major companies cover more than one segment. For example, Google and Facebook provide both content and communications services.

Internet CONTENT industry

Most of the Internet industry is based on content. Google's search engine provides access to a wide range of online content. YouTube provides access to video materials. Facebook organises content generated by users. Some of the traditional content providers such as Disney have evolved successfully into online content providers. The business priorities of these companies are closely linked to various Internet governance issues, such as IPR, privacy, cybersecurity, and net neutrality. Their presence is increasingly noticeable in the global Internet governance processes, including the WTO, WIPO, and the IGF.

Internet COMMUNICATIONS industry

The major players in Internet communications services are Skype, WhatsApp, WeChat, Snapchat, and Google Talk. Communication on these platforms is increasingly encrypted, and this is often challenged by national governments. Thus, the main challenge for the Internet communications industry is to ensure the use of encrypted communications and the protection of the privacy rights of their customers.

Internet SERVICES industry

The Internet services industry is also referred to as a platform industry. It includes new types of services such as Uber and Airbnb. These companies use the Internet to provide new types of services, such as the use of private cars for public transport (Uber). Their business model is closely linked to many Internet governance issues, including taxation, consumer protection, and labour rights.

Civil society

Civil society has been the most vocal and active promoter of a multistakeholder approach to Internet governance. Civil society is also the most diverse stakeholder group in Internet governance processes. Civil society groups focus on different Internet-related issues, with many of them being strong advocates of the protection of human rights on the Internet, including freedom of expression and privacy. One major difference among civil society groups is related to the role of governments in Internet governance. Traditionally, civil society actors have seen governments as one among other equal participants in Internet governance processes, alongside civil society, businesses, and the technical community. More recently, views have started emerging within civil society that governments should play a leading role in protecting public interests, based on their legitimacy. In particular, this position is supported by the view that only governments can counter-balance a very powerful role of the business sector in digital matters.[19]

The high diversity of views on various Internet governance topics has made the coordination of the civil society position in international meetings particularly difficult. In the WSIS process, civil society representation managed to harness this inherent complexity and diversity through different organisational forms, including a Civil Society Bureau, the Civil Society Plenary, and the Content and Themes Group. Due to WGIG's multistakeholder nature, civil society attained a high level of involvement in this process. Civil society groups proposed eight candidates for WGIG, all of whom were subsequently appointed by the UN Secretary General. As members of the group, they managed to influence many conclusions, including the decision to establish the IGF as a multistakeholder space for discussing Internet governance issues.

Civil society has continued to be actively involved in IGF activities. One of the *sui generis* forms of civil society representation in Internet governance processes is the Internet Governance Caucus (IGC). It includes individuals interested in sharing opinions, policy options, and expertise on Internet governance issues, which are discussed in a mailing list format.

Civil society organisations are active in almost all Internet governance topics – from infrastructure development through to economic models to rights and freedoms – mainly focusing on protection of public interest(s). Many organisations employ experts and academics with solid knowledge and understanding of Internet specificities, and provide valuable contributions to the decision-shaping process.

One of the main challenges for civil society organisations is the sustainability of their activities. In the early days of the WSIS process, most of civil society's participation was centred around committed individuals. While this provided early dynamism, it also created a risk for the sustainable participation of civil society. Sustainable involvement of civil society requires sustainable organisations. The APC has been one of the first organisational player involved in Internet governance. Best Bytes and Just Net Coalition have also emerged as organised initiatives of civil society.

With a few billion Internet users, the Internet's civil society reflects the diversities and differences of the real society. The main challenge for civil society will remain to represent this diversity of views and positions in digital policy.

International organisations

The ITU was the central international organisation in the WSIS process. It hosted the WSIS Secretariat and provided policy input on the main issues. ITU involvement in the WSIS process was part of its ongoing attempt to define and consolidate its new position in the fast-changing global telecommunications arena, increasingly shaped by the Internet. The ITU's role has been challenged in various ways. For example, it has been losing its traditional policy domain due to the WTO-led liberalisation of the global telecommunications market. The trend of moving telephone traffic from traditional telecommunications to the Internet (through VoIP) further reduced the ITU's regulatory footprint on the field of global telecommunications.

The possibility that the ITU might have emerged from the WSIS process as the *de facto* International Internet Organisation caused concern in the USA and in some other developed countries, while garnering support in some developing countries. Throughout WSIS, this possibility created underlying policy tensions. It was particularly clear in the field of Internet governance, where tension between ICANN and the ITU had existed since the establishment of ICANN in 1998. This tension was not resolved by WSIS, but was later largely defused. With the increasing convergence of various communication technologies, it is very likely that the question of the ITU's more active role in the field of Internet governance will remain on the global policy agenda; it is already active in the field of cybersecurity and child online protection, for example.

Another issue concerned the anchoring of the multidisciplinary WSIS agenda within the family of UN specialised agencies. Non-technical aspects of communications and Internet technology, such as social, economic, and cultural features, are part of the mandate of other UN organisations. The most prominent player in this context is UNESCO, which addresses issues such as multilingualism, cultural diversity, knowledge society, and information sharing. WIPO is also active in Internet governance debates, on issues related to the protection of IPR in digital space.

The balance between the ITU and other UN organisations was carefully managed. The WSIS follow-up processes also reflect this balance, with the coordinating role of the ITU, and the participation of UNESCO, UNDP, and UNCTAD. These UN agencies, for example, are the main organisers of the annual WSIS Forum, which has, over the past few years, included more and more debates on Internet-governance-related issues.

The technical community

The technical community includes institutions and individuals who have been involved in the development of the Internet and/or are managing Internet technical resources. The technical community has also created the initial spirit of the Internet, based on the principles of sharing resources, open access, and opposition to government involvement in Internet regulation. From the beginning, its members have protected the initial concept of the Internet from intensive commercialisation and extensive government influence.

Terminology: Technical community

Other terms are used interchangeably with 'technical community', such as Internet community, Internet developers, Internet founders, Internet fathers, and technologists. The term 'technical community' is used in the WSIS declarations and other policy documents.

The technical community fulfils all the criteria in Peter Haas's[20] definition of an epistemic community: 'a professional group that believes in the same cause and effect relationships, truth tests to accept them, and shares common values; its members share a common understanding of a problem and its solutions'.

The early technical community was coordinated by a few, mainly tacit, rules and one main formal procedure – the RFCs. All main and basic standards of the Internet are described through RFCs. While it did not have a strict regulation or formal structure, the early Internet community was governed by strong customs and peer-to-peer pressure. Most participants in this process shared similar values, appreciation systems, and attitudes.

The early management of the Internet by the technical community was challenged in the mid-1990s after the Internet became part of global social and economic life. Internet growth introduced a group of new stakeholders, such as the business sector, that came with different professional cultures and understanding of the Internet and its governance, which led to increasing tension. For example, in the 1990s, the Internet community and the company Network Solutions[21] were involved in the so-called DNS war, a conflict over the control of the root server and domain name system.

The Internet Society is one of the main representatives of the technical community. It hosts the IETF, advocates for an open Internet, and plays an active role in capacity development.

The technical community has been an important actor in the process of both establishing and running ICANN. One of the fathers of the Internet, Vint Cerf, was the Chair of the ICANN Board from 2000 to 2007. Members of the technical community hold important positions in various ICANN decision-making bodies.

Nowadays, with more than three billion users, the Internet has outgrown the initial ICANN-based policy framework focusing on the technical community as the main constituency. Following this argument, as the line between citizens and Internet users blurs, greater involvement of governments and other structures representing citizens is required, rather than those representing Internet users only (as the technical community has been described). Those who argue for more government involvement in Internet governance use this approach of representing citizens rather than Internet users and communities.

The technical community has usually justified its special position in certain Internet governance processes by its technical expertise. It used to argue, for example, that ICANN is mainly a technical organisation and, therefore, technical people using technical knowledge should run it. With the growing difficulty of maintaining ICANN as an exclusively technical organisation, this justification of the special role of the technical community has faced frequent challenge. It is very likely that the members of the technical community will gradually integrate into the other stakeholder groups, mainly civil society, business, and academia but also governments.

ICANN

ICANN was created in 1998 as a US-based non-profit corporation, and it was entrusted, by the US government, with the task of performing the IANA functions, i.e., managing, at the general level, the core Internet infrastructure, which consists of IP addresses, domain names, and root servers.

The growing interest in the role of ICANN developed in parallel with the rapid growth of the Internet in the early 2000s and ICANN came to the attention of global policy circles during the WSIS process (2003–2005).

ICANN's current mission, as reflected in its 2016 revised bylaws, is to ensure the stable and secure operation of the Internet's unique identifier systems. To this aim, the organisation coordinates the allocation and assignment of names in the DNS root zone, as well as the development and implementation of policies regarding gTLDs; facilitates the coordination of the DNS root name server system; and coordinates the overall allocation and assignment of IP numbers and autonomous system numbers.

While ICANN is one of the main actors in the Internet governance field, it does not govern all aspects of the Internet. It has sometimes, though erroneously, been described as the Internet government. ICANN manages the Internet technical resources, but it does not have direct authority over other Internet governance issues, such as cybersecurity, content policy, copyright protection, protection of privacy, maintenance of cultural diversity, or bridging the digital divide.

ICANN is a multistakeholder institution involving a wide variety of actors in different capacities and roles. They fall into three main groups.

- The technical and business communities, whose role within the ICANN system is to develop recommendations for the ICANN Board on policies covering areas related to the organisation's mission (e.g. gTLDs, security and stability of the DNS).

- National governments, whose increasing interest in having a more important role in ICANN started with the WSIS process. In the framework of ICANN's policy development process, governments have an advisory role: they provide advice to the ICANN Board, particularly on matters that may affect public policy issues.

- Internet users (the community at large), whose contribution to the policy development process is also of an advisory nature.

Involving Internet users

ICANN has experimented with various approaches to involving Internet users. In its early days, the first attempt was to involve Internet users through direct elections of representatives to ICANN governing bodies. It was an attempt to secure ICANN's legitimacy. With low turnout and misuse of the process, the direct vote failed: it did not provide a real representation of Internet users. Later on, ICANN started involving Internet users through an 'at-large' governance structure (the At-Large Advisory Committee – ALAC), public consultations, and crowdsourcing.[22] These organisational experiments are essential for ensuring ICANN's legitimacy.

ICANN's decision-making process was influenced by early Internet governance processes based on bottom-up, transparent, open, and inclusive approaches. One main difference between the early technical community of the 1980s and the current ICANN decision-making context is the level of 'social capital'. In the past, the technical community had high levels of mutual trust and solidarity that made decision-making and dispute resolution much simpler than it is now. The growth of the Internet extended to billions of new users and new stakeholders, far beyond the early technical community. Consequently, this fast growth of the Internet reduced the social capital that existed in its early days. Thus, the technical community's frequent proposals to retain the earlier, informal, decision-making process on the Internet has not been realistic. Without social capital, the main way of ensuring a fully functional decision-making process is to formalise it and to develop different checks-and-balances mechanisms.

Some corrections to decision-making procedures have already been made to reflect this changing reality. For example, the 2002 reform of ICANN included strengthening the GAC and abandoning the direct voting system for Internet users. More changes are currently being implemented with the aim to increase ICANN's accountability towards the global Internet community.

The issues

Technical vs policy management

The dichotomy between technical and policy management has created continuous tension in ICANN's activities. ICANN has portrayed itself as a technical coordination body for the Internet, that deals only with technical issues and stays away from the public policy aspects of the Internet. ICANN officials considered this specific technical nature as the main conceptual argument for defending the institution's unique status and organisational structure. The first chair of ICANN, Esther Dyson, stressed that: 'ICANN does not "aspire to address" any Internet governance issues; in effect, it governs the plumbing, not the people. It has a very limited mandate to administer certain (largely technical) aspects of the Internet infrastructure in general and the Domain Name System in particular.'[23]

Critics of this assertion usually point to the fact that no technically neutral solutions exist. Ultimately, each technical solution or decision promotes certain interests, empowers certain groups, and affects social, political, and economic life. Dealing with issues such as the .xxx TLD and the new gTLDs introduced in 2014 is increasingly illustrating the fact that ICANN has to deal with public policy aspects of technical issues.

IANA stewardship transition and ICANN accountability

Until 1 October 2016, ICANN performed the IANA functions on the basis of a contract with the US government (the Department of Commerce, through NTIA). In line with this contract, the US government had ultimate authority on every major change made within the DNS (e.g. when ICANN decided to approve certain new gTLDs, every such decision also needed formal validation from the US government).

In March 2014, the US government announced its intention to transition its stewardship role over the IANA functions to the global multistakeholder community.[24] ICANN was requested to launch a process for the development of a transition proposal. At the same time, work began on the elaboration of a set of recommendations for enhancing ICANN's

accountability mechanisms. Between 2014 and 2016, the ICANN community worked intensively on the elaboration of the transition and accountability proposals, which were approved by the ICANN Board in March 2016, and accepted by the US government in June 2016 as being compliant with its requirements.

In line with the IANA stewardship transition proposal, ICANN established PTI, as a subsidiary which became the IANA naming functions operator, on the basis of a contract with ICANN. This means that the IANA functions related to domain names continue to be performed with the ICANN framework, but with a more clear separation between the technical functions and the policy-making functions of ICANN. The revised ICANN bylaws, entered into force on 1 October 2016, also underline the condition under which a review process could lead to the separation of the IANA functions operators from ICANN. Major changes in the DNS root zone, previously subject to the US government formal approval, are now subject to validation by the ICANN Board of Directors.

The performance of the IANA functions related to the IP numbers and protocol parameters has also been entrusted to PTI. Agreements for the performance of these functions have been concluded between ICANN and the numbering resources community (mainly the RIRs responsible for the regional allocation and management of IP addresses), and the protocol parameters community (represented by the IETF and the IAB), and were followed by subcontract agreements between ICANN and PTI.

With regard to ICANN's accountability to the broader Internet community, in the absence of the stewardship role of the US government, new mechanisms have been put in place within the organisation. The most important is the creation of a new legal entity – the empowered community – functioning as an unincorporated association which has the ability to enforce a set of community powers, such as removing members of the ICANN Board, rejecting ICANN budgets, or rejecting changes to the ICANN bylaws. This entity acts as instructed by the its decisional participants – most of ICANN's advisory committees and supporting organisations representing Internet users, governments, the private sector, and the technical community.[25]

Endnotes

1 The Brazilian model of the management of its country domain name is usually taken as a successful example of a multistakeholder approach. The national body in charge of Brazilian domains – CGI – is open to all users, including government authorities, the business sector, and civil society. Brazil gradually extended this model to other areas of Internet governance, especially in the process of the preparation for IGF 2007 and 2014, which were held in Rio de Janeiro, and João Pessoa, respectively. Brazil has continued to be active in Internet governance, especially in NetMundial (http://netmundial.br), a process initiated in October 2013 by Brazilian President Dilma Rousseff and ICANN's President Fadi Chehadé, and the follow-up process, the NetMundial Initiative (https://www.netmundial.org/).

2 For an updated list of national IGF initiatives, refer to Internet Governance Forum (no date) National IGF initiatives. Available at http://www.intgovforum.org/multilingual/content/national-igf-initiatives [accessed 6 November 2016). The IGF website also includes a list of recognised regional IGF initiatives: Internet Governance Forum (no date) Regional IGF initiatives. Available at http://www.intgovforum.org/multilingual/content/regional-igf-initiatives [accessed 6 November 2016].

3 Géraud A (1954) The rise and fall of the Anglo-French Entente. *Foreign Affairs*. Available at http://www.foreignaffairs.com/articles/71095/andre-geraud-pertinax/rise-and-fall-of-the-anglo-french-entente [accessed 29 October 2016].

4 Lesage C (1915) *La rivalite franco-britannique. Les cables sous-marins allemands* Paris. p. 257–258; quoted in: Headrick D (1991) *The Invisible Weapon: Telecommunications and International Politics 1851–1945*. Oxford: Oxford University Press. p. 110.

5 Mueller M (1999) ICANN and internet governance: Sorting through the debris of 'self-regulation'. *info (The Journal of Policy, Regulation and Strategy for Telecommunications Information and Media)* 1(6), p 497–520. Available at http://www.icannwatch.org/archive/mueller_icann_and_internet_governance.pdf [accessed 14 March 2016].

6 US Secretary of State criticising the ITU for the initiative: 'without authorization of member governments to hold a global meeting involving an unauthorized expenditure of resources and concluding international agreements.' Quoted in Drake W (2004) Reframing Internet Governance Discourse: Fifteen Baseline Propositions, p. 9. Available at http://www.un-ngls.org/orf/drake.pdf [accessed 29 October 2016].

7 Internet World Stats (2015) Internet Usage in the European Union. Available at http://www.internetworldstats.com/stats9.htm [accessed 14 November 2016].

8 European Commission (2013) Antitrust: Commission seeks feedback on commitments offered by Google to address competition concerns. European Commission – IP/13/371. Available at http://europa.eu/rapid/press-release_IP-13-371_en.htm [accessed 29 October 2016].

9 Alibaba Group (no date) Electronic World Trade Platform. Available at http://www.alizila.com/wp-content/uploads/2016/09/eWTP.pdf [accessed 12 November 2016].

10 Ministry of Foreign Affairs of the People's Republic of China (2015) Remarks by H.E. Xi Jinping, President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference. Available at http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml [accessed 12 November 2016].

11 Rousseff D (2013) Statement by H.E. Dilma Rousseff, president of the Federative Republic of Brazil, at the opening of the general debate of the 68th Session of the United Nations General Assembly. Available at https://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf [accessed 29 October 2016].

12 NETmundial (2014) NETmundial Multistakeholder Statement. Available at http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf [accessed 29 October 2016].

[13] Goldstein D (2016) Indian Minister of Electronics and Information Technology Reaffirms Support of the Multistakeholder Model at ICANN's 57th Public Meeting. *Domain Pulse*, 6 November. Available at http://www.domainpulse.com/2016/11/06/india-reaffirms-support-multistakeholder-model-icann57/ [accessed 6 November 2016].

[14] United Nations General Assembly (1999) Resolution A/53/70. Developments in the Field of Information and Telecommunications in the Context of International Security. Available at http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70 [accessed 8 November 2016].

[15] Radu R (2013) Negotiating meanings for security in the cyberspace. *Info* 15(6), pp. 32–41. Available at https://www.researchgate.net/publication/255697155_Negotiating_meanings_for_security_in_the_cyberspace [accessed 14 March 2016].

[16] The convenience of 'one-stop shopping' was one of the arguments for establishing the ITU as the central Internet governance player.

[17] WSIS (2003) Declaration of principles. Available at http://www.itu.int/wsis/docs/geneva/official/dop.html [accessed 12 November 2016].

[18] Valuable comments were provided by Ayesha Hassan.

[19] This view has been supported, in particular, by the Just Net Coalition, and is reflected in various statements and declarations issued by the organisation. For details, refer to Just Net Coalition (no date) Statements. Available at http://justnetcoalition.org/statements [accessed 10 November 2016].

[20] Haas P (1990) *Saving the Mediterranean: The Politics of International Environmental Cooperation*. New York: Columbia University Press, p.55

[21] The technology company Network Solutions www.networksolutions.com was founded in 1979. The domain name registration business was the most important division of the company; the company diversified its portfolio to include web services for small businesses.

[22] Radu R *et al*. (2015) Crowdsourcing ideas as an emerging form of multistakeholder participation in Internet governance. *Policy & Internet 7(3)*, pp. 362–382

[23] Dyson E (1999) *Esther Dyson's response to Ralph Nader's Questions*. Available at http://www.icann.org/en/correspondence/dyson-response-to-nader-15jun99.htm [accessed 14 March 2016].

[24] NTIA (2014) NTIA Announces Intent to Transition Key Internet Domain Name Functions. Available at https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions [accessed 29 October 2016].

[25] For more details on the IANA stewardship transition and the ICANN accountability processes, refer to *GIP Digital Watch* observatory (no date) IANA Transition and ICANN Accountability. Available at http://digitalwatch.giplatform.org/processes/iana [accessed 29 October 2016].

DiploFoundation is a non-profit organisation dedicated to making diplomacy and international governance more inclusive and effective. In particular, Diplo is working to

- Increase the power of small and developing states to participate meaningfully in international affairs.
- Increase international accountability and inclusivity.
- Increase the legitimacy of international policy-making.
- Improve global governance and international policy development.

Diplo's main activities:

Capacity development: Diplo's capacity development support begins with individuals, but through the activities of these individuals, our impact reaches into the larger systems of which they and their organisations are a part. Our approach includes online training, policy research, policy immersion, and the development of communities of practice, combined in various ways, as appropriate to each policy context. Capacity development topics include Internet governance, e-diplomacy, public diplomacy, humanitarian diplomacy, and global health diplomacy.

Events: To deal with pressing issues in global governance, our events bring together people from different perspectives, including diplomats, business professionals, and members of civil society. We work to make our events more accessible through e-tools that support remote participation. Our events often evolve into training activities, publications, or online interaction.

Courses: We offer postgraduate-level academic courses and training workshops on a variety of diplomacy-related topics for diplomats, civil servants, staff of international organisations and NGOs, and students of International Relations. Combining a highly developed learning methodology with our unique online learning platform, our courses are flexible, personal, interactive, and community-building. Courses are delivered online, face-to-face, and in a blended format.

Research: We build on traditional policy research methods through Internet-based techniques including crowd-sourcing, trend analysis, and collaborative research. Topics include diplomacy, Internet governance, and online learning.

Publications: Our publications range from the examination of contemporary developments in diplomacy to new analyses of its traditional aspects. Many of our publications are available online as well as in print format and some have been translated into several languages.

Diplo was established in 2002 by the governments of Malta and Switzerland and has offices in Msida, Malta; Geneva, Switzerland; and Belgrade, Serbia. Diplo has consultative status with the UN ECOSOC since 2006.

For more information about Diplo, visit https://www.diplomacy.edu

Geneva Internet Platform

The Swiss Federal Department of Foreign Affairs (EDA) and the Federal Office of Communications (OFCOM) initiated the **Geneva Internet Platform** (GIP), which fulfils the mission of an observatory, a capacity-building centre (online and *in situ*), and a centre for discussion. The GIP is an initiative supported by the Swiss authorities and operated by DiploFoundation.

The GIP's activities are implemented based on three pillars:

- A physical platform in Geneva
- An online platform and observatory
- An innovation lab

The GIP's special focus is on assisting small and developing countries to meaningfully participate in Internet governance processes. The support is tailored to the needs of these actors, including training, awareness building, consultations, and briefings.

For more information on the GIP's activities, visit http://www.giplatform.org

DigitalWatch

The *GIP Digital Watch* aims to provide practitioners of Internet governance and digital policy with a tool allowing them to stay up-to-date with current information on Internet policy issues, participants, and ongoing developments. The *GIP Digital Watch* relies on materials, knowledge management expertise, and networks developed by DiploFoundation over the past 20 years.

Three pillars form part of the *GIP Digital Watch* initiative:

The *GIP Digital Watch* observatory provides a neutral one-stop shop for live developments, overviews and explanatory texts, events, resources, and other content related to Internet governance and digital policy.

The *Geneva Digital Watch* newsletter, a monthly newsletter, includes a round-up of developments, interviews with prominent experts, and articles on various digital policy areas.

Monthly GIP briefings on Internet governance in Geneva and online take place on the last Tuesday of every month. As of 2016, local hubs are being established worldwide to encourage sustainable discussions in local communities, and share regional perspectives during the monthly briefings.

For more information on the *GIP Digital Watch*, visit https://digitalwatch.giplatform.org

Glossary

3G	third-generation mobile networks
4G	fourth-generation mobile networks
5G	fifth-generation mobile networks
ACTA	Anti-Counterfeiting Trade Agreement
ADR	Alternative Dispute Resolution
AFRINIC	African Network Information Centre
AFTLD	Africa Top Level Domains Organization
AI	artificial intelligence
ALAC	At-Large Advisory Committee (ICANN)
APEC	Asia-Pacific Economic Cooperation
APC	Association for Progressive Communications
APNIC	Asia Pacific Network Information Centre
APTLD	Asia Pacific Top Level Domain Association
ARPAnet	Advanced Research Projects Agency Network
ARF	Association of Southeast Asian Nations (ASEAN) Regional Forum
ARIN	American Registry for Internet Numbers
ASEAN	Association of Southeast Asian Nations
AU	African Union
AXIS	African Internet eXchange System (AU)
BEREC	Body of European Regulators for Electronic Communications
BIS	Bank for International Settlements
BGPSec	Border Gateway Protocol Security
BRICS	Brazil, Russia, India, China, and South Africa
BTA	Basic Telecommunication Agreement
CA	Certificate Authority
CBMs	confidence-building measures
CCD COE	Cooperative Cyber Defence Centre of Excellence (NATO)
ccNSO	Country Code Names Supporting Organization (ICANN)
ccTLD	country code top-level domain
CDNs	content delivery networks
CEDAW	Convention on the Elimination of All Forms of Discrimination against Women (UN)
CEFACT	Centre for Trade Facilitation and Electronic Business (UN)
CEN	European Committee for Standardization
CENTR	Council of European National Top Level Domain Registries
CERN	European Organization for Nuclear Research
CERT	Computer Emergency Response Team

CGI.br	Brazilian Internet Steering Committee
CI	critical infrastructure
CIA	confidentiality, integrity, availability
CICTE	Inter-American Committee against Terrorism
CIDR	Classless Inter-Domain Routing
CIGF	Commonwealth Internet Governance Forum
CII	critical information infrastructure
CIIP	critical information infrastructure protection
CIR	critical Internet resources
CITEL	Inter-American Telecommunication Commission
CJEU	Court of Justice of the European Union
CND	content delivery networks
CoE	Council of Europe
COMESA	Common Market for Eastern and Southern Africa
COP	Child Online Protection (ITU initiative)
CRC	Convention on the Rights of the Child (UN)
CRPD	Convention on the Rights of Persons with Disabilities (UN)
CSIRT	Computer Security Incident Response Team
CSS	cascading style sheets
CSTD	Commission on Science and Technology for Development (UN)
DDoS	distributed denial of service
DMCA	Digital Millennium Copyright Act (USA)
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DOA	Digital Object Architecture
DoS	denial of service
DSL	digital subscriber line
DWDM	dense wavelength division multiplexing
ebXML	electronic business XML
ECHR	European Court of Human Rights
ECOSOC	Economic and Social Council (UN)
ECTS	European Credit Transfer and Accumulation System
EDI	electronic data interchange
eIDAS	Regulation on electronic identification and trust services for electronic transactions in the internal market (EU)
ENISA	European Union Agency for Network and Information Security
EPC	electronic product code
EPCIP	European Programme for Critical Infrastructure Protection
ETNO	European Telecommunications Network Operators
ETSI	European Telecommunications Standards Institute
EuroDIG	European Dialogue on Internet Governance
EuroISPA	European Internet Service Providers Association
Europol	European Police Office
FATF	Financial Action Task Force

FBI	Federal Bureau of Investigation (USA)
FCC	Federal Communications Commission (USA)
FIRST	Forum of Incident Response and Security Teams
GAC	Governmental Advisory Committee (ICANN)
GATS	General Agreement on Trade in Services
GATT	General Agreement on Tariffs and Trade
GCA	Global Cybersecurity Agenda
GCCS	Global Conference on CyberSpace
GCI	Global Cybersecurity Index
GFCE	Global Forum on Cyber Expertise
GIP	Geneva Internet Platform
GICGM	High-Level Panel on Global Internet Cooperation and Governance Mechanisms
GSM	Global System for Mobile Communications
GSMA	Groupe Speciale Mobile Association
gTLD	generic top-level domain
HD	high definition
HTCIA	High Technology Crime Investigation Association
HTML	HyperText markup language
HTTP	HyperText transfer protocol
IaaS	Infrastructure as a Service
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
IBP	Internet bandwidth provider
ICANN	Internet Corporation for Assigned Names and Numbers
ICC	International Chamber of Commerce
ICMEC	International Centre for Missing & Exploited Children
ICT	information and communications technology
IDC	International Data Corporation
IDN	internationalised domain name
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGC	Internet Governance Caucus
IGF	Internet Governance Forum
ILO	International Labour Organization
IMF	International Monetary Fund
IMPACT	International Multilateral Partnership against Cyber Threats
INHOPE	International Association of Internet Hotlines
INSAFE	Network of Safer Internet Centres
INTERPOL	International Criminal Police Organization
IoT	Internet of Things
IP	Internet protocol
IPR	intellectual property rights
IPSec	Internet protocol security

IPTV	Internet protocol television
IPv4	Internet protocol version 4
IPv6	Internet protocol version 6
IRP	independent review process
ISO	International Organization for Standardization
ISP	Internet service provider
ITAA	Information Technology Association of America
ITRs	International Telecommunication Regulations
ITU	International Telecommunication Union
ITU-D	ITU Telecommunication Development Sector
ITU-T	ITU Telecommunication Standardization Sector
IXP	Internet exchange point
LACNIC	Latin American and Caribbean Network Information Centre
LACTLD	Latin American and Caribbean ccTLDs Organization
LAN	local area network
LDCs	least developed countries
LED	light emitting diode
LGBTQ	lesbian, gay, bisexual, trans, and queer
LIR	local Internet registry
LPWAN	low-power wide-area network
LTE	long-term evolution
M3AAWG	Messaging, Malware, and Mobile Anti-Abuse Working Group
MDG	millennium development goal
MIS-NET	Committee of Experts on Internet Intermediaries (CoE)
MLAT	Mutual Legal Assistance Treaty
MoU	memorandum of understanding
NAT	network address translation
NATO	North Atlantic Treaty Organization
NIR	national Internet registry
NRI	Network Readiness Index (WEF)
NSA	National Security Agency (USA)
NSI	Network Solutions Inc.
NTIA	National Telecommunications and Information Administration (USA)
OAS	Organization of American States
OASIS	Organization for the Advancement of Structured Information Standards
ODR	online dispute resolution
OECD	Organisation for Economic Co-operation and Development
OSCE	Organization for Security and Co-Operation in Europe
OTT	over-the-top (services)
P2P	peer-to-peer
PaaS	Platform as a Service
PIPA	PROTECT IP Act

PKI	public key infrastructure
PLC	power line communications
PPP	public private partnership
PRISM	Personal Record Information System Methodology
PTI	Public Technical Identifiers (ICANN)
QoS	quality of service
REMJA	Ministers of Justice or Other Ministers or Attorneys General of the Americas
RFC	request for comments
RFID	radio frequency identifiers
RIPE NCC	Réseaux IP Européens Network Coordination Centre
RIR	regional Internet registry
RSC	Radio Spectrum Committee (EU)
RSPG	Radio Spectrum Policy Group (EU)
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition
SCO	Shanghai Cooperation Organisation
SDG	sustainable development goal
SGML	standard generalized markup language
SMEs	small and medium-sized enterprises
SNA	system network architecture
SOPA	Stop Online Piracy Act
SOXA	Sarbanes-Oxley Act
SSL	secure sockets layer
TACD	Trans Atlantic Consumer Dialogue
TASIM	Trans-Eurasian Information Super Highway
TCP/IP	transmission control protocol/Internet protocol
TLD	top-level domain
TPP	Trans-Pacific Partnership
TRIPS	Trade-Related aspects of Intellectual Property Rights
TTIP	Transatlantic Trade and Investment Partnership
UDHR	Universal Declaration of Human Rights
UDRP	Uniform Dispute Resolution Policy
UMAP	University Mobility in Asia and the Pacific
US(A)	United States (of America)
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law
UNDP	United Nations Development Programme
UNESCAP	United Nations Economic and Social Commission for Asia and the Pacific
UNGA	United Nations General Assembly
UN GGE	United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

UNHRC	United Nations Human Rights Council
UNODC	United Nations Office on Drugs and Crime
UNTOC	United Nations Convention against Transnational Organized Crime
UPC	universal product code
VAT	value added tax
VCR	videocassette recorder
VoIP	Voice over Internet protocol
VPN	virtual private network
W3C	World Wide Web Consortium
WCIT	World Conference on International Telecommunications
WEF	World Economic Forum
WGIG	Working Group on Internet Governance
WHO	World Health Organization
WiMax	worldwide interoperability for microwave access
WIPO	World Intellectual Property Organization
WLAN	wireless local area network
WML	wireless markup language
WSIS	World Summit on the Information Society
WTO	World Trade Organization
WTSA	World Telecommunication Standardization Assembly (ITU)
www	world wide web
XHTML	eXtensible HTML
XML	eXtensible markup language
ZB	zettabytes

For a more comprehensive list of acronyms, initialisms, and abbreviations used in Internet governance parlance, refer to DiploFoundation's Internet Governance Acronym Glossary, available at https://www.diplomacy.edu/resources/books/internet-governance-acronym-glossary

About the author

Dr Jovan Kurbalija is the founding director of DiploFoundation and head of the Geneva Internet Platform. A former diplomat, his professional and academic background is in international law, diplomacy, and information technology. In 1992, he established the Unit for Information Technology and Diplomacy at the Mediterranean Academy of Diplomatic Studies in Malta. After more than ten years of training, research, and publishing, in 2002 the Unit evolved into DiploFoundation.

Since 1994, Dr Kurbalija has been teaching courses on the impact of ICT/Internet on diplomacy and Internet governance. Currently, he is visiting lecturer at the College of Europe in Bruges, Belgium, and the University of St Gallen, Switzerland. He has lectured at the Mediterranean Academy of Diplomatic Studies in Malta, the Vienna Diplomatic Academy in Austria, the Dutch Institute of International Relations (Clingendael), the Graduate Institute of International and Development Studies in Geneva, Switzerland, the UN System Staff College, Torino, Italy, and the University of Southern California, in Los Angeles. He conceptualised and has directed DiploFoundation's Internet Governance Capacity Building Programme since 2005. Dr Kurbalija's main research interests include the development of an international regime for the Internet, the use of the Internet in diplomacy and modern negotiations, and the impact of the Internet on modern international relations.

Dr Kurbalija has published and edited numerous books, articles, and chapters, including: *The Internet Guide for Diplomats, Knowledge and Diplomacy, The Influence of IT on Diplomatic Practice, Information Technology and the Diplomatic Services of Developing Countries, Modern Diplomacy, and Language and Diplomacy*. With Stefano Baldi and Eduardo Gelbstein, he co-authored the Information Society Library, a set of eight booklets covering a wide range of Internet-related developments.

jovank@diplomacy.edu

AN INTRODUCTION TO INTERNET GOVERNANCE

Jovan Kurbalija

An Introduction to Internet Governance provides a comprehensive overview of the main issues and actors in this field. Written in a clear and accessible way, supplemented with figures and illustrations, it focuses on the technical, security, legal, economic, development, sociocultural, and human rights aspects of Internet governance. Providing a brief introduction, a summary of major questions and controversies, and a survey of different views and approaches for each issue, the book offers a practical framework for analysis and discussion of Internet governance.

Since 1997, more than 3000 diplomats, computer specialists, civil society activists, and academics have attended training courses based on the text and approach presented in this book. With every delivery of the courses, materials are updated and improved, making the book particularly useful as a teaching resource for introductory studies in Internet governance.

9789993253303