Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA
Directorate of Political Affairs DP
Division for Security Policy DSP

No. 57

Politorbis

Zeitschrift zur Aussenpolitik
Revue de politique étrangère
Rivista di politica estera

www.eda.admin.ch/politorbis

Switzerland and Internet governance:

Issues, actors, and challenges

2 / 2014

Contact:

Federal Department of Foreign Affairs FDFA
Directorate of Political Affairs DP
Division for Security Policy DSP
Politorbis
Bernastrasse 28
3003 Bern

Phone: + 41 58 464 37 77
Fax: + 41 58 464 38 39

mailto: politorbis@eda.admin.ch
www.eda.admin.ch/politorbis

Die Texte werden normalerweise in der Sprache der Verfasser gedruckt.
Der Inhalt muss nicht zwingend mit der Meinung des EDA übereinstimmen.

En principe, les articles sont publiés dans la langue de travail de leurs auteurs.
Le contenu ne reflète pas nécessairement la position du DFAE.

The articles are published usually in the language in which they were written.
The contents do not necessarily reflect the views of the FDFA.

Politorbis

Table of Contents

Preface 5

Benno Laggner

Switzerland and Internet governance: Issues, actors, and challenges

Jovan Kurbalija

A summary – in 10 tweet-style statements 7

Introduction 9

The evolution of Internet governance 11

WHY is Internet governance important for Switzerland? 13

What are the Internet governance issues? 17

What are the seven Internet governance baskets? 19

WHO are the main players? 33

HOW is Internet governance debated? 37

WHERE is Internet governance currently debated? 41

Foreseeable scenarios 43

Recommendations 45

Annexes 49

Endnotes 65

Preface

Benno Laggner[1]

'Any sufficiently advanced technology is indistinguishable from magic'. The words of Arthur C. Clarke prevail in the 21st century more than ever – the change and the rapid pace brought about by digital devices have indeed a touch of magic.

Today, it is unthinkable to imagine the world without the Internet. It enables us to do things which only a few years ago would have been impossible. The Internet reaches every facet of our lives and permeates almost every aspect of our society. Being only twenty years old, it has become the key driver of the most extensive, far reaching and fastest technological revolution in history. The Internet is the engine of change and a true game changer!

While other technological innovations have spread comparatively slowly, the Internet has had an impact on a vast part of the world in only a short period of time, taking only a couple of years for the Internet population to reach 3 billion people. Compared to the telephone, for example, which took more than 50 years to reach the 100 million mark after its invention in the 19th century, Internet-related technologies have had shorter cycles for their adoption.

And yet, the Internet constitutes a young technology which is still developing. In fact, everything we have witnessed so far is nothing but the beginning. As we are entering a new era, entitled the 'Internet of Things', more than 50 billion physical devices will be interlinked and over 5 billion people will be online.

As one of the world's leading countries in the use of information and communication technologies, Switzerland fully benefits from the Internet. It is estimated that more than 80% percent of the population have Internet connection. Almost 80% use the Internet several times a week and more than 60% percent use it daily. Switzerland's future viability depends on an open, secure and reliable Internet which has become an indispensable driver of economic development and a key means of social interaction.

Switzerland is determined to seize the opportunities that are generated by using the Internet and the technologies that underpin it. At the same time, this commonly shared digital space is not risk-free: these risks ranging from cyber espionage and sabotage to 'cybered' conflicts have to be effectively managed.

In order to mitigate the risks associated with the Internet, the Federal Council adopted the 'national strategy for the protection of Switzerland against cyber risks' on 27 June 2012. This strategy has laid the foundation for a comprehensive, integrated and holistic approach and also calls for an active participation of Switzerland in the realm of Internet governance.

With regard to Internet governance, Switzerland has been actively engaged for a long time. Since the beginning of the Internet governance debate at the World Summit on the Information Society (WSIS) in Geneva, Switzerland has played an active role in shaping the Internet governance process and defended principles such as inclusiveness and democratic participation, transparency and accountability in Internet governance.

Switzerland's contribution to the ongoing debate is anchored in its own long experience in consensus-finding and policy-making in a multicultural environment. In order to maintain an open, inclusive, interoperable, reliable and secure

[1] Ambassador Benno Laggner is currently the Head of the Division for Security Policy and Ambassador for Nuclear Disarmament and Non-Proliferation in the Swiss Federal Department of Foreign Affairs.
Prior to this appointment, Benno Laggner was the Deputy Chef de Cabinet of the President of the 65th session of the United Nations General Assembly. Earlier postings included serving as Head of the UN Coordination Unit in the Federal Department of Foreign Affairs (2007-2010), as Head of the Political Section at the Swiss Embassy in Berlin (2004-2007) and as Head of the Political Section at the Permanent Mission of Switzerland to the United Nations in New York (2000-2004).
Benno Laggner holds a Master's Degree in International Relations (University of St.Gallen, Switzerland) and also completed postgraduate studies in European Affairs at the College of Europe in Bruges, Belgium.

Internet, Switzerland is committed to fostering an approach that allows all stakeholders, in their respective roles, to shape the discussion and decision-making on an equal footing.

Switzerland will not only continue to advocate a multistakeholder approach, but it will also reflect on ways to invigorate it. As more and more people interact in the digital environment and as the cyberspace gradually evolves, it is imperative to develop a common set of rules and expectations as well as to define not only the roles, but also the responsibilities of all participants and stakeholders within the cyber ecosystem.

However, the above described vision is not uncontested. The question how and by whom the Internet should be governed was a major topic of 'NETmundial – the Global Multistakeholder Meeting on the Future of the Internet Governance' in Sao Paulo. This meeting confirmed the multistakeholder principle. It remains, however, open how it will be implemented. In this context, Switzerland thinks the Internet Governance Forum should play a key role.

Against this background, the Division for Security Policy within the Swiss Federal Department of Foreign Affairs commissioned DiploFoundation to prepare a report on Internet governance, outlining the main issues, actors and challenges. Dr. Jovan Kurbalija, the founding Director of DiploFoundation and author of the paper, is an expert in the field of information technology and international law. His main areas of research are diplomacy and the development of an international Internet regime, online negotiations and diplomatic law.

The report highlights the main milestones regarding the Internet governance debate since the WSIS held in Geneva in 2003. It illustrates the roles and responsibilities of key actors in the course of the development of the Internet and describes the key challenges, such as the protection of fundamental human rights (e.g. the right to privacy). It moreover provides recommendations as to how Switzerland can promote its foreign policy in the digital realm. Given that cyberspace constitutes a cross-cutting domain, the study finally examines the interplay between cyber-security, human rights and innovation.

A summary – in 10 tweet-style statements

- Swiss digital assets owned by citizens and companies are increasingly hosted on digital clouds abroad and subjected to foreign laws.

- Billions CHF lost from cyber-attacks. The vulnerability of the Internet is the vulnerability of modern Swiss society.

- The more inclusive and universal Internet governance (IG) is, the better Swiss interests will be safeguarded.

- Existing IG is not robust enough to handle major economic and geo-political tensions triggered by the fast growth of the digital sphere.

- CH cannot determine global IG. With like-minded countries, it may influence it. By acting internationally, CH will deal with national issues as well.

- IG is multidisciplinary (technology, law, economics), multistakeholder (government, civil society, business) and multi-levelled (local-national-regional-global) approach.

- Aim for preferable outcome (genuine multistakeholderism), but prepare for possible outcome (intergovernmentalism).

- Smart approach: mix of careful planning and flexibility to adapt to changes & input from society; in 3 years digital world will be very different!

- Cannot predict (digital) earthquake – major crisis, but CAN prepare to deal with consequences – by maintaining robust & efficient IG.

- Aim for win/win solutions; if not possible strike right balance: cybersecurity/human rights; protection of public goods/business interests

Indroduction

Jovan Kurbalija[1]

The way the Internet is governed is of strategic importance to modern societies. With close to three billion users, the Internet is a critical communication infrastructure. The Internet is deeply embedded in our daily routines. It accounts for over 20% of the gross domestic product (GDP) growth in the world's largest economies. Billions of euros are lost from cyber-attacks. Increasingly, the vulnerability of the Internet is the vulnerability of countries worldwide.

Yet, current Internet governance (IG) is not robust enough to address the critical relevance of the Internet for modern societies. The Snowden revelations created a major earthquake in digital politics, showing the limitations of the existing IG institutions in dealing with major economic and geo-political tensions.

To continue to thrive, the Internet needs effective and sustainable governance. Many governments, international organisations, think-tanks, and experts have started a search for a new IG formula. IG has moved from the realm of engineers and geeks into the premier league of global politics.

The challenges are enormous. On the one hand, due to the trans-border character of the Internet, many countries – including Switzerland – face digital limitations in effectively performing their core sovereign functions: providing security (e.g. cybersecurity, which impacts critical national infrastructures), protecting the rights of their citizens (e.g. privacy and child protection on the Internet), and protecting citizens' and businesses' properties (e.g. private data and online corporate assets being targeted by Internet-based industrial espionage operations).

On the other hand, too intrusive government regulation could reduce the innovative potential of the Internet. IG has to strike the right balance between addressing risks and vulnerabilities, while ensuringfuture Internet growth, as the main enabler of social and economic development.

Switzerland has positioned itself as a trusted, reliable, and competent player in global IG. It has gained this reputation, in particular, as the host of and one of the key players during the World Summit of the Information Society (WSIS; 2003–2005), and as one of the main supporters of the Internet Governance Forum (IGF), especially in an early critical phase. In addition, Switzerland has supported Diplo's Internet Governance Capacity Building Programme (IGCBP) since 2002, which has enabled many small and developing countries to participate in global IG processes. At the regional level, Switzerland – together with the Council of Europe (CoE) – has been and still is the driving force behind the European Dialogue on Internet Governance (EuroDIG), a pan-European space for addressing IG issues.

As a well-respected and constructive international partner, Switzerland has an interest and the opportunity to influence the discussions and to act as a mediator to help bridge differing visions of IG which, at present, have led to divisive and sterile discussions in different international forums.

This report starts with a brief evolution of IG, followed by chapters answering the core questions: Why is IG relevant for Switzerland? What are the main IG issues? Who are the main players? How and where is IG performed? The future – when – question is addressed through an analysis of three main IG scenarios.

[1] Dr Jovan Kurbalija is the founding director of DiploFoundation. He is a former diplomat with a professional and academic background in international law, diplomacy, and information technology. In 1992, he established the Unit for IT and Diplomacy at the Mediterranean Academy of Diplomatic Studies in Malta. In 2002, after more than ten years of successful work in training, research, and publishing, the Unit evolved into DiploFoundation.

Annexes

Annex I
Swiss contribution to Internet governance

Annex II
Geneva Internet Governance Index (CIGI)
The role of Geneva in global Internet governance

Annex III
Internet governance glossary

The evolution of Internet governance

The current debate cannot be understood outside the broader historical context of the Internet development. Thirty years ago, engineers, academics, and geeks, based mainly at US universities, started managing the Internet through the principle of 'running code and rough consensus'. This functional and inclusive approach facilitated the explosive growth of the Internet, making it one of the most important inventions in the history of humanity. There was no central governance, no central planning, and no grand design. The Internet has developed incrementally as a unique, collaborative endeavour. The Internet community created a specific ethos which John Perry Barlow, one of the Internet pioneers, describes thus:

'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.'

This view explains the current prevailing non-governmental approach to IG and the scepticism of the Internet community about the role of government in IG.

In the early days of the Internet, the US government played the role of 'distant guardian'. It was close enough to support research on the Internet – mainly financially – but far enough away not to interfere in how the Internet was governed.

The 'sunny period' of early IG ended in 1994, when the US government started the privatisation of the management of the Internet Domain Name System (DNS), the Internet's 'address book'. The Internet community, guided by a non-profit approach, strongly resisted this move. This led to the so-called DNS war, which ended in 1998, with the creation of the Internet Corporation for Assigned Names and Numbers (ICANN) as a privately led organisation overseen by the US government. Since its creation, ICANN has been the focus of most IG debates.

In the early 2000s, governments started becoming involved in IG, with the beginning of the World Summit on the Information Society (WSIS), which officially placed IG on the global diplomatic agenda. Many developing countries argued for the internationalisation of ICANN's function, giving a stronger role to the United Nations (UN) and other inter-governmental organisations. The USA and its allies opposed these proposals. A compromise was struck when the WSIS established the IGF for multistakeholder discussions on IG issues. The WSIS 'Tunis compromise' satisfied advocates of a government-centred approach by bringing the IG discussion under the UN umbrella for the first time, since the IGF is convened by the UN secretary-general. The Tunis compromise was also acceptable for the USA and other developed countries, because it promoted a multistakeholder approach, and diminished the risk of ICANN's function being passed to inter-governmental organisations.

Since WSIS-2005, the Internet has grown enormously. Facebook and Twitter did not exist in 2005, and social media was just emerging. The number of Internet users tripled from 1 billion in 2005 to almost 3 billion in 2014. China has now overtaken USA in the number of the Internet users. It remains to be seen how these changes to the Internet will affect IG. The first signal of tectonic shifts was the revision of the International Telecommunication Regulations (ITRs) of the International Telecommunication Union (ITU), which ended in a split vote at the World Conference on International Telecommunication (WCIT-12) in December 2012; voting was split mainly between developed and developing countries. Some authors even marked this as the beginning of a digital Cold War. The Snowden revelations accelerated the pace of the IG debate. Most of the upcoming debates, including the WSIS +10 review process, will revisit the compromise reached at WSIS-Tunis back in 2005. The main challenge will be to preserve the legacy of the early IG (inclusive, effective, and open) while ensuring a stronger role for governments when it comes to the protection of public and national interests.

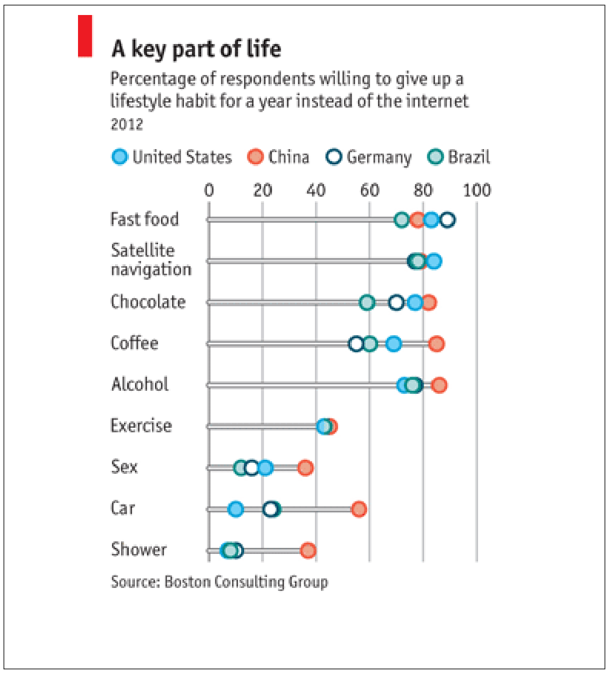
WHY is Internet governance important for Switzerland?

The Internet is a critical infrastructure for Swiss society. On the risk side, the cost of a security failure would be very high – over half a billion CHF for a day of Internet outage. On the opportunity side, most economic and societal growth is Internet-driven.

The strategy Switzerland will develop, and the role Switzerland will play in the elaboration of future Internet norms and institutions, are therefore essential. At stake are the performance of the Swiss economy, the rights of its citizens, and Swiss national security. The core of the Swiss brand and reputation – a country that is safe, strong, neutral, and smart – might be endangered if these Internet-related vulnerabilities and opportunities are not addressed.

3.1. Social relevance

With a very high penetration rate (82.1% of the total population, ranked in top 10 countries) the Internet impacts all segments of social life in Switzerland. Social relevance starts with each individual, moves to the family, and then to society as a whole.



Source: Boston Consulting Group

On the **individual** level, the Internet impacts our preference and life style. According to a study by the Boston Consulting Group, more than 60% of people would rather stop drinking coffee or alcohol or eating chocolate for a year rather than give up the Internet.[1] This study confirms what we know intuitively. We depend a lot on the Internet; our online presence is deeply embedded in our daily routines and in our way of living, yet apart from a few surveys, there is a lack of psychological and anthropological studies on the impact of the Internet on values and life style.

According to the 2012 OECD *Internet Economy Outlook*, the Internet is becoming 'a domestic intercom' as a way of communicating on a **family** level. According to the study in the UK, 20% of parents use Information and Communication Technologies (ICT) to communicate with their children. The most frequent message is 'dinner is ready' (13%) followed by 'clean your room', and 'do your homework'.[2] With the increasing use of Internet of Things (connecting refrigerators, cars, and domestic appliances to the Internet) dependence of families on the Internet will further increase. Families will also generate additional data.

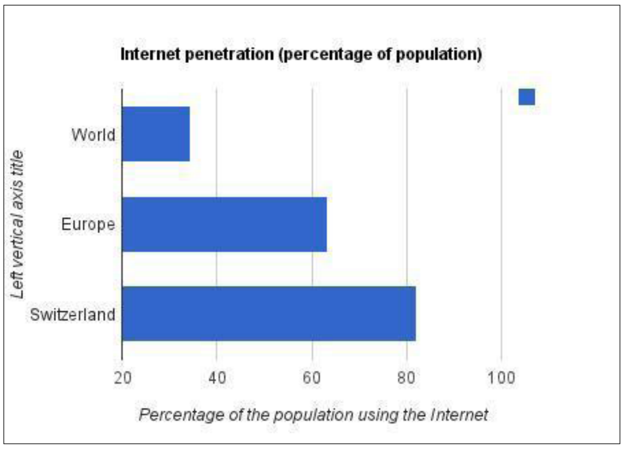


Figure 1. Internet penetration

On the **societal** level, Switzerland is ranked among the top 10 countries with the highest Internet penetration (82.1% of the total population; Figure 1).

In social networking Switzerland follows the European pattern with 47% of Internet users being also Facebook users. Switzerland is just a little behind France and ahead of Italy and Austria.[3]

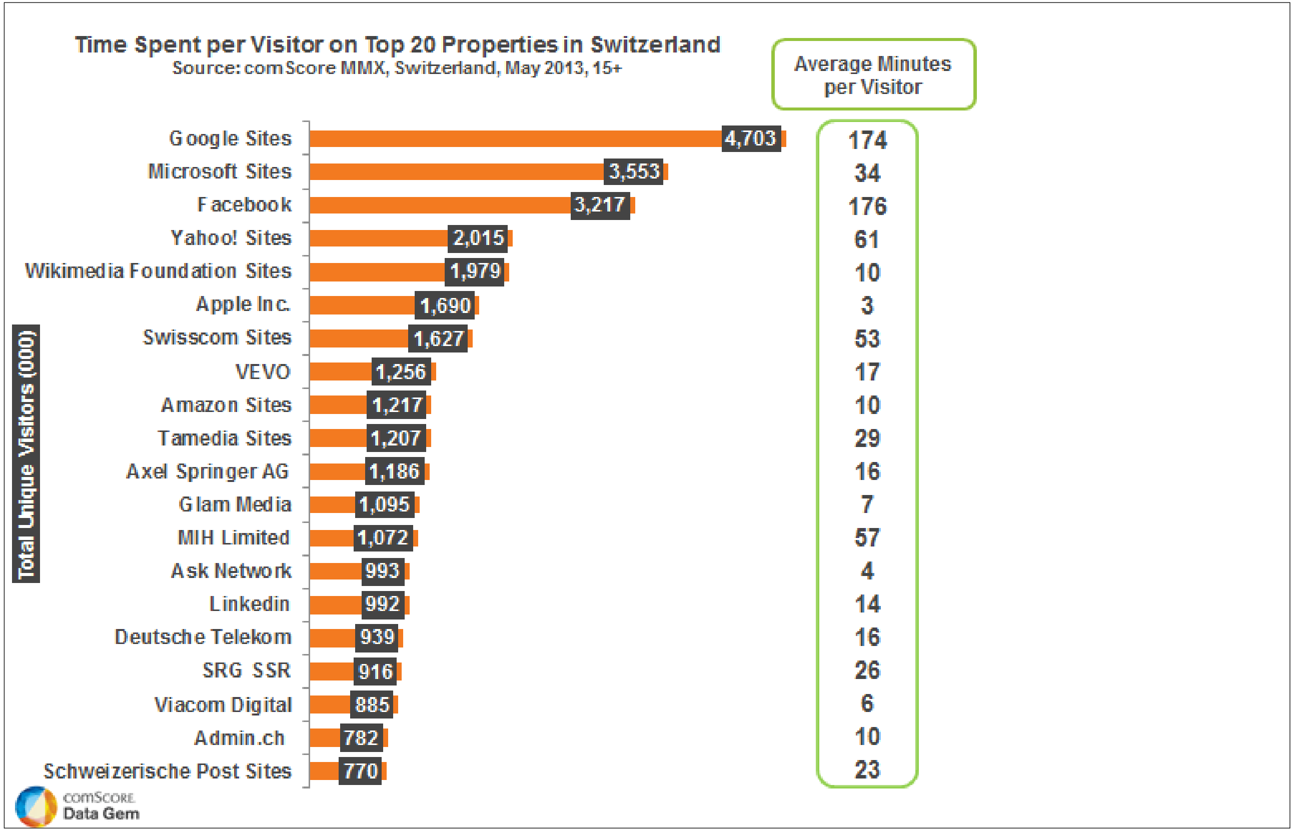
	Facebook users (% of Internet users)	Internet users	Facebook users
Switzerland	47%	6 502 247	3 056 800
Europe	48%	518 512 109	250 934 000
World	23%	3 609 854 920	835 525 280

Table 1. Facebook users and the Internet

According to ComScore MMX, 4.7 million users in May 2013 spent an average of 174 minutes on the Google website. The first Swiss site on the list is Swisscom with 1.6 million users in May 2013 (Figure 2).

3.1.1. Geo-emotions and Facebook

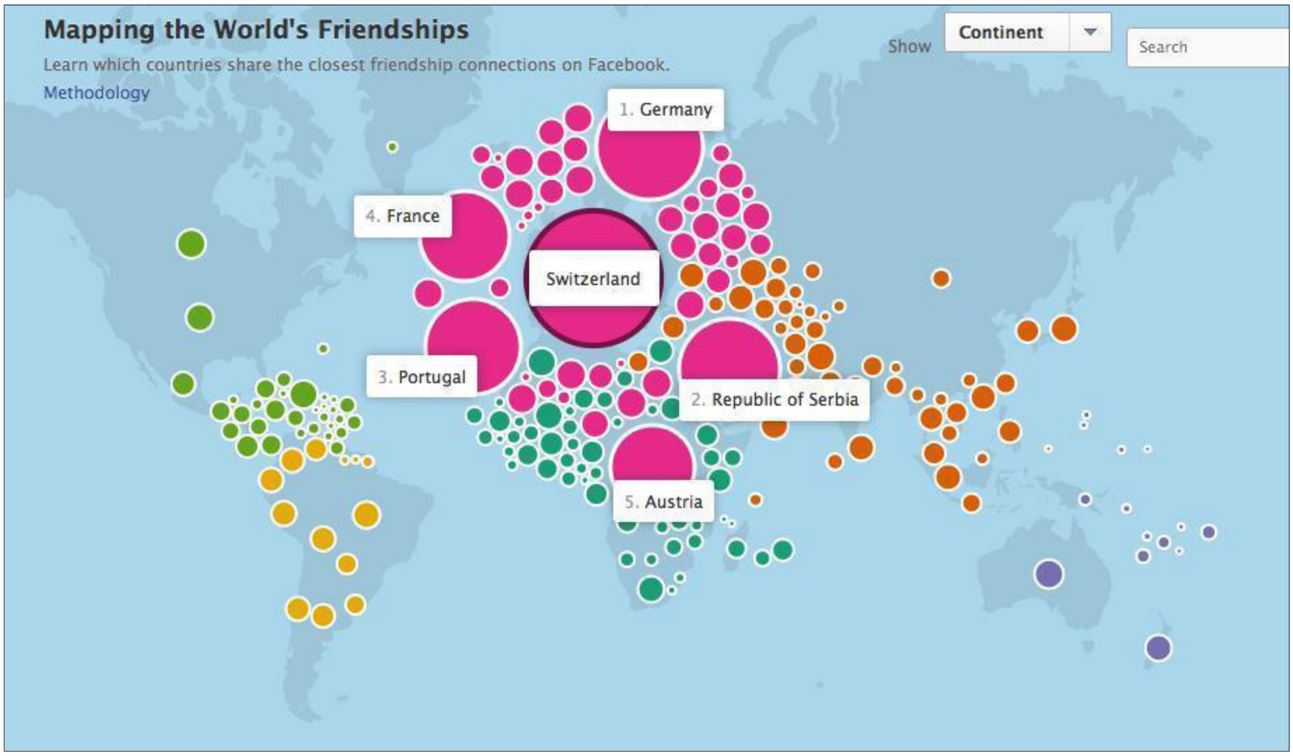
The Internet as a social media platform provides new possibilities for interaction. The Closer Look project by Stanford graduate Mia Newman maps Facebook friendships among users in different countries (Figure 3). In the case of Switzerland, Facebook friendship includes the following countries: 1. Germany, 2. Serbia, 3. Portugal, 4. France and 5. Austria. Germany, France and Austria have high status due to numerous historical, professional, and family links with neighbouring countries. The high position of Serbia and Portugal is related mainly to links between immigrants and their home countries. Both Serbia and Portugal have a big migrant community in Switzerland. This shows another layer in Internet interdependence. It also shows the importance of the Internet for communication with the diaspora.



Time Spent per Visitor on Top 20 Properties in Switzerland

Source: comScore MMX, Switzerland, May 2013, 15+

Figure 2. Swiss Internet user habits.[4]



Mapping the World's Friendships

Learn which countries share the closest friendship connections on Facebook.

Figure 3. Mapping the world's friendships.[5]

Switzerland is also among the leading countries in the field of e-government. It takes 15th position globally in the UNPAN-report on e-government, while, a prestigious Waseda University e-Government Ranking ranks Switzerland in 13th position for 2012.

3.2. Economic relevance

The Swiss economy is highly dependent on the Internet infrastructure (100% of business – the highest in OECD). In addition, the Swiss export industry and services use the Internet as a communication infrastructure with clients and partners abroad. The financial sector and knowledge-intensive industries (pharmaceuticals and engineering) are particularly vulnerable to cyber crime and industrial cyber espionage. Switzerland has the third fastest-growing online retail market, after the UK and Germany.[6]

While Switzerland has a high level of Internet use in business, it does not have a well-developed Internet industry (i.e. among 50 leading Internet companies – e.g. Google, Facebook, Twitter – there are no Swiss companies). Such an economic landscape impacts Swiss digital policy. It has to protect the robustness of the Internet as a global network and as the infrastructure of the Swiss industry. However, it does not have specific economic interests to safeguard (e.g. Internet industry), which provides it more room for manoeuvre to act as a constructive player in global digital policy.

3.3. Security relevance

With its high Internet dependence, Switzerland faces numerous vulnerabilities at citizen, institutional and national level. These should be addressed at the appropriate level.

As early as 2004, academics from the Swiss Federal Institute of Technology, Centre for Security Studies (CSS) warned about the possible effects of a wholesale cyber-attack on the Swiss infrastructure, resulting in an Internet outage for 24 hours. The calculated economic loss yielded almost 310 million CHF at that time.[7] Deploying the same mathematic model and set-up with up-to-date ground data, the total economic loss of an eventual 24-h Internet outage across Switzerland today is estimated at more than 500 million CHF.

Switzerland is among the responsible cybersecurity players. Switzerland is a low 'polluter' of the global Internet space when it comes to using the Internet and associated technical measures. According to Europol statistics, Switzerland is among the countries with less that 1% of global cyber crime. Few botnet attacks, viruses, and other malware are generated from Switzerland. For instance, it is not listed among the top countries of sources of attacks on the German Telecom Cyber initiative monitor in August 2013, nor is it listed under the top countries hosting malware or botnet servers in the Websense Security Report of 2012. World Bank statistics show that Switzerland is the 7th top country in the world with regard to the number of secure Internet servers per million people (Figure 4), way above France, the United Kingdom (UK), the USA and other advanced cyber economies.

Securing its own cyber operations requires capability for both the prevention and the cure. The prevention includes addressing various flaws: in software and hardware developed by the vendors, in hardware settings by the institutions and individuals, and in the knowledge and awareness of users about safe use and hygiene.

The *national strategy for the protection of Switzerland against cyber risks of 2012* outlines the main threats on a national level. It is obvious, however, that there is not much a country can do to protect itself from cyber threats without comprehensive cooperation on a global level. Switzerland has high economic and political stakes in assuring effective cybersecurity cooperation, not only among most of the states, but also among key stakeholders.

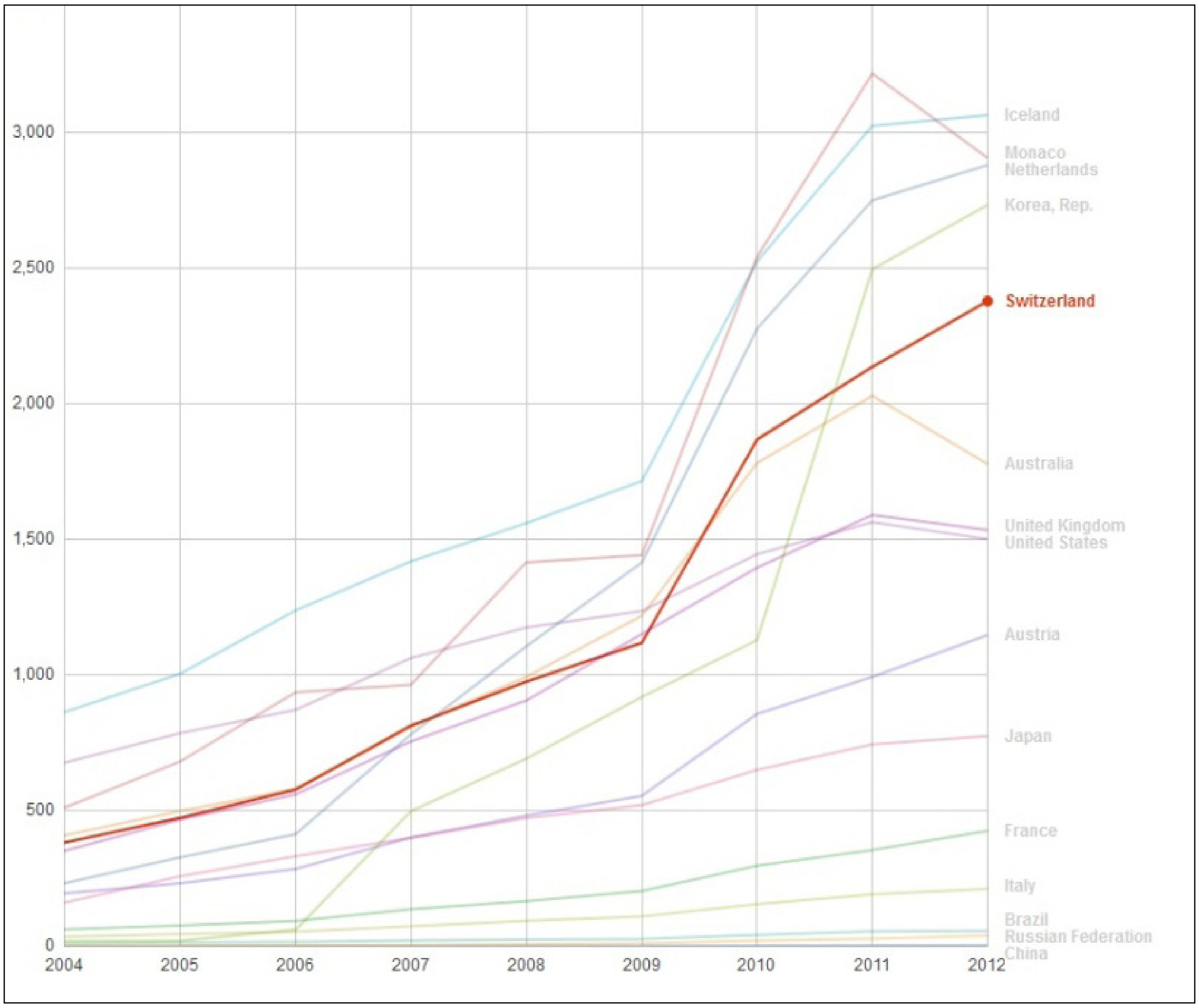


Figure 4. Number of secure Internet servers per one million people. (Source: World Bank, graphic: Google Public Data)

What are the Internet governance issues?

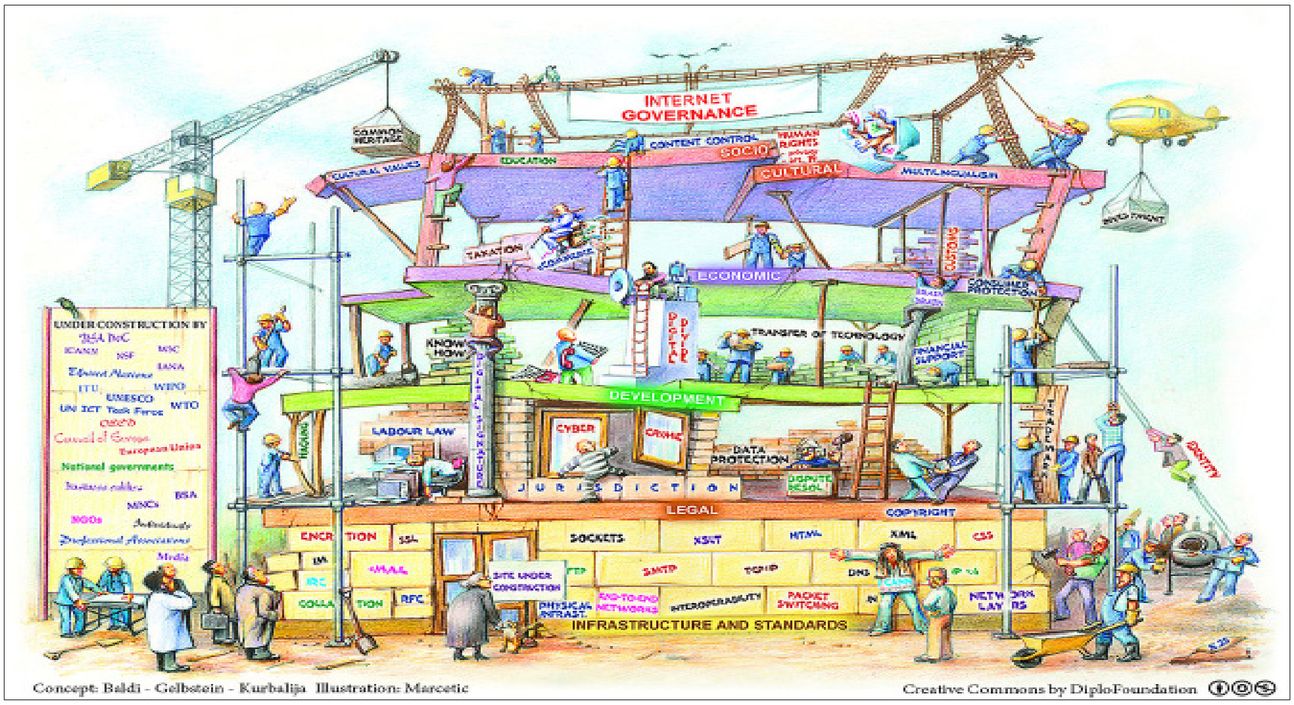
The governance of the Internet consists of more than 50 policy issues that affect the way it is organised, managed, and used. Diplo classifies IG policy issues in seven baskets: infrastructure and standardisation, cybersecurity, legal, economic, development, human rights, and sociocultural.

This wide set of IG issues could be separated in two major realms:

- Cyber issues which deal in a narrow sense with the proper functioning of the Internet (e.g. domain name system (DNS), root servers, Net neutrality).
- 'Old' policy issues, whose current (state-led) governance is touched, or even transformed by the advent of the Internet. While crime is an 'old' issue, for example, it took a new form with the Internet and evolved into cyber crime. Similar examples of the Internet having transformed 'old' issues are taxation, intellectual property, commerce, privacy, and content control to name a few.

Most IG issues are of a multidisciplinary nature. Thus, an understanding of the *whole* of IG begins with an understanding of the *parts*. For example, changes in critical Internet infrastructure, such as how an individual computer locates other computers or applications, may affect security issues. As PRISM/National Security Agency (NSA) has shown, state security surveillance may affect privacy and data protection. Legal issues of intellectual property rights (IPR) may affect economic issues of e-commerce in the sale and lending of books or music. Government regulation of pricing, designed to increase low-cost access, may affect investment and innovation.

The main challenge in dealing with multidisciplinary nature of the IG issues is how to ensure policy coherence (how to address various aspects of IG issues).



Concept: Baldi - Gelbstein - Kurbalija Illustration: Marcetic

Creative Commons by DiploFoundation

IG building under construction

4.1 Main Internet governance issues

IG is often associated with **ICANN,** the organisation that manages the Internet 'address book' – the global Domain Name System (DNS). The DNS handles Internet addresses (such as www.google.com) and converts them to unique Internet protocol (IP) numbers. The main controversy is ICANN's status (a legal entity incorporated in California, USA) and mandate (received from the US government). Many countries insist that this arrangement must be changed in order to have a completely international management reflecting the global nature of the Internet. On 14 March 2014, the US Department of Commerce's National Telecommunications and Information Administration (NTIA) announced that it is ready to end the US oversight of ICANN. In this statement, the NTIA invited the Internet community to propose an alternative solution. The NTIA indicated that it 'will not accept a proposal that replaces the NTIA role with a government-led or an inter-governmental organisation solution'. The discussion on an alternative to US oversight is likely to dominate the IG debate.

Switzerland is vice-chair of ICANN's Government Advisory Committee (GAC), the main channel for governments' influence on ICANN's activities, and plays an important role in bridging various divides within ICANN. The question of the protection of the Red Cross and related name against fraudulent use on the Internet could be of potential relevance for Switzerland as the host of the International Committee of the Red Cross (ICRC) and one of the main players in the international humanitarian field. In the context of discussions on the internationalisation of ICANN, Switzerland has also been considered as a possible venue for hosting ICANN. One legal study commissioned by ICANN indicated the status of the ICRC as the most suitable for the multistakeholder and international status of ICANN. Switzerland should follow up on this possibility.[8]

Privacy, data protection, and **cloud computing** are three IG issues that came into public focus after the Snowden revelations. In addition to concerns about the surveillance, online privacy and data protection discussion has been triggered by a major shift in the way users are managing their applications and data: the transfer of services, and in particular data, from hard disks on personal computers, to Internet servers (e.g. gmail, hotmail, wikis), which form the so-called clouds in cloud computing. Digital assets of individuals and organisations 'migrated' to servers managed by companies located in other countries, mainly in the USA. Governments worldwide are concerned about the limited protection of digital assets of citizens and business corporations abroad.

Switzerland, like other European countries, should safeguard the level of data protection guaranteed by the CoE Convention on data protection and national legislation. The main challenge is to ensure that intermediaries (Internet companies), often located abroad, observe Swiss data protection regulation when dealing with the digital assets of Swiss citizens and institutions. The Safe Harbour agreement between the USA and the EU (and other European countries Fortries) was an early – not particularly successful – attempt to ensure the protection of European data handled by US companies. In the search for a solution to the problems of protection of privacy and data on the Internet, Switzerland is part of the 'online privacy coalition' that sponsored the adoption of the UN General Assembly resolution on online privacy and follow-up activities in the UN Human Rights Council.[9]

What are the seven Internet governance baskets?[10]

Fifty-one IG issues are divided in seven baskets. For each specific issue, there is a brief introduction, a list of the main controversies and the position of Switzerland (if there is a specific aspect and available information).

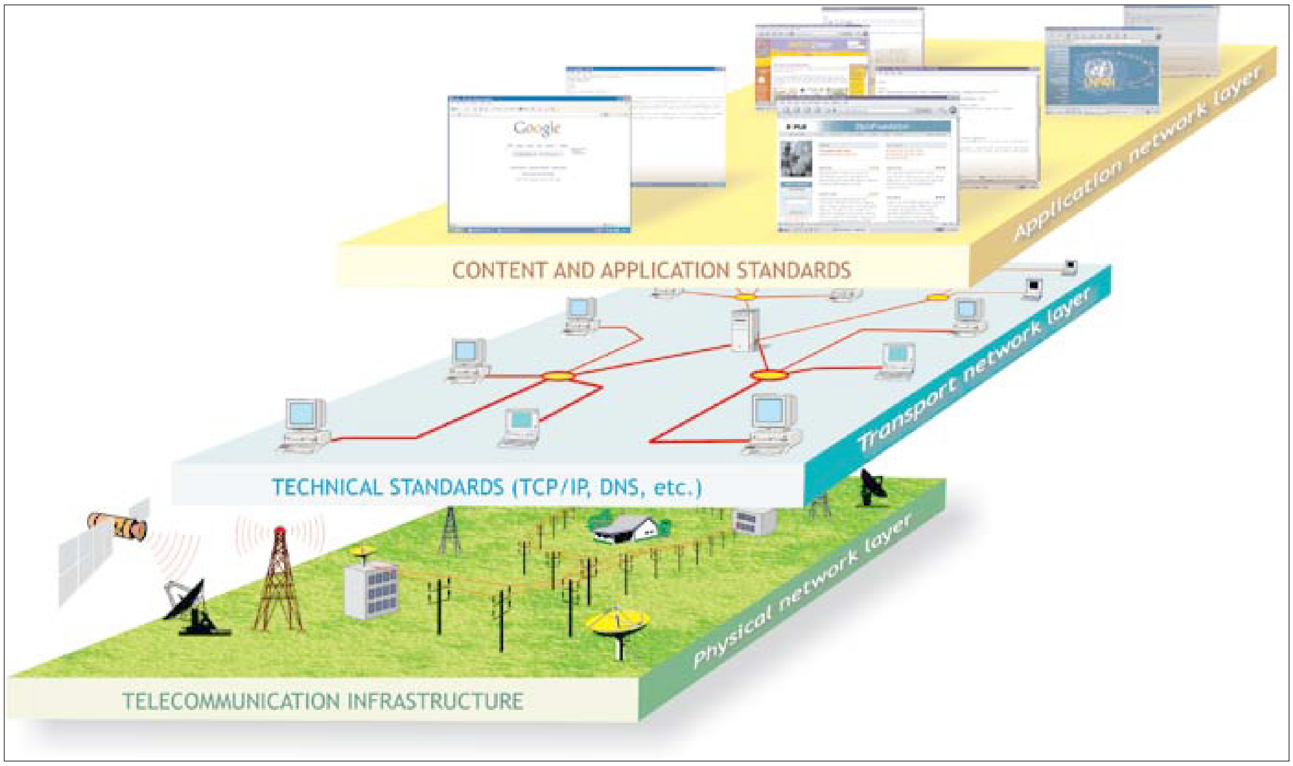

Google
CONTENT AND APPLICATION STANDARDS
Application network layer
TECHNICAL STANDARDS (TCP/IP, DNS, etc.)
Transport network layer
TELECOMMUNICATION INFRASTRUCTURE
Physical network layer

Figure 5. The layers of the Internet

A name indicates what we seek. An address indicates where it is. A route indicates how we get there
~attributed to Jon Postel (1943–1998) an Internet pioneer and author of principal protocol standards for the Internet

5.1. Infrastructure and standardisation basket

Infrastructure and standardisation include the underlying, principally technical, issues which explain how the Internet functions:

This quotation explains quite well how the Internet works. The *name* is the website domain (such as http://www.diplomacy.edu) that the user is looking for. The *address* is the number assigned to that web domain in the DNS – the global 'Internet address book'. The *route* is the transmission protocols and applications that resolve the address, resulting in the web page being displayed on the user's screen. In a simplified manner, the IG infrastructure can be viewed as having three parts:[11] the **physical network** of the infrastructure – a medium like copper or fibre cables, wireless or satellite signal – which carries all Internet traffic; the **protocols** by which the computers communicate with each other and carry out the exchange of data (like DNS and Transmission Control Protocol and Internet Protocol (TCP/IP); and the **applications** and standards that enable computers to communicate with users, including, for example, Hyper Text Markup Language (HTML) for web browsing, the protocols for email clients (the post office protocol, known as POP, Simple Mail Transfer Protocol (SMTP), streaming video, web servers and browsers used for authentication, error checking, and retrieving files.

Policy challenges related to the infrastructure include building regulatory environments (national, regional, and global) for a competitive market with spectrum regulation; offering incentives for investment in broadband infrastructure (especially the last mile); setting up Internet Exchange Points (IXPs);[12] offering incentives for development of local content and services and preservation of the open and neutral Internet; managing the Internet domain names and IP addresses – including decisions about the new generic Top Level Domains (gTLD),[13] administering the root zone servers and file;[14] transitioning from the outdated Internet Protocol version 4 (IPv4) to the new Internet Protocol version 6 (IPv6)[15] and developing cloudcomputing services and supporting infrastructure (data farms, cashing servers) within desired strategic coordinates with regard to the technical aspects of security, privacy, and data protection.

Issues that address the security and stability of the Internet infrastructure are strongly linked to infrastructure, but are here comprised in another group which will be discussed in the section on cybersecurity.

While the engineers are certainly most qualified to discuss the infrastructure and technical standards, due to the growing strategic importance of the Internet for countries and communities, the decisions about standards are not any more the exclusive interest of engineers: influence in setting future standards of the Net could result in strategic advantage in industry development, security (both defence and offence), and surveillance options, as the case of PRISM global surveillance programme of the NSA in mid-2013 illustrated. For the same reason, the management of the critical Internet resources – the domains and the DNS, as well as the IP numbers – represents a high-pitch political and diplomatic topic. The review of main infrastructure-related political controversies is presented in Table 2.

Table 2. Main IG infrastructure issue controversies

Issue	Controversies	Proposed solutions
Telecommunication Infrastructure	Review of International Telecommunication Regulations (ITRs) at the Dubai Conference (December 2012).	ITRs are the key instrument in the global telecommunication policy. In the past, they mainly regulated questions of the telecommunication infrastructure. Some governments (e.g. Russia, Saudi Arabia, Iran, and China) opted for extending the ITRs' coverage to broader IG issues, possibly including the management of CIR, security and content issues. ITR negotiations were one of the decisive IG developments in 2012, resulting in high polarisation between developed and developing countries.
Transport Control Protocol/Internet Protocol (TCP/IP)	How to deal with the limitations of IP numbers and facilitate the transition from IPv4 to IPv6 especially in developing countries, and how to assure fair global distribution.	This transition requires awareness, knowledge and skills, and new equipment. Delay in this transition, especially in developing countries, may result in an inability to access new services that will be increasingly IPv6-only.

Issue	Controversies	Proposed solutions
The Domain Name System (DNS)	Introduction of new generic top level domains (gTLDs)	On 12 January 2012, ICANN began the registration process for new gTLDs. Controversial preparatory discussion between governments, trademark lobbies, and international organisations about implementation of new gTLDs seek resolution for the process. The political divide between different constituencies within ICANN (commercial, non-commercial, governmental, and the board) is widening with disagreements about 'objectionable' gTLDs like '.amazon' and '.wine'.
Internet root servers	Internationalisation of control of root servers Proposed sentence How can oversight of the root server transition from one government (USA) towards a more inclusive and global arrangement?	States have concerns about the current arrangement in which the ultimate decisions about the content of root zone files, stored in the root servers, remains the responsibility of the USA, through the delegated function of IANA. The US announcement of the intention to end US oversight over ICANN will also open the question of the function of IANA function and the supervision of the root servers. Solutions are likely to be sought in ICANN reform through globalisation, and a possible relocation outside the USA. One solution could be to grant international inviolability to the root zone file and root servers.[16]
Net neutrality	Maintaining the open Internet by limiting the ability of Internet (access and broadband) providers to block or throttle certain types of traffic or services.	On one side, Internet providers (especially major telecom providers and their associations, such as the European ETNO) ask for an unregulated market that would allow 'specialised' or 'managed' services –faster delivery and better quality of service for over-the-top (OTT) services that are willing to pay for such treatment (possibly Google, Facebook, etc.) – to run in parallel with the 'unrestricted Internet'. On the other side of the discussion, Net neutrality is requested through equal treatment of the Internet traffic. This approach is supported by civil society and most of technical community. In addition, there is a rising trend in European countries to guarantee Net neutrality by law: the Netherlands, Slovenia, and Luxembourg.

5.2. Legal basket

Principal legal issues are more within the grasp of today's diplomats, dealing with issues addressed in major global forums. Nonetheless, there are increased complexities due to the debate over 'real' law versus 'cyber' law, and implications such as the following:

5.2.1. 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. The cross-border nature of Internet exchange has increased complexity for determining jurisdiction. The state of origin, state of transaction, state of purchase, and state of manufacture may vary with physical merchandise, and be even harder to trace with *digital* merchandise, for example. Cyber crime similarly can complicate jurisdiction as the attribution – even a physical location for the crime, whether it be a security breach or child pornography – may be hard to determine. Dealing with jurisdiction will be one of the key challenges in the implementation of international Internet regulations.

5.2.2. Arbitration

Arbitration is an area where Internet issues have required new dispute resolution resources. For example, the case of domain name (such as whether there is a limited right to cocacola.com, mcdonalds.com or the like) disputes, problematic issues may arise from trademark rights. The Uniform Domain-Name Dispute-Resolution Policy (UDRP) was negotiated by the World Intellectual Property Organisation (WIPO) and is overseen by ICANN to resolve disputes in this area. Other controversies and e-commerce may require new techniques to address jurisdiction and other elements.

5.2.3. Intellectual property rights (IPR)

Internet file-sharing, copyright, and digital rights management have complicated the arena of IPR. Citizens have always lent and borrowed books, and audio disks and tapes. Does that mean they can share digital files? Digital files are more easily copied than hard copies, and are open to manipulation and commercialisation in new forms, often across borders. The Anti-Counterfeiting Trade Agreement (ACTA), Stop Online Piracy Act (SOPA), and PROTECT IP Act (PIPA) caused global controversy and protests, indicating the level of importance these issues have for business, states, and citizens. These dilemmas will need to be addressed by professionals who understand the technical, legal and diplomatic implications of the issues, in the search for a balanced solution.

5.2.4. Labour law

Not only online or teleworkers, but even traditional office workers may now be expected to check e-mail, and be 'on call' for more hours each day, and even on traditional weekends and holidays. Will this affect labour policies? Some companies surveil and control their employees' Internet access and use, and often claim the full ownership of their employees' data stored within the used computers or email accounts. This raises serious questions of privacy and other rights. Will states need to intervene both domestically and internationally to protect their own and their citizens' rights?

Issue	Controversies	Proposed solutions
Arbitration/ Jurisdiction	How to address the increasing number of court cases on the Internet involving cross-border elements.	• Improve efficiency of traditional jurisprudence by using International Private Law. • Adjust traditional arbitration for Internet cases. • Develop a new approach based on arbitration (such as UDRP).
Intellectual Property Rights (copyright)	ACTA-triggered controversy: how to strike the right balance between protection of IPR and fair use of protected materials. How to enforce intellectual property rights in cyberspace.	• Introduce a new legal framework which would involve stricter protection of IPRs (ACTA attempt). • Amend the existing international legal framework (WIPO/WTO) in order to achieve the right balance between protection of IPR and fair use.

Table 3. Main IG legal issue controversies

5.3. Cybersecurity basket

The cybersecurity basket includes the following IG issues:

Cyber conflicts, often labelled as cyber wars, have high media visibility. However, this is a rarely analysed aspect of cybersecurity. Cyber conflicts should be addressed through three main areas of the traditional law of armed conflicts: conduct of war (mainly The Hague Convention), weapons and disarmament (what is a cyber weapon and how can it be controlled), and humanitarian law (Geneva conventions and protocols).

Critical information infrastructure protection (CIIP) is ever more important because the global critical infrastructure now depends on the Internet. Many vital parts of global society, including energy, water, and finance, are heavily dependent on the Internet and other computer networks as the information infrastructure. This includes not only the equipment and links, but also the protocols, data centres, and the overall critical Internet infrastructure (CIR). The vulnerability of the Internet is the vulnerability of modern society.

Cyber crime is crime committed via the Internet and computer systems. It includes unauthorised access, damage to computer data or programs, and child pornography, among others. The fight against online child pornography is the most developed area of the international cooperation in the field of cyber crime. This cooperation is missing, however, in tracing and dismantling the global cyber crime black market which offers outsourcing of criminal services, but also dangerous and often easy-to-use digital weapons (e.g. viruses and botnets) to almost anyone.

Cyber terrorism came into sharper focus after 9/11, when an increasing number of cyber terrorist attacks were reported. Cyber terrorists use similar tools to cyber criminals, but for a different end. While cyber criminals are motivated mainly by financial gain, cyber terrorists aim to cause major public disruptions and chaos.

Issues & Gaps	Solutions and approaches
Lack of **international cybersecurity framework** (policy principles,legal instruments and institutions).	Developed economies have a strong economic and political interest in a secure and safe Internet. At the same time they are reluctant to have a comprehensive cybersecurity treaty that could be a backdoor for overall regulation of the Internet; some focus so far on bilateral agreements (like the USA with China), limited multilateral regulation (party to the CoE Convention on Cyber crime), and private security initiatives. The Russian Federation, China, Tajikistan and Uzbekistan submitted a proposal to the UN for an international Code of Conduct for Information Society. In case of adoption, The Code of Conduct would go beyond cybersecurity issues and address overall IG issues; this initiative creates the risk of a 'backdoor' approach, which would undermine the existing check-and-balances and multistakeholder approach in IG. The OSCE adopted a first set of confidence building measures (CBM) on cybersecurity in December 2013. It is a landmark decision, since the OSCE is the first regional security organisation that has not only developed CBMs in cybersecurity, but also adopted them with the consensus of 57 member states. The ITU uses a comprehensive approach, including: - Policy level: the Global Cybersecurity Agenda – GCA and keeping cybersecurity track in the follow-up to the WSIS (Action Line C5). - Legally binding level: the amended International Telecommunication Regulations, adopted in December 2012 by 89 countries while 55 countries have not signed it introduced the articles on security (5A) and unsolicited messages i.e. spam (5B)
Cyber conflicts – conduct Lack of updated rules of conduct of the war. Problems with applicability of existing legal instruments due to specifics of the cyber-space (e.g. problem of attribution).	Can the existing law, mainly The Hague Conventions, be applied to cyberspace? If not, what type of new legal instruments should be developed? Many countries are introducing cyber into their military strategy and operational procedures. There is a risk of increasing militarisation of the cyberspace by having the army in lead of the national cybersecurity efforts. Global discussion is still in decision-shaping phase. NATO-commissioned *Tallinn Manual* is one elaborated analysis of the application of existing international legal instruments.
Cyber conflicts – weapons and disarmament Need to define cyber weapons and introduce them into the disarmament processes.	Most weapons used for possible cyber warfare originate from the global black markets and are primarily used for cyber crime, then also adopted by states. Since most cyber weaponry comes from cyber crime, a practical disarmament could be achieved by increasing cooperation against cyber crime. A broader, more diplomatic, disarmament process will require more time and political support from the main cyber powers.
Cyber conflicts – humanitarian law Need to identify and regulate specific humanitarian aspects of cyber war attacks.	An analysis of the impact of cyber conflicts on humanitarian issues is in its early stage. This link is particularly relevant for Geneva, as a global humanitarian capital. In the first phase, an analysis of this link will crystallise various policy linkages and issues through research and events (workshops, seminars, and panels). In the second phase, some proposals could be moved from decision-shaping to decision-making spaces (e.g. draft proposals).

Issues & Gaps	Solutions and approaches
Critical information infrastructure protection Lack of global regulatory framework and policy mechanisms.	Two main approaches: - Bottom-up: develops current network of professional organisations (Computer Emergency Response Teams (CERTs). This approach has been initiated by the G7/G8 and supported by the USA and most developed countries. - Top-down: includes protection of critical infrastructure in cybersecurity treaties and ensures its protection through newly established international mechanisms (hosted by the UN or the ITU); supported by China, Russia and many developing countries.
Cyber crime Lack of global legal instrument on cyber crime.	There are three main and mostly competing approaches: - The CoE is trying to extend coverage of the existing cyber crime Convention to a global level (advantages: existing, well-established practice, adopted by the CoE – it has strong human rights tradition; disadvantages: certain sovereignty clauses are not acceptable by some countries such as Russia; The Convention needs updating).
	- The ITU utilises a holistic approach to become the host of the defining 'global arrangement against cyber crime' (a) it offers a bottom-up approach with model cyber crime law for states; (b) it features cyber crime prominently in the Global Cybersecurity Agenda; (c) it provides technical assistance and capacity building; (d) it has included cyber-security in the new 2012 ITR. - The UN Office on Drug and Crime: trying to extend its crime conventions and instruments to cyberspace.
Cyber terrorism Lack of coordinated global approach and balance between anti cyber terrorism measures and protection of human rights.	XYZ The policy action should focus on three main areas: - Lack of a globally agreed definition of cyber terrorism.[17] - Strengthen cross-border cooperation. - Improve public-private partnership. - Introduce balancing acts in dealing with cyber terrorism and human rights. The Global Counter Terrorism Forum could emerge as the appropriate platform to address cyber terrorism.

Table 4. Main cybersecurity issue controversies.

5.4. Economic basket: Internet money politics

One possible way of analysing IG issues is to follow the flow of money in the digital economy. Who pays for the Internet? What is the economic chain on the Internet? How is profit generated on the Internet? In essence, there are two business models that run the Internet economy: the Internet *content* business model and the Internet *access* business model.

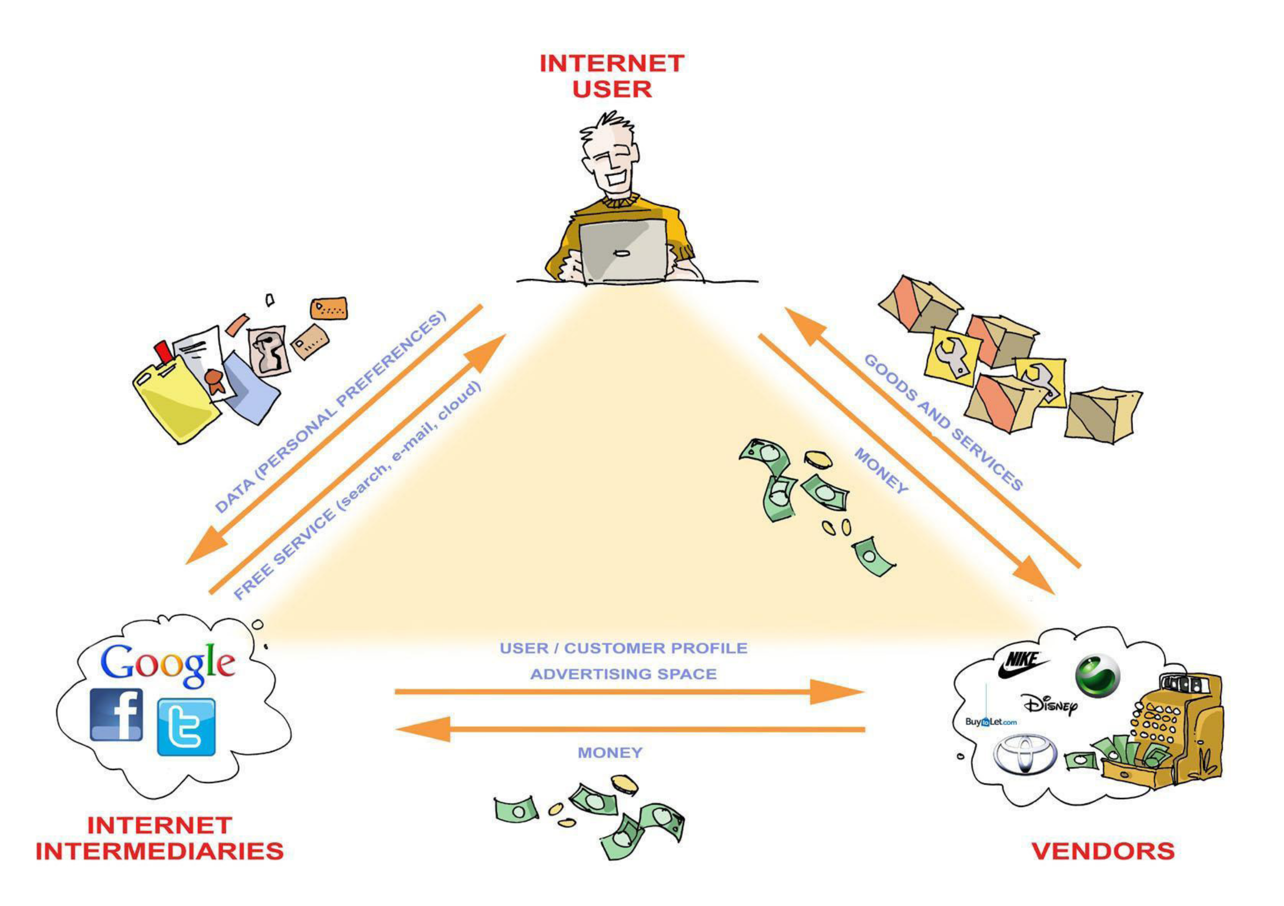


Figure 6. Internet content model.

5.4.1. Internet CONTENT business model

At first glance, the Internet content business model is counter-intuitive since it appears that there is no money flow. We can search on Google, use e-mail, socialise via Facebook, and save our photos on Flicker without paying a penny for these services. Taking it that there is no such thing as a free lunch, we may well ask who *is* paying for it. Internet companies have to design these tools, run powerful servers, and provide support. All of this costs money.

If we do not pay for searches, e-mail, and storage, it remains to be seen how the Internet content companies became financially so successful.

The currency we use to pay Internet companies is our data, or the information we generate – our 'electronic footprint' – as we search or communicate on the Internet. Internet companies analyse our data in order to extract bits of information about our tastes and preferences. They learn how people interact and influence each other. They also mine the data to extract information about a group, for instance the behavior of teenagers in a particular city or region. They are able to predict what a person with a certain profile is going to buy or do.

Internet companies sell this information/data to various vendors, who use it for better defining their marketing and selling. In 2011, 96% of Google's US$37.9 billion annual revenue came from this type of service and advertising.

Currently, there is a tacit deal between Internet companies and users that we provide free data about ourselves in exchange for a free service. This tacit deal is increasingly questioned.

5.4.1.1. Customer protection

Problem: Do we make informed decisions by clicking 'I agree' to long, fine-print contracts required by Internet companies such as Google and Facebook? In most cases, we do not. While formally speaking, we accept the conditions proposed by companies, we may not make an informed decision protecting our interests.

Possible action: Public authorities should require clear, comprehensible summaries of terms of service that are understandable to end users. Choices, data management policies, and default settings should be stated clearly. When terms or conditions depend on foreign jurisdictions, this should be clearly indicated to the final user as well. States should require Internet companies to have legally acceptable solutions (e.g. data protection in accordance with internationally accepted regulations) as a default with the possibility for users to derogate (opt out) of this protection by deciding to share more information.

5.4.1.2. Market monopolies and transparency

Problem: The nature of the Internet industry is prone to the establishment of market monopolies (e.g. Google's share of Internet searches is more than 80% in Europe). The risk for market monopolies is also increased by the little transparency in how the Internet industry operates. For example, vendors factor their advertising costs into the price of the goods and services they sell to us. It's the same thing as traditional advertisements in the paper. This service is hidden, though, and the final price may be excessive. As the recent case with Booking.com shows, we may end up paying much more for our holidays than if we were to book directly through hotels or traditional travel agencies.

Possible action: Since most Internet companies are based in the USA it will complicate matter for many national anti-monopoly authorities. It is very likely that the solutions will be negotiated and set by the EU's anti-monopoly authorities which have leverage (market of 500 million people) to force Internet companies to follow the EU's market regulations. The EU initiated anti-monopoly action against Google, focusing on – among other issues – the positioning of paid advertisement on the list of search results. Other countries with smaller Internet markets and less policy leverage are likely to follow an arrangement negotiated between the EU and Internet companies.

5.4.1.3. Cloud computing and data protection

Problem: Cloud computing is the shift of data from computer hard disk to servers in the clouds (i.e.big farms of data servers). Data generated by Internet content companies is stored in the clouds. Most of the digital clouds are owned by leading Internet companies: Google, Microsoft, Apple, Amazon, and Facebook. One of the main questions is that of privacy and data protection. In addition, with a growing volume of information assets going digital, countries are becoming increasingly uncomfortable about having national information assets stored outside national jurisdiction. Snowden's revelations – in particular those related to access by the NSA to personal data hosted by Internet companies – accelerated discussion on the status of digital cloud. Brazil and the European Union have been considering possibilities of developing national and regional clouds.

Possible action: States must require more transparent regulation of the use of clouds. The existing international regimes on data protection and privacy protection should be applied to clouds as well. If implementation mechanisms are not regulated, they should be developed at international level.

5.4.2. Internet ACCESS business model

Individual Internet users and organisations pay ISPs for Internet access and services. Typically ISPs have to cover the following expenses from the fees collected:

- Cost of telecommunication expenses and Internet bandwidth to the next major Internet hub.
- Cost for IP addresses obtained from regional Internet registries (RIRs) or local Internet registries (LIRs). An IP address is needed by a device to access the Internet.
- ISPs also have to pay for equipment, software, and maintenance of their installations.

5.4.2.1. Re-distribution of revenue between telecommunication and Internet companies

Telecommunication operators are raising the question of re-distribution of the revenue generated by the Internet. They are trying to increase their share of the 'revenue pie' generated by the

Internet economic boom. So far, the main business beneficiaries of the Internet's economic growth are Internet content companies due to their innovative business model based on online advertising. The telecommunication companies argue that their share in the profit should be increased since they facilitate access to Internet content through their cables and telecommunication infrastructure.

Thus, they should have a higher income from Internet-generated revenue which should help them invest in the upgrading of the telecommunication infrastructure. Content companies, on the other hand, argue that access providers already charge the end users for Internet access, and that the main reason for their alleged lower incomes are their obsolete business models ('all you can eat' charges like flat rates). European telecommunication operators organised into the European Telecommunications Network Operators' Association (ETNO) created a lot of waves during the preparation for WCIT Dubai by making a concrete proposal that would alter the current revenue model by proposing that content providers (Facebook, Google) pay for access to their services. The proposal, which was officially proposed at WCIT Dubai by Cameroon, did not gain support, but is likely to remain an open issue in future IG negotiations. This discussion strongly underpins the network neutrality debate – for example, should all Internet traffic have the same status as it is today, or should it be segregated into different Internet(s) depending on the quality of services, payment and reliability (e.g. having a range of Internets from VIP to the Internet for poor).

5.4.2.2. Problem of telecommunication revenue sharing with developing countries

Many developing countries have been complaining about the unfavourable 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 – the developing countries that have to connect to backbones located mainly in developed countries. As a result, paradoxically, small and poor countries may end up subsidising the Internet in developed countries.

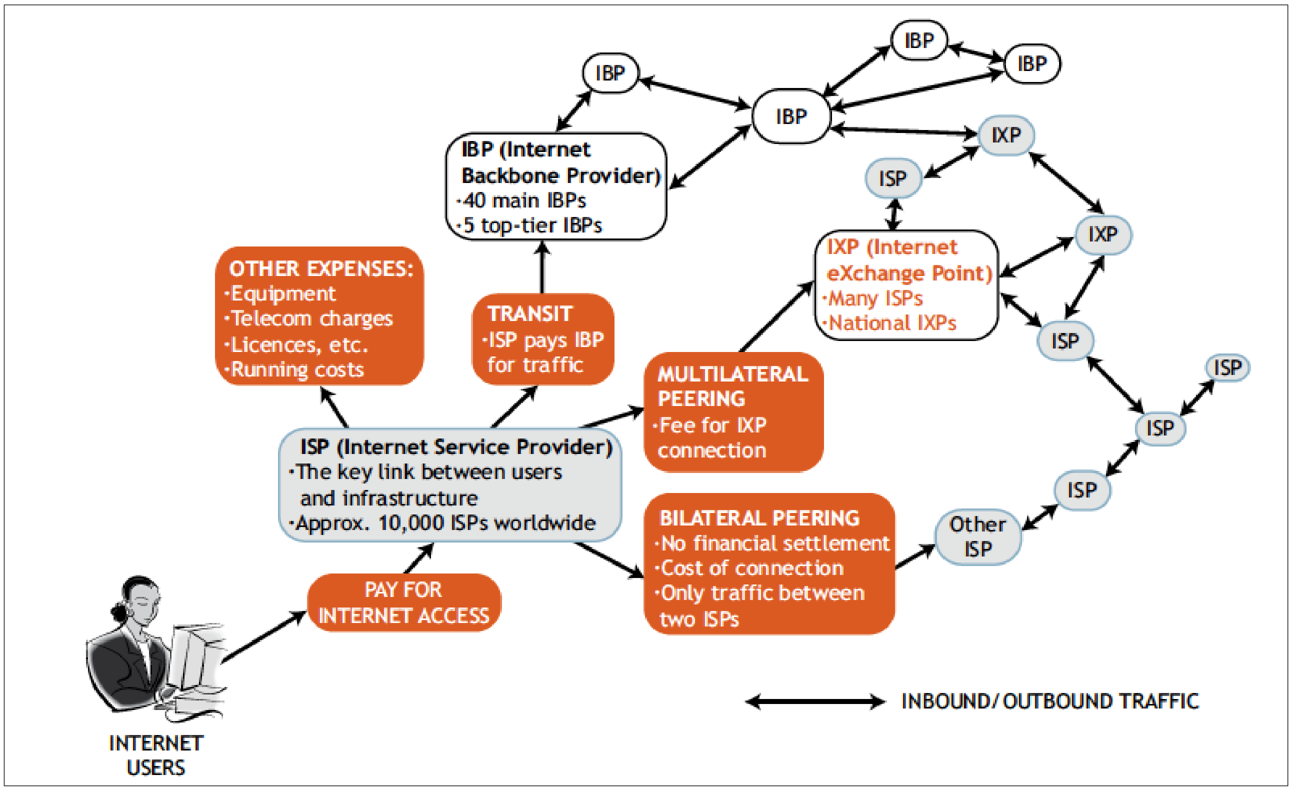


Figure 7. Internet access model.

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 are raising the question of fairer Internet access business models during WSIS, ITU working groups and, recently, at the WCIT Dubai negotiations.

5.5. Development basket

The most significant concern about the so-called digital divide is that Internet resources and access be best utilised to decrease the digital another divides. New Internet resources must offer opportunities and support for least developed and developing countries. Vigilance must be carried out that technologies do not increase the divide for the have-nots, as the developed and richer countries use Internet innovations to improve their positions.

In the highly interdependent network, IG in developing countries is relevant for the overall stability of the Internet. Developing countries are often the 'weakest link' in cybersecurity protection chain. Thus, by strengthening IG capacity of developing countries, the resilience of the overall network is addressed.

Development issues are generally of a cross-cutting nature. Other IG issues have development aspects, and they are often addressed in those areas. For example, the questions of access and costs are discussed in infrastructure strategies. Legal and IPR issues affect access to knowledge, applications and copyrighted materials. Developing economy advantages and disadvantages are appropriately discussed in the relevant economic issues.

Switzerland could also contribute to bringing the digital dimension to sustainable development, in the context of the Post-2015 Development Agenda. In some areas, such as capacity development and management of e-waste, Switzerland has already made a major contribution which is globally acknowledged as a practical, innovative, and concrete contribution to both fields: the Internet and sustainable development.

5.6. Human rights basket

IG is increasingly addressed through human rights perspectives. The Snowden revelation put in the focus the question of online privacy and data protection. In addition, the human rights are central for the business model used by the Internet companies such as Google and Facebook. The freer data move on the Internet the more income Internet industry generates and vice versa.

The human rights debate is centred on two sets of inter-related issues: freedom on the Internet, and protection of privacy and data. The USA, developed countries, and the Internet industry are strong supporters of the 'freedom' set of issues, including freedom of expression and freedom of information. Besides values and ethical aspects, the Internet industry (e.g. Google, Facebook) has a business interest in promoting freedom of information, since the more data they can access and use, the more profitable their business will be.

Brazil and Germany, as the countries most affected by NSA surveillance, lead a coalition of countries and actors lobbying for stronger protection of online privacy. The main issue is how to protect personal data collected by major Internet companies and stored on servers in so-called clouds. European countries have a higher level of privacy and data protection than the USA. One of the main challenges is how to apply European privacy and data protection rules for data of their citizens and institutions stored on servers abroad, mainly in the USA. The Safe Harbour agreement between the EU and the USA has been one – so far unsuccessful – attempt to bridge regulation differences. Another approach, which is increasingly promoted by Germany and other European states, is to adopt a 'data protocol' in the International Covenant on Civil and Political Rights from 1966 which should apply the Covenant's rules on privacy and data protection to the digital world.[18]

Switzerland should extend its human-centred foreign policy to the digital field. Switzerland's concrete contribution could be in streamlining the digital dimension in reporting of the various human rights bodies and Universal Periodical Review process. The vibrant human rights policy scene in Geneva could be the place for discussing and nurturing new approaches and ideas that ensure the protection of human rights in the digital space.

Switzerland can make a major contribution by addressing cybersecurity and human rights in a multidisciplinary way (Section 5.8).

5.7. Sociocultural basket

Sociocultural issues include content policy, preservation of language, and cultural diversity. They have a strong link to human rights, such as access to information, freedom of expression, and the right to communicate.

Table 5. Main human rights controversies.

Issue	Controversies	Proposed solutions
Addressing human rights in a holistic way	How to establish the right balance between freedom of expression and protection of public order on the Internet. How to deal with cultural differences in dealing with global policy.	The process of dealing with human rights issues was initiated at the UN Human Rights Council. A way of achieving the right balance in other policy areas should be also used in addressing digital human rights.
Privacy and data protection	How to protect personal data collected by major Internet services such as Facebook, Google and Twitter and others. Since the business model of these Internet companies depends on access to their user's data, the question of privacy and data protection has high economic relevance.	Possibilities include: - Extending European (higher) level of data protection to other regions and countries (opposed by the USA) - Implementing a compromise solution such as Safe Harbour agreement (USA –EU) Privacy and data protection is likely to influence major developments on the Internet, including future economic models (advertising) and cloud computing.
Freedom of expression	Discussion on freedom of expression online reflected general discussion on freedom of expression. Freedom of expression was strongly promoted by Sweden, USA and other western countries. The other side – China, some Arab countries – insisted on addressing freedom of expression in the broader context of human rights.	Besides multilateral processes dealing with the freedom of expression (e.g. UN Human Rights Council), there is a need for awareness building and capacity development in the field of freedom of expression on the Internet.

Issue	Controversies	Proposed solutions
Content control	How to ensure the free flow of information while addressing problems with child pornography and hate speech.	High level of controversy and different views; unlikely to establish international regime; a possibility of introducing filtering for internationally prohibited activities (e.g. child pornography).
Multilingualism	While there is a strong support for multilingualism among all players, controversies are mainly related to the way how to implement multilingualism without endangering universal access to all Internet resources.	It should be supported through activities of various standardisation and technical bodies.
Online education	Are online learning courses commodity or a public good? If they are considered a commodity, the WTO's free trade rules will be used. If online education is a public good, providers will have status as institutions of importance for national culture.	The status of online education is discussed within the WTO – interpretation of the GATS regulation. It is also introduced in the policy processes in the UN Human Rights Council in the context of Internet freedom.

Table 6. Main sociocultural controversies.

5.8. Policy area for multidisciplinary action by Switzerland

Like many other countries, Switzerland should select priority areas which both reflect Swiss core values and interests and comparative advantages that Switzerland can contribute to the international community. Three specific areas should be in focus: cybersecurity, digital human rights, and innovation-friendly business regulation. The selection is based on the protection of vital interests (the Internet as a critical infrastructure), core principles of Swiss foreign policy (the promotion of human rights), and economic well-being (ensuring policy environment for the growth of Swiss economy). In all three areas Switzerland can contribute as an active facilitator of the policy processes, a mediator in controversial issues, and a provider of innovative solutions.

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 (freedom of information, privacy, access) is not only a value-based priority, it is also a very practical tool for ensuring that the Internet remains open and secure. Human rights are a matter of cyber realpolitik.

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

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 Swiss cybersecurity strategy includes reference to links between cybersecurity and human rights.[19] The EU's cybersecurity strategy considers protection of human rights as one of its five strategy pillars.[20]

Cybersecurity and human rights are closely linked to business and economic well-being. Internet stability and safety is vital for the growth of e-commerce. In addition, the way human rights issues such as online privacy addressed directly affect business model of the Internet industry. Competition law should avoid the creation of digital monopolies that could block innovative growth. Consumer law should protect users as a vital and creative segment of the Internet economy (contributors of blogs, tweets, and photos). Standards should ensure open interoperability among different platforms (e.g. having simple and transparent ways to move content from one platform – for example, Facebook – to new platforms created by start-ups). By ensuring innovation-friendly regulation on the global Internet, Switzerland will provide space for its – still under-developed – Internet industry to grow in the future.

Switzerland can provide a valuable contribution to the international community by building a functional and balanced interplay between cybersecurity, human rights and Internet business. By doing this, Switzerland would also promote its core foreign policy principles (national security and human rights), as well as the unique Swiss expertise in fields such as human security (e.g. soft security). In addition, Geneva is ideally placed for such discussion since it hosts the key international organisations for human rights (the UN Human Rights Council), cybersecurity (the ITU, UN Conference on Disarmament, the IETF via ISOC) and Internet business (WTO) and many other NGOs and business organisations dealing with interplay among these three areas.

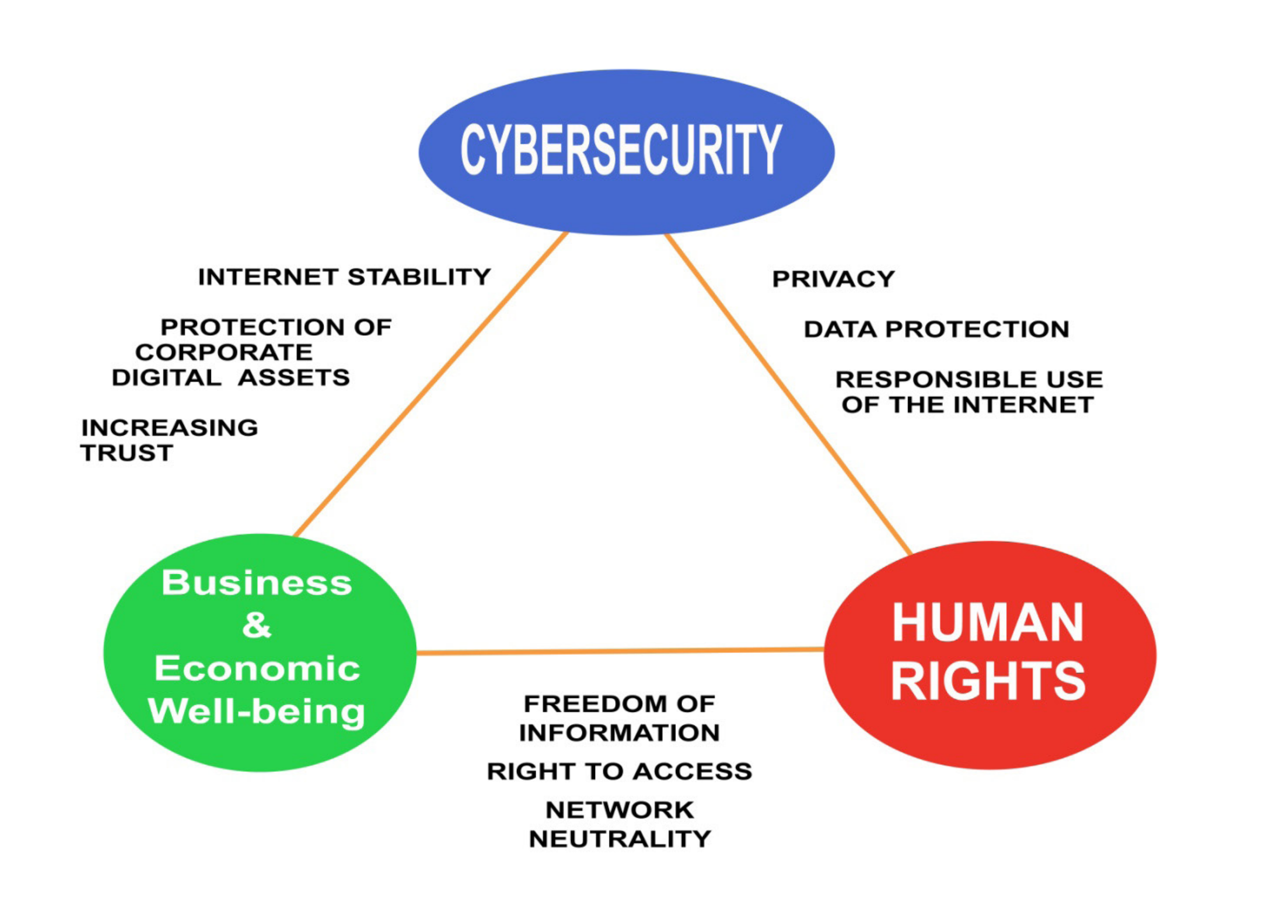


Figure 8. Priority IG issues and their interplay.

WHO are the main players?

At the moment, IG involves a wide variety of players, or stakeholders, as they are often called. Internet stakeholders include national governments, international organisations, the business sector, civil society, and the technical community (as specified in the article 49 of the 2005 Tunis WSIS Declaration). Their degree of legitimacy varies markedly, and with it, their accountability. While multistakeholderism is adopted as a principle, the main debate is on the specific role of each actor focusing mainly on the relation between state and non-state actors. The most prominent players are national governments and the business community.

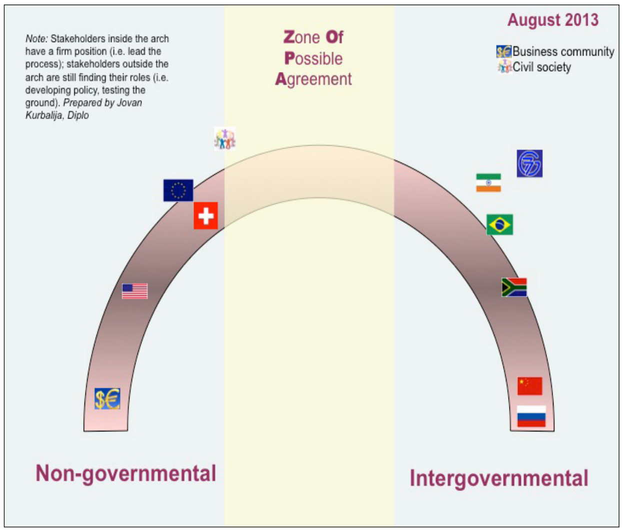

August 2013
Note: Stakeholders inside the arch have a firm position (i.e. lead the process); stakeholders outside the arch are still finding their roles (i.e. developing policy, testing the ground). Prepared by Jovan Kurbalija, Diplo
Zone Of Possible Agreement
Business community
Civil society
Non-governmental
Intergovernmental

Figure 9. Position of the main actors in Internet governance (January 2014). For details see Annex VII: Internet politics - position of the main actors

National governments are late arrivals to IG. With the exception of some of the developed world (the USA, EU member states, Australia), most countries got involved in IG during the last 10 years, within the framework of the World Summit on the Information Society (WSIS) held in Geneva (2003) and Tunisia (2005). An IG policy spectrum started to take shape with countries developing their national positions. On one side of the IG spectrum lies the USA and like-minded countries, who argue for the maintenance of the current, predominantly, non-governmental IG model. On the other side sit Russia and China, who argue that the Internet should be governed at the international level by inter-governmental organisations, such as the ITU.

XYZ

The USA is the most powerful and important player in IG. It is the birthplace of the Internet, and home to Google, Facebook, and Twitter, major global Internet companies. For the USA, IG has a complex interplay of political, security, and economic aspects. For example, the USA's oversight of ICANN, including the possibility of deleting a country's domain name, is often quoted as the source of US power over the Internet. This is not real power, however, since it cannot be used. The power element would require forcing the other side to act in a way the power holder wants. If the USA actually used its power over ICANN, this would have far-reaching, unintended consequences, including countries and regions establishing their own separate Internets. Every new national digital border would reduce the market space of the US-based Internet industry (Google, Facebook, and Twitter). Fragmentation of the Internet would also be detrimental for the global promotion of US core values, including democracy and freedom of expression. This is one of the reasons why the USA has been extremely careful as the guardian of ICANN, and why it has a strong interest in finding a new global arrangement for ICANN that will ensure the existence of a unified Internet. In this context, the US National Telecommunications and Information Administration (NTIA) initiated on 14 March 2014 a policy process aimed at transferring the super vision of the Internet Assigned Numbers Authority (Internet 'address book' IANA) from the NTIA and US government to appropriate global body or policy mechanism. This transition should be completed by the 30 September 2015.

While the ICANN arrangement is likely to be finalised by September 2015 (when the current oversight agreement expires), a more strategic issue will be regulation of data as a key resource of the Internet industry. As a consequence of the Snowden revelations, countries will aim to preserve as much of their data as possible within their own national borders. Although trends towards the 'nationalisation of data' are inspired by security and human rights considerations, they may have major impact on the economic interests of the US Internet industry. Thus, it is expected that US Internet diplomacy will shift focus from ICANN-related issues to securing free flow of data through human rights (freedom of information) and trade agreements.

The European Union has a unique mix of hard and soft digital power for forging future IG compromise. The EU's hard digital power is based on the attraction of a wealthy 500-million-person market with high Internet penetration (65%). 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 when, for example, Google controls 82% of the global search market and 98% of the mobile search market, the EU is the only inte national institution that could prevent Google's market monopoly.

The EU's soft digital power is based on some sort of digital jiu-jitsu diplomacy of turning weaknesses into strengths. Namely, the EU does not have any major Internet company since Skype was bought by Microsoft. Paradoxically, this weakness could be turned into strength in IG. 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, and network neutrality). 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 (and the world's) Internet industry. The EU can achieve both ethical and strategic goals, which is not often case in international politics.

One of the main challenges for the EU is the high diversity of IG positions within member states. Scandinavian member states are more often aligned with the US position than the southern one. One new development triggered by the Snowden revelations is the much more active role of Germany, who used to have a low profile in the IG debate. Germany focuses on privacy and data-protection issues.

The EU's approach of developing different issue-based alliances has started to emerge. At WCIT-12, Europe supported the USA; while in discussions about ICANN's status, the EU often allies itself with BRICS and developing countries. On data protection and privacy, the EU's position is close to the position of the Latin American countries.

With the highest number of Internet users, *China* is an important player in IG. It has been balancing digital politics between the economy-driven free communication with the rest of the world and politically-driven filtered access to the Internet for Chinese users. The protection of sovereignty as a cornerstone of Chinese foreign policy is also mirrored in cyberspace. Lu Wei, Minister of China's State Internet Information Office, said: 'Just as the seventeenth century saw the extension of national sovereignty over parts of the sea, and the twentieth over airspace, national sovereignty is now being extended to cyberspace.' 'Cyberspace', he said, 'cannot live without sovereignty.'

China achieved a high level of 'digital sovereignty' by banning and/or restricting access to the Chinese market for foreign Internet companies (Facebook, Google, Twitter) and developing Chinese social media companies such as RenRen and Sina Weibo. Most of the data belonging to Chinese individuals and institutions are stored on servers in China. In foreign digital politics, China supports an inter-governmental approach. However, it keeps a low profile, leaving Russia and other countries to lead the inter-governmental initiatives in global forums.

Russia has been the most vocal and consistent promoter of an inter-governmental approach to IG. At WCIT-12, Russia tried to include the Internet in the ITU's work through the ITRs. Russia also has a strong focus on cybersecurity through the work of the first committee of the UN General Assembly.

India is one of the swing countries in the IG debate with diverse – sometimes conflicting – positions on IG. India's diplomatic service supports an inter-governmental approach to IG. India's business sector, with strong ties to the US ICT industry, promotes a non-governmental approach to IG. This dichotomy has created some surprising moves. For example, India proposed the establishment of the UN Committee for Internet-related Policies (CIRP) as a way to achieve inter-governmental oversight of critical Internet resources. However, it shifted to the other side of the Internet policy spectrum by siding with the USA and other developed countries at WCIT-12. India did not sign the amended ITRs and departed from the position of the G-77 countries. This surprising move was explained by the huge lobbying power of the Indian ICT industry.

Brazil has been one of the most active countries in global digital politics. 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 IG debate (inter-governmental and non-governmental). This role became obvious in the aftermath of the Snowden revelations. As one of the main target of the massive NSA surveillance, Brazil took strong diplomatic action. In her speech at the 68th Session of the United Nations General Assembly, Brazilian president, Dilma Rousseff, requested that: '[t]he United Nations must play a leading role to regulate the conduct of states with regard to these technologies.' In addition, she defined the surveillance as 'a breach of international law' and 'a case of disrespect to the national sovereignty' of Brazil. When it seemed that Brazil was sliding towards the inter-governmental side of Internet policy spectrum, President Rousseff shifted back to the middle space of the policy spectrum by proposing to co-organise a NETmundial aimed at further developing multistakeholder IG. Brazil had a complex role at NETmundial. Brazil's main aim was to ensure the successful outcome of NETmundial. It reduced Brazil's room to manoeuvre. If the meeting had been held somewhere else, Brazil would have been more assertive on many substantive issues, including Net neutrality and surveillance. At the NETmundial, Brazil could not manage to maintain BRICS solidarity: Russia openly opposed the NETmundial declaration; India expressed serious concerns and delayed adoption of the outcome statement; and China and South Africa kept a very low profile. It remains to be seen if Brazil's high convergence capacity to foster a middle ground in IG negotiations will be tarnished by the distancing of some core BRICS partners. At the first post-NETmundial major event – the meeting of the UN Commission on Science and Technology for Development (CSTD) – Brazil adopted a low profile and did not lobby extensively for the reference of the NETmundial in the CSTD resolution as it was proposed by some developed countries. The reference for NETmundial will take lower profile by being mentioned in the CSTD Chairman's report.

The Swiss government has been one of the most active players in IG. In the forthcoming period, Switzerland can play an important role in creating a 'zone of possible agreement', together with other prominent actors (e.g. European Union, Brazil, India).

The business community is the other powerful group in IG, as it includes a wide range of players: Internet content companies (e.g. Google, Facebook, Disney, Skype),[21] domain name vendors (e.g. VeriSign, Nominet), Internet service providers (ISPs),[22] telecommunication companies,[23] and software and hardware developers (e.g. Microsoft, Cisco). The main players are Internet content companies, basing their business models on the freest possible access to data. The more data they can collect, process, and use, the more profitable their advertising-driven business model becomes. The Internet content companies are averse to public supervision and policy restriction, especially on the international level.

One can expect increasing tension between governments willing to impose norms on data protection, and Internet content companies, who will remain in favour of a de-regulated environment. These tensions will be heightened by the fact that the main Internet companies and intermediaries are beyond the reach of most national jurisdictions and can be legally accountable to the USA authorities.

Switzerland does not have any company among 50 leading Internet companies. Its Internet industry is still in its infancy. It is reflected by the low involvement of the Swiss Internet business sector in the IGF and other IG processes.

The technical community, finally, includes institutions and individuals who have developed and promoted the Internet since its inception. Historically, members of the technical community were mainly linked to US universities, where they worked primarily to develop technical standards and establish the basic functionality of the Internet. Today, the technical community is centred on ICANN and the Internet Engineering Task Force (IETF) which operates under the Internet Society (ISOC) and develops and promotes Internet standards. The technical community has been an important actor in the process of both establishing and running ICANN. Its legitimacy has been based on the fast growth and reliability of the Internet.

In spite of CERN being the cradle of the World Wide Web, Switzerland has low participation in this segment of IG today. More efforts should be made to involve the Swiss technical community in Internet-related standardisation processes. Three prominent players in the Internet-related standardisation are based in Geneva: the ITU, the International Standardisation Organisation (ISO), and the International Electrotechnical Commission (IEC).

Among **International organisations,** the most prominent player has been the Geneva-based ITU, the central organisation in the WSIS process. The ITU's area of competence (telecommunication) is the closest to IG among all international organisations. This is why China, Russia, and some developing countries see the ITU as the main international player in IG. This possibility triggered strong opposition from the USA and most developed countries, especially during the WCIT Dubai process. Other international organisations involved in IG include those that deal with traditional issues transformed by the Internet: intellectual property (WIPO), trade (WTO), crime (UNODC and Interpol), human rights (CoE), culture and education (UNESCO), and development (UNDP).

The main challenge will be how to address the multidisciplinary nature of most IG issues, which cannot easily fit into the issue-specific mandates of specialised organisations (the ITU – telecommunications, WIPO – intellectual property, WTO – trade, UNESCO – culture and education).

Main Internet-related international organisations (the ITU, WIPO, the WTO) are based in Geneva. Switzerland is an active player in specialised international organisations. In addition, it has a particularly fruitful cooperation with the CoE. Switzerland and the CoE are initiators and leading players of the European IGF.[24] *Future Swiss involvement with the CoE could be beneficial because of CoE's unique coverage of cybersecurity and human rights issues (suggested Swiss priorities), advanced form of involvement of various stakeholders in the CoE, pan-European membership, and activities of the CoE. Switzerland should also use its OSCE Chairmanship in order to address cybersecurity issues. Not least, it should influence a greater level of multistakeholderism and inclusive participation within the ITU and other specialised organisations.*

Civil society is often viewed as a supporter of Internet users and an important provider of content, knowledge-sharing, and capacity building. It is a highly diverse IG stakeholder group. The main tension in civil society concerns protecting the global public interest. Some members of civil society, in particular from developing countries, see a stronger government role as the way to counterbalance the enormous power of the Internet industry. Civil society from developed countries, on the other hand, often allies itself with the Internet industry and technical community, especially on the issue of the free flow of data.

In order to perform its important function in IG, civil society must be strengthened. It must increase its accountability and the transparency of its role in global IG as a decision-shaper with a clear strategy of representation of global civil society; it needs to be better skilled to perform traditional diplomacy in order to be able to negotiate its interests directly.

Switzerland has many prominent civil society activists in the IG debate. However, besides few organisations focused on capacity building and online freedoms, there is still low participation of civil society institutions. The situation has started changing after the Snowden revelations with growing interest of civil society for online privacy and data protection issues.

HOW is Internet governance debated?

There is a wide variety of procedures and approaches used to govern the Internet. UN procedures have been used, for instance, by the UN Council on Human Rights to address online freedom of expression. Traditional treaty-making processes were used at the WCIT in Dubai, for negotiating the ITRs. Formal multistakeholder procedures are used by ICANN, while the IETF, the main Internet standardisation organisation, relies on a very informal and consensus-based decision-making process.

In addition to the formal procedures, the following approaches and patterns substantively shape argumentation and overall IG discussion.

Multistakeholder approach is one of the pillars of IG. Non-state actors played an early, leading role in the development and management of the Internet. While other global policy processes, concerning climate change or trade for example, have gradually opened to non-governmental players, in the case of IG, governments were obliged to enter an already existing non-governmental process, managed by ICANN and other non-state actors.

A multistakeholder approach to IG was officially endorsed in the WSIS Tunis Agenda for the Information Society (2005) and operationalised by the establishment of the IGF as a multistakeholder body. Since its introduction, multistakeholderism has been a controversial issue. While it is predominantly considered as a step towards more democratic decision-making, there are views that multistakeholderism could confuse the policy scene and, in the most radical form, undermine democracy and legitimacy in policy-making. The following strengths are usually associated with multistakeholderism:

- *Democracy*: include more people in policy-making by extending the policy space beyond limited political circles both on national and international level.

- *Expertise:* harvest the wide range of knowledge, views, and expertise that could lead towards better policies and laws.

- *Implementation:* spread the ownership of the processes and their outcomes to a wider population, an important pre-condition for full implementation of an agreed policy.

Of these three strengths we can say that the current IG achieved a lot with regard to **expertise**. All major IG spaces (the ITU, ICANN, and the IGF) are examples of very vivid and professional exchanges between different professions. This variety of views contributes to the quality of the policy process.

On **democracy** and multistakeholderism, the following critical arguments are often used:

Can multistakeholderism satisfy democratic potential in the world when almost all citizens of the world are stakeholders IG? The user community is approaching three billion and the rest of the world's population is indirectly impacted by the Internet through infrastructure and services. Medical services, markets, electricity grids, etc., are all related to the Internet. It makes all of the world's citizens – be they connected or unconnected – stakeholders to some extent. In such circumstances one can wonder if there is still a need to use the concept of stakeholders. This criticism of the democratic potential of multistakeholderism usually concludes that if we accept that all citizens are concerned with how the Internet is governed, we can move towards how citizens decide on all other policy matters in functional democracies.

When it comes to **implementation**, there is very little evidence on the relationships between owner-ship of policy processes and level of implementation. It will be an important aspect to follow, especially in areas such as copyright, where there is a low level of compliance with international regulations, especially in developing countries.

Although it has great potential, multistakeholderism has to prove its value as an inclusive and efficient way of participating in policy-making. The following issues should be considered:

- Multistakeholderism cannot substitute traditional representation on both national and international level. Multistakeholder bodies should not substitute for national parliaments or international organisations, especially in dealing with public policy issues (e.g. security, human rights).

- Multistakeholderism should be a fully transparent process with clear roles for all stakeholders. For example, it is not realistic to expect businesses not to lobby in IG forums, but, such lobbying has to be clearly indicated and acknowledged. Civil society organisations also have to have clearer and more transparent organisational structures. In this way, civil society will be more accountable and resistant to capture by undeclared lobbying interests.

- The most controversial issue is decision-making by multistakeholder entities. If a particular entity wants to enact policy and rules, it has to have a decision-making structure. In the case of international organisations, this is done in councils and assemblies with state representatives. ICANN is a good example of a multistakeholder decision-making body. ICANN also shows that decision-making requires a proper institutional setting (representation of various constituencies, due processes, checks and balances, etc.). The main question is representation. ICANN's Board consists of representatives of the main stakeholders involved in the ICANN system. For any multistakeholder body that has to make decisions, the question of representation will come in the focus. Proper and transparent representation is pre-condition for legitimacy on both national and international levels.

Variable geometry characterises the position of most IG actors. Alliances are not fixed. It makes IG more complex, but also provides space for flexible arrangements and compromises without having major conflict, described as a 'digital Cold War'. For example, the same governments (the EU, Switzerland) who were not in favour of a stronger inter-governmental role at WCIT Dubai, have been promoters of more governmental involvement in ICANN activities. The clustering of countries around specific issues provides a more conducive space for trade-offs and possible package deals in IG negotiations.

Intermediaries have the key role in implementing Internet rules and policies. Governments, nowadays, increasingly rely on agents or intermediaries to do their bidding (e.g. collection of VAT by retailers). Compounding complexities, many Internet intermediaries (e.g. Facebook and Google) are beyond the national jurisdictions (with the exception of the USA). This situation creates a broad gap between governments' responsibility to implement rules and their limited means to do so. This gap is particularly noticeable in the fields of cyber crime, intellectual property, and data protection. Some international players, such as the EU, can use their market power to force Internet intermediaries to follow their rules (Microsoft and Google anti-monopoly cases, European Court of Justice ruling on 'right to be forgotten'.) However, there are no international mechanisms to implement legal rules via intermediaries in an efficient and proportional way (i.e. avoid using long and expensive international juridical processes).

The end of territoriality and emerging virtual space has been used to argue that the Internet is different and its governance should be different with implying the limited role of governments. However, there is no stateless space, including cyberspace. Ultimately, any Internet service, the companies that operate them, and the individuals who use are, are under the jurisdiction of some of the 193 states.[25] Internet clouds, where most online data resides, are servers hosted at physical locations under the legal jurisdiction of a specific country. A new concept that should promote the uniqueness of the Internet space is the 'Internet ecosystem'. Wherever there is ample choice, as in markets, the state may stay aloof and limit itself to establishing and enforcing the laws of contracts and property rights. Yet, the state remains the ultimate legal authority over its territory and population, whether physical or online.

That technical solutions are neutral has long been the main argument of the technical community against broader involvement of governments in IG. This view was particularly used in the ICANN-related debates. However, technical solutions are rarely neutral; they favour certain values and policy interests. Thus, Internet policymakers should make a much clearer delimitation between the policy aspects of technical architecture (the responsibility of public institutions) and technical operations (the running of the network). The main battles are fought along this blurring line between designing technical solutions, where policy preferences can be in-built, and running the networks, which is more technical task.

WHERE is Internet governance currently debated?

At the moment, the Internet does not have a dedicated governance venue, such as health (WHO), trade (WTO), or intellectual property (WIPO). One of the reasons is its unique historical development, which grew out of a very informal technical community of governance. While in other negotiations (e.g. climate change), inter-governmental spaces gradually opened to non-government actors, in IG, governments had to enter an already existing non-governmental regime, built around ICANN and ISOC. The currently dominant policy spaces for addressing IG are:

1. The ITU, which is preferred by those who argue for inter-governmental management of the Internet.

2. ICANN, a showcase of non-governmental space that currently manages the global core Internet resources (CIR) – domains names and numbers.

3. The IGF – created by the 2005 WSIS as a compromise between inter-governmental and non-governmental approaches – aims at bridging these two spaces. Over the last few years, there have been discussions and attempts to empower this deliberative forum by adding more coordinating and policy mapping functions. So far, these attempts have not been successful. The evolution of the IGF towards more effective policy-shaping space will be decisive for the future global IG. The NETmundail Multistakeholder Statement highlighted the strengthening of the ICF as the priority in developing the future Internet governance arrangement.

In a new policy area, as IG is, there is high relevance for a decision-shaping space. Many players are trying to develop their approaches and priorities. A decision-shaping space is important for both framing the issues (main arguments, approaches, languages) and influencing the agenda setting.

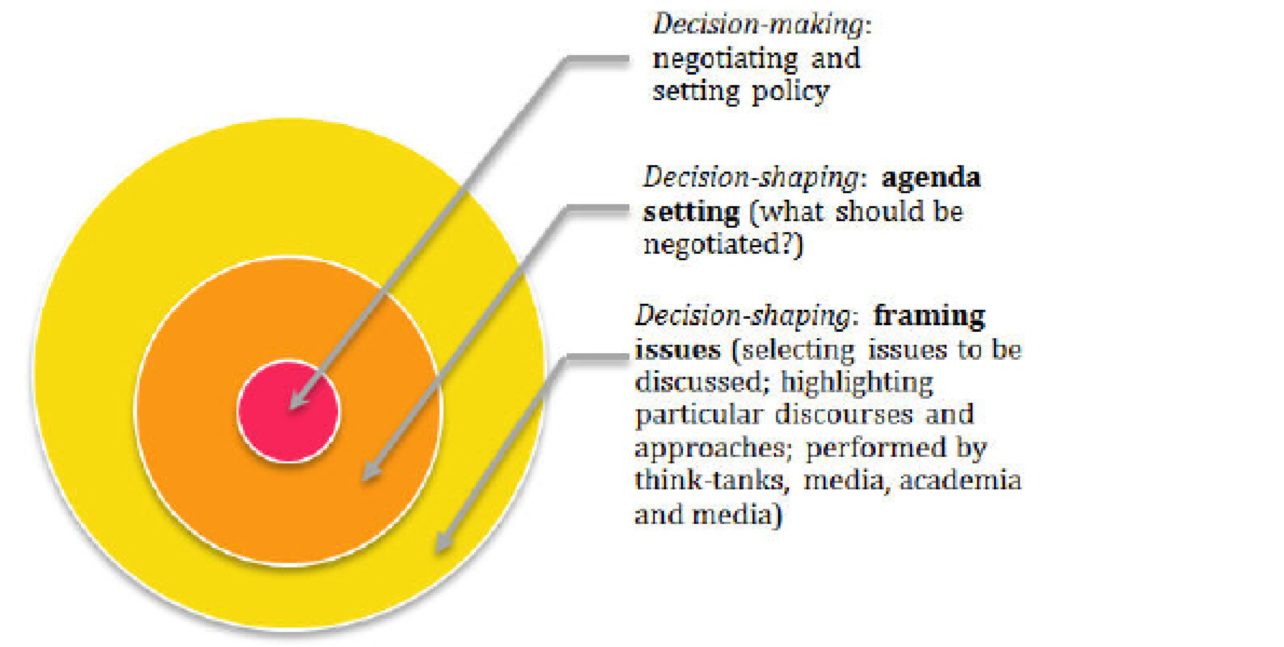

Decision-making: negotiating and setting policy
Decision-shaping: **agenda setting** (what should be negotiated?)
Decision-shaping: **framing issues** (selecting issues to be discussed; highlighting particular discourses and approaches; performed by think-tanks, media, academia and media)

Figure 10. Visualisation of decision-making and decision-shaping processes.

Foreseeable scenarios

IG is in a transitory phase. The Snowden revelations reduced trust in the existing IG architecture, and prompted the search for a new formula. The following three main scenarios for IG development can be envisaged for the period till 2020.

a) Status quo with the risk of sliding into a 'wild west' scenario

The current absence of a globally agreed and functional model of IG will increase tensions and demands for a solution. In such an environment, national governments and private entities could find 'solutions' by creating their own Internet spaces, resulting in the fragmentation of the Internet as we know it.

Internet fragmentation could take various forms. One could be 'data nationalisation'. Instead of storing data in the cloud servers abroad, governments could require Internet companies to keep data in servers physically located within their own national territories. This approach, already under consideration by Brazil and the EU, would increase costs for the Internet companies, such as Facebook and Twitter, but it would not endanger the basic functionality of the Internet. 'Data nationalisation' could be prevented by the adoption of global rules that guarantee to all governments that their data, and the data belonging to, and about, their citizens, are protected and managed according to their own national laws.

A second form could be the fragmentation of the root zone file (Internet address book), which could endanger the basic functionality of the Internet. Countries could take on the responsibility of managing the 'Internet address book' for their nationals. Practically speaking, it means that the access to – for example, www.google.com – would no longer be universally resolved, as is currently the case. It would only be possible to resolve (and access) from countries that decided to put www.google.com in their 'national address book'. This fragmentation would end the Internet as we know it. This type of fragmentation could be caused by the lack of reform by ICANN, to adopt an appropriate global/international mechanism, as perceived by the global IG community. As an alternative, some governments might decide to create a national or regional 'Internet address book'.

Other types of fragmentation, through the filtering of Internet traffic, have already started happening. More countries, in addition to those that are frequently mentioned, such as Iran and China, might try to increase their control of cross-border Internet traffic, using different – mainly security-based – justifications. While countries have the power to filter content (or entire services like Facebook or YouTube), and, ultimately, stop the flow of Internet traffic, as happened in Egypt in 2011, such moves are likely to lead to tensions and civil unrest, and to destabilise countries, or even whole regions, as was seen during the Arab Spring.

In the absence of globally shared norms and principles, and ways to enforce them among countries or companies, the bigger and stronger entities will attempt to impose their rules globally. Smaller countries or communities will have to choose to either follow their lead, or to isolate themselves, and set their own internal policies within their specific fragments of the global network. In the worst case, such a 'wild west scenario' could lead to tensions and conflicts – maybe even to cyber battles.

Multistakeholder institutions are likely to become the first victims of the digital *real politique* in the 'wild west' scenario. The IGF would likely already have become irrelevant. In the case of the fragmentation of the domain name system, ICANN might lose its *raison d'être*.

b) The 'radical change' towards an inter-governmental regime scenario

In this scenario, IG will be controlled by an intergovernmental organisation. This scenario could be triggered by a major crisis. It could be a *Titanic* moment, as the *Titanic* catastrophe triggered the accelerated regulation of international radio communication. The aftermath of the Snowden revelations has already seen a certain shift towards inter-governmental solutions, and has placed the issue before the highest UN bodies, such as the UN Security Council and General Assembly. The inter-governmental scenario has an attraction for small and developing countries that find practical difficulties in following the numerous IG processes and spaces. For them, a one-stop-shop solution in a familiar policy space, such as an international organisation, could be a viable option. The inter-governmental option could take one of two probable forms:

First, the ITU mandate could be extended to include IG. As the divided vote at the WCIT-Dubai (December 2012) showed, a stronger role for the ITU in IG would meet strong resistance from developed countries. Even if there is a political will, the ITU would face the serious limitation of being a principally technical institution, while IG increasingly involves legal, economic, social and development issues.

Second, a new international organisation could be established within or outside of the UN. Such proposals have been already made (at different times and in different venues) by Brazil, China, India, Russia, and South Africa. The latest, and still active, proposal is India's proposal to create a UN Committee for Internet-related Policies (CIRP).

c) The evolution scenario towards 'genuine multistakeholderism'

This scenario could emerge as a compromise solution between the non-governmental and inter-governmental sides (like the IGF, which was the result of a compromise at the 2005 WSIS in Tunisia). It would require extensive innovation in institutional and policy design. The new arrangement would need to address the main shortcomings of the current multistakeholder model, ensuring that the role of the different stakeholders is better defined and more transparent; public accountability is increased; and necessary checks and balances are established. The roles of the stakeholders would have to be differentiated according to the issues. For example, governments would need to have leading roles when it came to the protection of fundamental rights, and to security issues, while the technical community might assume a more active role in setting Internet technical standards.

In this scenario, the role of the IGF would need to be strengthened through its acceptance by all stakeholders as a policy-shaping body, and the place where the global 'IG menu' could be established, for other organisations and actors to 'prepare specific dishes' (e.g. draft new rules, establish standards, address conflicts). IGF policy recommendations and requests for action would be formally fed into specialised international organisations (the ITU, WIPO, the WTO, UNESCO), that would play an important role in their particular fields of specialisation. The IGF would also request action from business and other non-governmental players within their areas of responsibility (e.g. the IETF, W3C, and ICANN).

The success of this scenario would depend on whether all stakeholders were ready to accept responsibility for their actions in the global Internet community, in such a genuine multistakeholder model. A system of political, and other forms of pressure and sanctions, would have to be developed, in order to ensure that all stakeholders, in particular powerful private sector actors, would fulfil their commitments, and respect the core Internet principles.

As a compromise, this solution might satisfy both sides: the non-governmental camp would preserve the IGF as a multistakeholder body, and avoid the shift towards a fully inter-governmental arrangement. The inter-governmental camp would make the IGF more operational, and strengthen the role of specialised UN agencies in the implementation of specific aspects of IG (e.g. e-commerce, human rights, intellectual property).

The success of this scenario would depend on many balancing acts among different stakeholders. The make-or-break points for this scenario would be the way the dividing line between decision-making and decision-shaping spaces was handled; how well the roles and responsibilities of all the stakeholders were defined and agreed upon by all parties; and how governments were integrated into this new architecture.

Positioning around these three scenarios has already started. The evolution scenario with the central role of the IGF was the main winner at the NETmundial. Almost all of the main players pledged their support for the IGF. It was one of the few points of convergence points at NETmundial. The next major events in IG negotiations are the ITU Plenipotentiary Conference in Busan, South Korea (October 2014), where proponents of the intergovernmental solution are likely to table proposals for a stronger role for the ITU in IG. In 2015, the WSIS+10 review and the decision about the globalisation of ICANN oversight, could provide the foundation for the future IG arrangement.

Recommendations

These recommendations can be implemented separately or in a coordinated manner.

***Mainstream digital dimension** in Swiss foreign policy*

A digital dimension should be included in Swiss foreign policy strategies and in Switzerland's development agenda. Swiss foreign policy priorities (rule of law, universality, and neutrality) should be realised in the digital realm. The implementation activities should include organisational adjustments and training of staff in IG issues.

*Develop **partnerships** and join **favourable clusters of actors***

Switzerland should seek like-minded countries in pursuing similar policy preferences. In light of its own priorities, it can either take the lead or run with the pack. Concretely speaking, Switzerland could continue to develop coordination with the EU – whose sizeable market confers digital leverage in negotiations with the Internet industry. Switzerland is a member of the EU High Level Group on Internet Governance, a formal mechanism for coordinating IG policy. Switzerland should also develop cooperation with countries that are likely to shape future IG compromise (e.g. Brazil, India, and Mexico).

*Focus on **cybersecurity** as one of the Internet governance priority areas*

Switzerland should play an active and important role in cybersecurity. It should use its comparative advantages, including its wide global acceptance as a neutral player in security matters, its expertise in 'soft security' (human security), and its experience in managing the interplay between security and human rights.

*Strengthen the role of **international Geneva** in Internet governance*

Switzerland is already benefitting from the fact that Geneva is one of the main IG hubs. Many countries follow global digital policy via their Geneva-based permanent missions to the UN. Switzerland should increase – the still weak – decision-shaping space in Geneva. It should reinforce Geneva's attractiveness by facilitating the work of think-tanks and research centers from the major IG players, in particular BRICS countries. 'Maison de la paix' could be the physical venue for hosting them, and facilitating discussions and research on IG. In addition, global online communities should be developed around IG activities in international Geneva (e.g. webinars, online discussions).

*Support analysis and research to promote **evidence-based digital policies***

Switzerland and other global actors need stronger evidence to ensure informed and reliable policy-making. In this endeavour, Switzerland should support initiatives and entities providing evidence-based policy research on IG (e.g. statistics, open data, data-mining). As one of the research priorities, Switzerland could address the lack of data and reporting on cybersecurity attacks. It could also encourage the creation of a Swiss network of academic and research programmes on digital policy issues.

Strengthen the rule of law on the Internet

The elaboration of a legal system applicable to the Internet is in its early phase. Switzerland can contribute to this process by ensuring that existing international law is applied to the Internet through specific actions (such as introducing digital dimensions in the reporting on the human rights conventions) and by making sure that new Internet rules rely on sound legal principles (due process, transparency, checks and balances, public oversight). Lastly, Switzerland could provide innovative regulatory solutions.

Support universality and inclusiveness in Internet governance

The more inclusive and universal IG is, the better Swiss interests will be safeguarded. To reach this objective, Switzerland should promote participation in Geneva-based IG activities by underrepresented small and developing states. In addition, it should support online participation as the way to facilitate the involvement of actors and stakeholders who would not be able to take part in traditional IG processes.

Provide good offices and mediation in Internet governance
Switzerland could extend its traditional role of provider of good offices to the digital policy realm. WCIT Dubai (2012) ended up in a split vote, mainly along the lines of developed/developing countries, creating a kind of 'digital Cold War' according to some commentators. More recently, the PRISM/NSA crisis increased tensions and divides in the global Internet policy. Switzerland could identify, with the help of like-minded countries and actors, 'zones of possible agreement' or convergence towards broadly accepted solutions, provide venues and context for Internet 'track two diplomacy', and highlight the role of Geneva as a neutral and inclusive digital policy hub.

*Act towards **a global institutional framework for the Internet***
The future of the Internet – as a global system – will depend on creating an appropriate and accepted governance space. Switzerland should promote a set of principles to address present shortcomings. It should request stakeholder transparency and accountability, ensure a level playing field, help produce tangible outcomes of IGF activities, and apply adequate subsidiarity.

*Support **policy coherence** approach when dealing with cross-cutting digital issues*
Currently, most IG takes place in policy silos. On a national level, Switzerland should strengthen interdepartmental coordination mechanisms among departments and federal offices that cover different aspects of IG issues (e.g. technology, security, juridical, commercial, social, and cultural). On an international level, it should support a holistic approach to IG involving various UN organisations and agencies. The priority areas for cross-cutting approach should be cybersecurity and human rights.

Annexes

Annex I. Swiss contribution to Internet governance: What has Switzerland done so far?

Switzerland has laid a solid basis for its future role in IG. For the last 10 years, since the Geneva WSIS in 2003, Switzerland has been one of the most active participants in global IG, providing both a substantive contribution to IG policy-making and supporting the development of an institutional architecture and capacity building foundation on both European and global levels.

Policy-making contribution

Switzerland has been a very active contributor in all three main IG spaces: ICANN, the IGF, and the ITU. For example, according to Diplo's data-mining project *The Emerging Language of IG*, Switzerland is the 5th most active government – after Egypt, the United Kingdom, Brazil, and Kenya – in the IGF debate between the first IGF in Athens (2006) and the 6th IGF in Nairobi (2011). The survey is based on transcripts of the IGF main sessions, workshops, and preparatory meetings. Besides this quantitative aspect, Switzerland's interventions have been highly relevant for shaping consensus among the IGF actors.

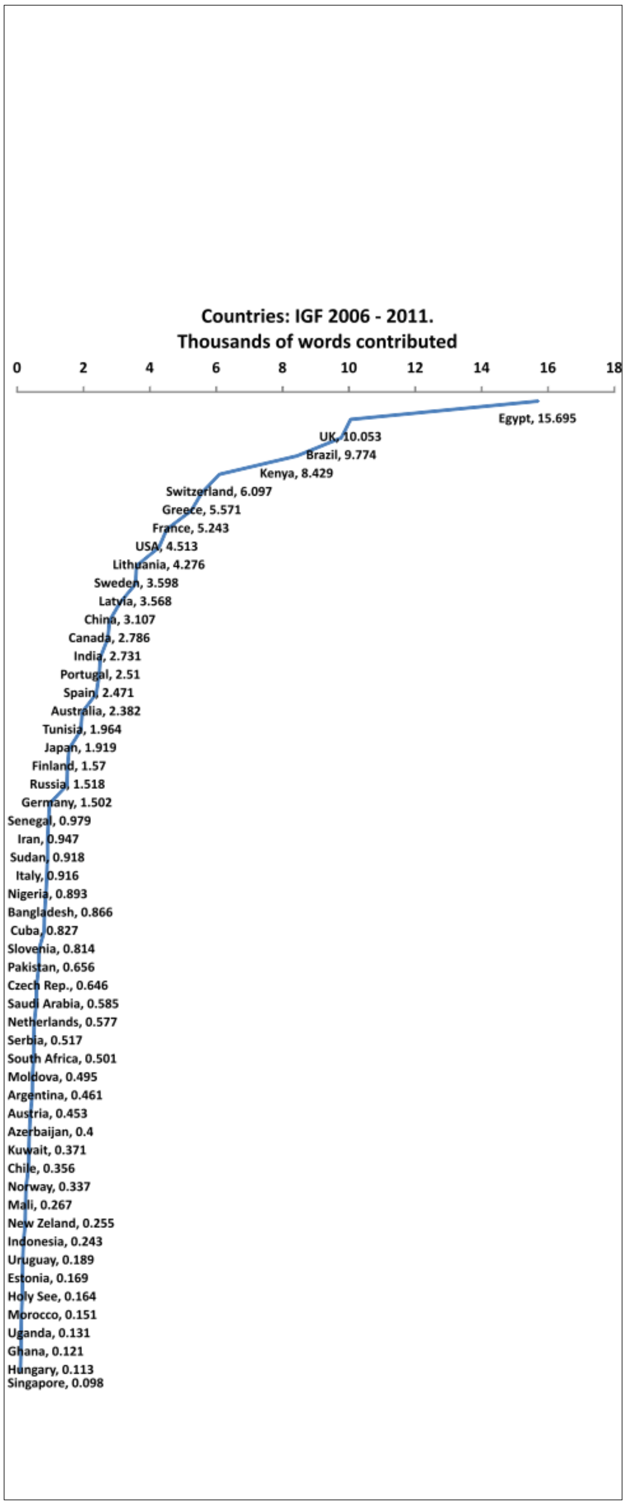


Figure A1. Total verbal contribution to the IGF 2006 – 2011 for 54 countries. The scale is given in thousands of words. Analysis is based on word frequency distributions that were drawn from the pilot version of the IGF Text Corpus, where approximately 50% of the complete verbal contribution to the IGF was automatically tagged and mapped to relevant actors and events.

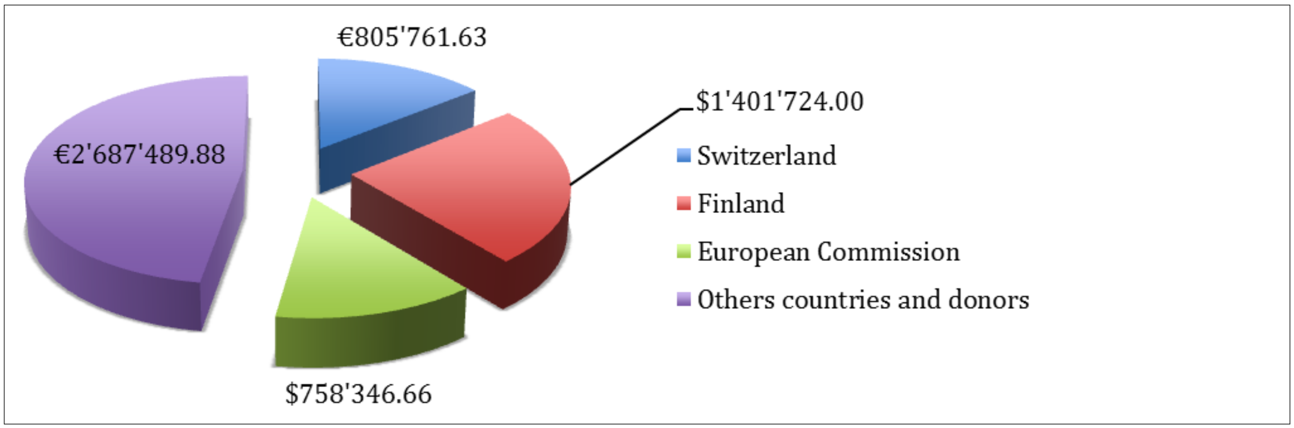


Figure A2. Contributions to IG institutional architecture.

Switzerland is the second greatest financial contributor to the IGF (after Finland). The Swiss contribution was particularly relevant during the first formative phase of the IGF.

In 2008, Switzerland initiated the European Internet Governance Dialogue (EuroDIG), a pan-European space for addressing IG issues. EuroDIG has been managed by Switzerland (OFCOM) and the CoE since then. It is considered to be one of the most successful regional initiatives in the field of IG.

Geneva hosts the main global spaces for addressing IG issues (the ITU, WIPO, ISO, the WTO, and the IGF).

Capacity building

The Swiss Development Corporation (SDC) supported the Internet Governance Capacity Building Programme (IGCBP) which helped many small and developing countries participate in the global IG process. The IGCBP, run by DiploFoundation, is an annual programme involving online training, policy research, and policy immersion. Since 2005, the IGCBP has involved 1121 participants from 142 countries. Many small and developing countries trained their first representatives in global and regional IG forums via this Swiss-supported capacity building programme. For example, 12 out of 56 members of the IGF governing body (Multistakeholder Advisory Board (MAG) are IGCBP alumni. In ICANN's Government Advisory Council (GAC), 15 small and developing countries are represented by diplomats and officials trained in the context of the IGCBP. The African IGF and many regional policy initiatives – Latin America, Pacific, and Caribbean – were nurtured in the framework of the IGCBP.

Annex II. Geneva Internet Governance Index (GIGI)[26] – The role of Geneva in global Internet governance

Geneva's role is indicated for each IG issue and for the complete basket (indicated with red line and red number). A summary of the methodology used to develop the Geneva Internet Governance Index is available on the next page.

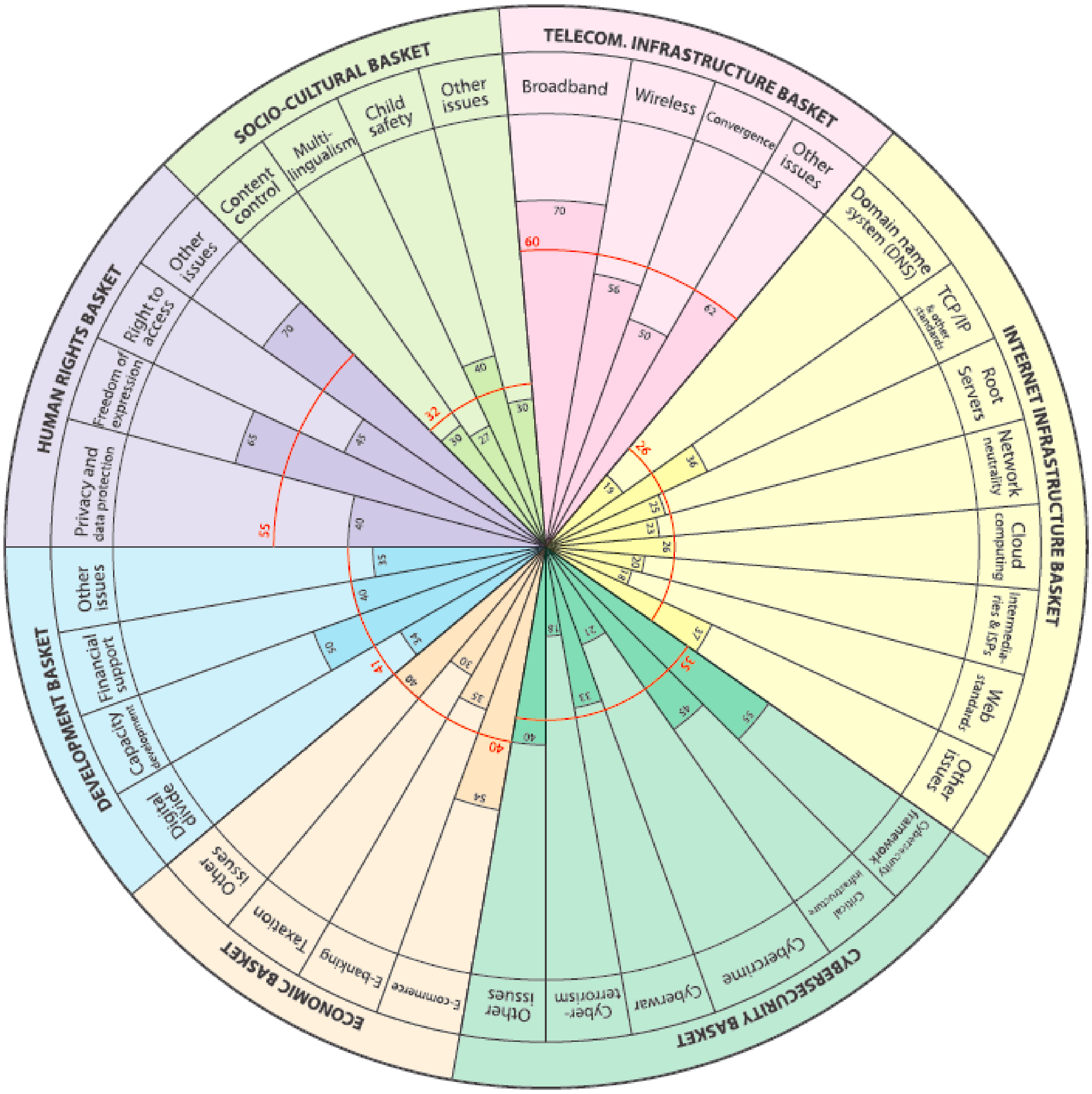


Figure A3. Geneva's role in global IG indicated in percentages (Geneva Internet Governance Index).

- WHO? **Location:** the number of IG actors (e.g. international organisations, NGOs, think-tanks) based or represented in Geneva. The scoring of the indicator is as follows:

GIGI provides an approximate indication of Geneva's role in comparison with all other places globally. It is done by calculating the following indicators:

0 = No representation in Geneva

1 = Representation in Geneva

2 = Based on in Geneva (official seat)

3 = Based in Geneva and less than 60% activities performed in Geneva

4 = Based in Geneva and all activities performed in Geneva

- HOW? **Decision-making**: the number of legal and policy instruments adopted and managed from Geneva; the number of decision-making processes performed in Geneva (including approximate number of meetings and participants). The scoring of the indicator is as follows:

0 = No policy and legal instruments

1 = Occasional adoption of policy instruments (standards, recommendations)

2 = Regular adoption of policy instruments (at least 3 per year)

3 = Adoption of legally binding instruments

4 = Legally binding instruments with developed regime (secretariat, implementation, reporting).

- HOW? Decision-shaping: the number of events (conferences, panels, awareness-building sessions), research projects, and Internet spaces run by Geneva-based institutions (social media, Internet). The scoring of the indicator is as follows:

0 = No decision-shaping activities

1 = Occasional organisation of events

2 = Regular organisation of events (more than 3 per year)

3 = Preparing research and policy papers

4 = Comprehensive approach combining events, research, and prominent web presence

- HOW? **Relevance**: The role of Geneva-based institutions and policy processes in addressing the most relevant IG issues, including policy gaps and controversies. This policy study contains the list of these issues in each issue area (e.g. infrastructure, legal issues, and development issues). The scoring of the indicator is as follows:

0 = No coverage of pressing IG issues

1 = Decision-shaping coverage of relevant IG issues (events, conferences, research)

2 = Policy-making coverage of relevant IG issues

3 = Negotiation of legal instruments on relevant IG issues

4 = Comprehensive coverage of relevant IG issues (implementation, secretariat, reporting)

Annex III. Internet Governance Glossary

Abbreviation	Full term	Link	Short definition
ACTA	Anti-Counterfeiting Trade Agreement	https://www.eff.org/issues/acta	Proposed multinational agreement to establish enforcement of intellectual property rights, signed in 2011, which triggered protests across Europe and the USA.
AFRINIC	African Network Information Centre	http://www.afrinic.net/	One of five Regional Internet Registries (RIRs) representing the African region.
AoC	Affirmation of Commitment	http://www.icann.org/en/about/agreements/aoc	An assertion of agreement or commitment. In IG language, commonly refers to the latest stage of the legal relations between ICANN and US Department of Commerce, signed in 2009.
APC	Association for Progressive Communications	http://www.apc.org/	One of the oldest civil society organisations on Internet issues aimed to promote access to free and open Internet, empowering users through ICT. In December 2010, APC had 50 members in 35 countries, the majority from developing countries.
APEC	Asia-Pacific Economic Co-operation	http://www.apec.org/	Asia-Pacific economic forum.
APNIC	Asia-Pacific Network Information Centre		One of five Regional Internet Registries (RIRs) representing the Asia-Pacific region.
ARIN	American Registry for Internet Numbers	https://www.arin.net/	One of five Regional Internet Registries (RIRs) representing the North America region (the USA, Canada, parts of the Caribbean and Antarctica).
ARPANET	Advanced Research Projects Agency Network	http://computer.howstuffworks.com/arpanet.htm	Academic network precursor to the Internet.
ASCII	American Standard Code for Information Interchange	http://www.ascii-code.com/	7-bit character code. Each single bit represents a unique character.
AT&T	American Telephone and Telegraph	http://www.att.com/shop/internet/internet-service.html#fbid=5AH6V5gJ_ps	Large US telecom and Internet provider.
BBS	Bulletin Board System	http://en.wikipedia.org/wiki/Bulletin_board_system	Computer system using software to connect users/user groups in the 1980s and early 1990s.
BGP	Border Gateway Protocol	http://en.wikipedia.org/wiki/Border_Gateway_Protocol	One of the main protocols of the Internet, carrying out fully decentralised routing based on path, network policies and/or rule-sets

Abbreviation	Full term	Link	Short definition
blog	from weblog: web + blog or online blog	http://www.thefreedictionary.com/weblog	A website that displays in chronological order the postings by one or more individuals and usually has links to comments on specific postings.
CC	Creative Commons	http://creativecommons.org/	An open licensing system that assists authors in sharing their work.
ccTLD	country code Top Level Domain	http://www.icann.org/en/resources/cctlds	Two-letter country code top level domain names, such as .ve (Venezuela) or .uk, (United Kingdom) which are administered by the country code manager.
CERN	European Centre for Nuclear Investigations	http://home.web.cern.ch/	Leading Geneva-based scientific organisation, involved in many breakthroughs in Internet technology (invention of WWW and grid-computing).
CERT	Computer Emergency Response (or Readiness) Team	http://www.enisa.europa.eu/activities/cert	Teams of security and computer experts organised national and government, corporate or other levels, to prevent and instantly react to cyber-attacks or major incidents on networked systems in order to limit damage and ensure continuity of critical services.
CI	Critical Infrastructure	http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf	CI is generally considered as the key system, services and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security or any combination of these. CI is composed of both physical elements (such as facilities and buildings) and virtual elements (such as systems and data).
CIIP	Critical information infrastructure protection	http://ec.europa.eu/digital-agenda/en/news/policy-critical-information-infrastructure-protection-ciip	One of the main objectives of cybersecurity strategies and policies, to protect critical information infrastructure of the country (and institutions) including links, data, hardware and software.
CIX	Commercial Internet Exchange	http://en.wikipedia.org/wiki/Commercial_Internet_eXchange	An early step towards the Internet, which permitted exchange of TCP/IP traffic.
CoE	Council of Europe	http://hub.coe.int/	European organisation with 47 member states active in Internet governance: cybersecurity, digital human rights, data protection, etc.
CSTD	Commission on Science and Technology for Development of UN ECOSOC	http://unctad.org/en/Pages/cstd.aspx	A body of the Economic and Social Council (ECOSOC) which gives advice to the UN General Assembly on science and technology issues. Mandated to review the IGF process and to initiate discussions about Enhanced Cooperation in Internet Governance.
Cyclades	not an acronym, a name taken from the Greek	http://en.wikipedia.org/wiki/CYCLADES	One of technical predecessor to the Internet.
DARPANET	Defence Adv. Research Projects Agency	http://searchnetworking.techtarget.com/definition/DARPANET	US defence precursor to the Internet, sometimes used interchangeably with ARPANET.

Abbreviation	Full term	Link	Short definition
DCAF	Democratic Control of Armed Forces	http://www.dcaf.ch/	Geneva-based think-tank which supports security sector governance through security sector reform; active in cybersecurity issues.
DDoS	Distributed Denial of Service	http://en.wikipedia.org/wiki/Denial-of-service_attack	A systematic attack to disable a network resource by causing suspension of service, for example through server overload.
DMCA	Digital Millennium Copyright Act	http://en.wikipedia.org/wiki/Digital_Millennium_Copyright_Act	US copyright law implementing two 1996 World Intellectual Property Organisation (WIPO) treaties which criminalise circumvention of digital rights management (DRM).
DNS	Domain Name System	http://en.wikipedia.org/wiki/Domain_Name_System	A system managed by Internet Corporation for Assigned Names and Numbers (ICANN), allowing strings of letters (the domain name) to be assigned to an Internet Protocol (IP) address, for ease of url management by the user.
DNSSEC	Domain Name System Security Protocol	http://www.icann.org/en/about/learning/factsheets/dnssec-qaa-09oct08-en.htm	Technology to secure the DNS.
DoC	Department of Commerce	http://www.commerce.gov/	The US Department of Commerce is relevant in the IG context because it is the mandated to perform US oversight over ICANN as a non-for-profit registered in state of California.
DoD	Department of Defence	http://www.defence.gov/	The US Department of Defence was involved in DARPANET and the early stages of Internet development.
DPI	Deep Packet Inspection	http://en.wikipedia.org/wiki/Deep_packet_inspection http://www.youtube.com/watch?v=OFPHUv1LfS4&list=PLa6vw8V5aV_VXFdFmnqABXWcMA&index=6	Inspection or review of the data (content) of each digital packet, to improve protocol and routing and avoid security threats. There is concern that it can be used for surveillance, privacy breaches or other types of data-mining.
DRM	Digital Rights Management	http://computer.howstuffworks.com/drm.htm	Technologies that impose rights-based limits and controls on the software, media, and applications on users' devices.
EC	European Commission	http://ec.europa.eu/	A body that represents the EU as a whole, made up of 28 commissioners, and proposing and enforcing laws for the EU.
ECOSOC	Economic and Social Council (UN)	http://www.un.org/en/ecosoc/	The UN platform to address economic and social issues.
EuroDIG	European Dialogue on Internet Gov.	http://www.eurodig.org/	A regional European discussion forum on Internet governance.
enQuire	Not an acronym, but the name of a software project written in 1980	http://en.wikipedia.org/wiki/ENQUIRE	A predecessor to the World Wide Web, enQuire was a software program written by Tim Berners-Lee.

Abbreviation	Full term	Link	Short definition
GAC	Governmental Advisory Committee (part of ICANN)	https://gacweb.icann.org/display/gacweb/ental+Advisory+Committee	Representatives of State governments, forming an advisory committee which reports to and advises the Internet Corporate for Assigned Names and Numbers (ICANN) board.
gTLD	generic Top Level Domain	http://www.icann.org/en/about/learning/glossary	Sponsored or unsponsored generic top level domains. The first seven gTLDs established in 1980 were .com, .edu., gov, .int., .ml, .net, .org.
HTML	HyperText Markup Language	http://en.wikipedia.org/wiki/HTML	Commonly used mark-up language for creating web pages and for preparing information for display in a web browser.
IANA	Internet Assigned Numbers Authority (IANA)	http://www.ntia.doc.gov/page/iana-functions-purchase-order	Originally the global coordinator of the domain name system (DNS) root, Internet Protocol (IP) addressing and other IP resources, IANA allocated IP addresses to the Regional Internet Registers (RIRs) and implemented the changes in the root zone file. ICANN has been mandated by the US DoC to perform IANA functions through a contract with NTIA.
IAP (IBP)	Internet Access Providers (also Internet Bandwidth Providers)	http://searchsoa.techtarget.com/definition/IAP	Major national, regional or global Internet service providers (ISP) or entity that provides broadband Internet access to users and other ISPs (commonly big telecom companies).
ICANN	Internet Corporation for Assigned Names and Numbers	http://www.icann.org/	Corporation registered in the state of California, USA that coordinates key technical services for the Internet domain name system (DNS), generic Top Level Domains and country code Top Level Domains, as well as Internet numbering resources.
ICC	International Chamber of Commerce	http://www.iccwbo.org/	Paris-based global business forum addressing issues of world economy.
ICT	Information and Communication Technology	http://en.wikipedia.org/wiki/Information_and_communications_technology	A synonym for Information technology (IT), describing the use of all media communications and computer technologies. Its strategies and access are important for development and the economy, and are documented globally by the International Telecommunication Union (ITU).
IDN	Internationalised Domain Name	http://en.wikipedia.org/wiki/Internationalized_domain_name	Domain names that include characters in character sets other than the basic Latin alphabet. In 2010, the first Arabic IDNs were put into use.
IEC	International Electrotechnical Commission	http://www.iec.ch/	Geneva-based leading global organisation for publication of international standards for electrical, electronic, and related technologies (electrotechnologies).
IEEE	Institute of Electrical and Electronics Engineers	http://www.ieee.org/about/ieee_history.html	An association for the advancement of technology and innovation.

Abbreviation	Full term	Link	Short definition
IETF	Internet Engineering Task Force	http://www.ietf.org/	A technical supporting organisation for the Internet organised by the Internet Society (ISOC).
IG	Internet Governance	http://www.diplomacy.edu/IGBook	The management of the Internet, emphasising the legal, social, linguistic and economic perspectives of the Internet, in addition to its technical base.
IG4D	Internet Governance for Development	http://www.africatelecomit.com/event/internet-governance-for-development-ig4d-2013/	Emphasis on the capacity of the Internet to foster development.
IGC	Internet Governance Caucus	http://igcaucus.org/	A civil society online discussion group to address Internet governance as it affects human rights, social equity and interdependence, cultural concerns, and social and economic development.
IGF	Internet Governance Forum	http://www.intgovforum.org/cms/	A forum for multistakeholder policy dialogue to discuss public policy issues related to key elements of Internet governance as established in Paragraph 72 of the Tunis Agenda of the World Summit on the Information Society (WSIS).
IGO	Inter-governmental organisation	http://www.law.harvard.edu/current/careers/opia/public-interest-law/public-international/interngovernmental-organisations.html	An organisation created by a treaty between two or more nations, to work on issues of common interest, particularly peace and security.
INTERNET	INTERconnected NETworks	http://dictionary.reference.com/browse/Internet	The global computer network which links computers and users worldwide.
IoT	Internet of Things	http://en.wikipedia.org/wiki/Internet_of_Things	First proposed by Kevin Ashton in 1999, the Internet of Things would assign a unique identifier to each unique identifiable object, no matter how small or large, in an Internet-like structure.
IP	Internet Protocol	http://www.icann.org/en/about/learning/glossary	The communications protocol that allows a unique identifier to be assigned to a computer, which we call the IP address, which identifies the location of a device on the Internet.
IPO	Initial Public Offering	http://www.investopedia.com/terms/i/ipo.asp	The first sale of stock by a private company (to the public).
IPR	Intellectual Property Rights	http://www.wto.org/english/tratop_e/trips_e/intel1_e.htm	IPRs are the rights a creator has to their creation, for a certain period of time, especially copyright and industrial property rights.
IPv4	Internet Protocol version 4	http://www.techterms.com/definition/ipv4	The fourth and most commonly used version of the Internet protocol, which uses a 32-bit format.

Abbreviation	Full term	Link	Short definition
IPv6	Internet Protocol version 6	http://www.techterms.com/definition/ipv6	The sixth version of the Internet protocol, which uses 128-bit addresses, increasing the number of available IP addresses to an extremely large, though still finite number (IPv6 allows approximately 340 trillion trillion trillions of IP addresses, compared to IPv4, which uses 32-bit addresses. IPv4 has approximately 4.3 billion addresses).
IRC	Internet Relay Chat	http://www.irchelp.org/	Networks of separate servers which allow users to connect as large groups of users, instead of the typical on-to-one chat of text messaging.
ISOC	Internet Society	http://www.internetsociety.org/	A global organisation aligned with the technical community, dedicated to keeping the Internet open, transparent, and user-defined.
ISP	Internet Service Provider	http://en.wikipedia.org/wiki/Internet_service_provider	An organisation (generally a business) that provides access to the Internet, and related support services.
IT	Information Technology	http://en.wikipedia.org/wiki/Information_technology	The use of computers and other telecommunications devices to store, retrieve, transmit, and manipulate data as a support mechanism for a larger enterprise.
ITR	International lecommunication Regulations	http://www.internetsociety.org/itr	A treaty developed at the 1988 World Administrative Telegraph and Telephone Conference, to facilitate global interconnection and interoperability of telecommunications traffic across national borders, and amended during WCIT Dubai in 2012 in a controversial voting process.
ITU	International lecommunication Union	http://www.itu.int/en/Pages/default.aspx	Geneva-based UN specialised agency for information and communication technologies.
IXP	Internet eXchange Point	http://en.wikipedia.org/wiki/Internet_exchange_point	A physical infrastructure through which Internet service providers (ISPs) exchange Internet traffic between their networks, usually through peering (i.e. settlement-free) agreements.
JPA	Joint Project Agreement	http://www.icann.org/en/about/agreements	The Joint Project Agreement (JPA) of 2006 is an iteration in relations between the US Department of Commerce and ICANN, towards managing the transition of the DNS to the private sector. It builds on the previous Memorandum of Understanding (MoU) between the two parties.
kB	Kilobyte	http://www.t1shopper.com/tools/calculate/	A measure of data capacity, kB is 1024 bytes. Similarly, MB stands for Megabyte and refers to a thousand kilobytes (i.e. a million bytes) per second; GB stands for Gigabyte and refers to a thousand Megabytes (i.e. a billion bytes), etc.

Abbreviation	Full term	Link	Short definition
kbps	Kilobits per second	http://www.webopedia.com/TERM/K/Kbps.html	A measure of data transfer speed, kilobits per second is 1024 bits per second. Similarly, Mbps stands for Megabits per second and refers to a thousand kilobits (i.e. a million bits) per second; Gbps stands for Gigabits per second and refers to a thousand Megabits (i.e. a billion bits) per second, etc.
LACNIC	Latin America and Caribbean Network Information Centre	http://www.lacnic.net/web/portal/inicio	One of five Regional Internet Registries (RIRs) representing Latin America and parts of the Caribbean.
LIR	Local Internet Registry	http://www.ripe.net/lir-services/resource-management/faq/independent-resources/phase-three/what-is-a-local-internet-registry-lir	Members of a Network Coordination Centre (NCC) called LIRs because they are responsible for the distribution of address space and registration of the address space on a local level.
MGDs	Millennium Development Goals	http://www.un.org/millenniumgoals/	An agreement by all UN countries to work to reach eight goals to meet the needs of the world's poorest people.
mbps	Megabits (millions of bits) per seconds	http://www.webopedia.com/TERM/M/Mbps.html	A measure of data transfer speed: megabits per second or one million bits per second (Mbps). Similarly kB is 1024 bits per second.
MILNET	Military Network	http://www.webopedia.com/TERM/M/Mbps.html	A measure of data transer speed: megabites per second (Mbps). Similarly kB 1024 bits per seceond.
MIT	Massachusetts Institute of Technology	http://web.mit.edu/	A university founded in 1861 in the state of Massachusetts, USA, for the study of science and technology.
modem	MOdulate-DEModulate	http://en.wikipedia.org/wiki/Modem	A device used to transmit and decode digital data.
MoU	Memo of Understanding	http://www.investopedia.com/terms/m/mou.asp	A legal document outlining the terms and details of an agreement between parties, including each party's requirements and responsibilities. In IG language, it commonly refers to the agreement between ICANN and the US Department of Commerce.
MP3	Music file MPEG Layer 3	http://en.wikipedia.org/wiki/MP3	A commonly used encoding format for digital audio which uses a form of lossy data compression, a data encoding method that compresses data by discarding (losing) some of it.
MSP	Multistakeholder process	http://toronto45.icann.org/node/34391	Strategy to foster consensus between all involved stakeholders, even with diverging interests, to include the public domain, governments, the private sector and civil society.

Abbreviation	Full term	Link	Short definition
MUD	Originally Multi-User Dungeon, later both Multi-User Dimension and Multi-User Domain	http://www.thefreedictionary.com/Multi-User+Domain	A computer program, usually run over the Internet that allows multiple users to participate in virtual reality role-playing games.
NIC	Network Information Centre	http://en.wikipedia.org/wiki/InterNIC	A network information centre, but usually referring to one of five Regional Internet Registries (RIRs) representing Latin America and parts of the Caribbean (LACNIC), Africa (AFRINIC), Asia and the Pacific (APNIC), North America and parts of the Caribbean (ARIN) and Europe (RIPE). NIC also refers to the national registries of country-code top level domains (ccTLDs).
NNTP	Network News Transfer Protocol	http://en.wikipedia.org/wiki/Network_News_Transfer_Protocol	An application protocol used for transporting Usenet news articles (netnews) between news servers and for reading and posting articles by end user client applications.
NRO	Number Resource Organisation	http://www.nro.net/	Formed by the Regional Internet Registries (RIRs) to formalise their co-operative efforts, the NRO exists to protect the unallocated Number Resource pool, to promote and protect the bottom-up policy development process, and to act as a focal point for the Internet community's input into the RIR system.
NSF	National Science Foundation	http://www.nsf.gov/	An independent US federal agency created by the US Congress in 1950 to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defence.
NSFNET	National Science Foundation Network	http://www.nsf.gov/about/history/nsf0050/internet/launch.htm	NSF's supercomputing program, launched in 1984, designed to make high performance computers accessible to researchers around the country (USA).
NTIA	The National communications and Information Administration	http://www.ntia.doc.gov/about	NTIA is the US President's principal adviser on telecommunications and information policy. It is one of the main points of contact of the US government with ICANN.
OECD	Organisation for Economic Co-operation and Development	http://www.oecd.org/	Paris-based organisation established in 1961 to provide a forum in which governments can work together to share experiences and seek solutions to common problems.
OSCE	Organisation for Security and Co-operation in Europe	http://www.osce.org/	World's largest regional security organisation with 57 member states from Europe, Central Asia and North America; addresses cybersecurity through confidence building measures.
OSI	Open Systems Interconnection	http://www.webopedia.com/TERM/O/OSI.html	An ISO standard for worldwide communications that defines a networking framework for implementing protocols in seven layers.

Abbreviation	Full term	Link	Short definition
OTT	Over-the-top (services or providers)	http://www.itvdictionary.com/definitions/over-the-top_definition.html	General term for service utilised over a network that is not offered by that network operator (commonly referring to Skype, Google, Facebook and other online content and service providers).
PC	Personal Computer	http://en.wikipedia.org/wiki/History_of_personal_computers	A general purpose computer meant for individual use.
PGP	Pretty Good Privacy	http://searchsecurity.techtarget.com/definition/Pretty-Good-Privacy	A popular software program used to encrypt and decrypt e-mail over the Internet.
PKI	Public Key Infrastructure	http://en.wikipedia.org/wiki/Public-key_infrastructure	A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.
PS	Packet-switching	http://compnetworking.about.com/od/networkprotocols/f/packet-switch.htm	The approach used by some computer network protocols to deliver data across a local or long distance connection. Examples of packet switching protocols are Frame Relay, IP and X.25.
RFC	Request for Comments	http://www.ietf.org/rfc.html	Usually refers to the publication of the Internet Engineering Task Force (IETF), established in 1969 by Steve Crocker to record ARPANET notes. They are now used to record Internet specifications, communications protocols, etc.
RFID	Radio Frequency Identification	http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid.htm	Smart labels or intelligent bar codes that can communicate with a networked system for tracking purposes.
RIPE	Ripe Network Coordination Centre	http://www.ripe.net/	One of five Regional Internet Registries (RIRs) representing the European region.
RIPE NCC	Réseaux IP Européens Network	http://www.ripe.net/	One of five Regional Internet Registries (RIRs) representing the European region.
RIP	Routing Information Protocol	http://www.cisco.com/en/US/tech/tk365/tk554/tsd_technology_support_sub-protocol_home.html	A distance-vector protocol that uses hop count as its metric. RIP is widely used for routing traffic on the global Internet and is an interior gateway protocol (IGP), which means that it performs routing within a single autonomous system.
RIR	Regional Internet Registry	https://www.arin.net/knowledge/rirs.html	Non-profit corporations that administer and register Internet Protocol (IP) address space and Autonomous System (AS) numbers within a defined region. RIRs also work together on joint projects.
SOPA	Stop Online Piracy Act	http://money.cnn.com/2012/01/17/technology/sopa_explained/index.htm	Known as SOPA, this proposed bill aims to crack down on copyright infringement by restricting access to sites that host or facilitate the trading of pirated content.

Abbreviation	Full term	Link	Short definition
Spam	Adopted from the brand name SPAM (Hormel Spiced Ham).	http://en.wikipedia.org/wiki/Spam_%28electronic%29	Use of electronic messaging systems to send unsolicited bulk messages, especially advertising, indiscriminately.
SRI	Stanford Research Institute, now SRI International	http://www.sri.com/about	US-based independent, 501(c)(3) non-profit research institute conducting client-sponsored research and development for government, industry, foundations, and other organisations.
SSL	Secure Sockets Layer	http://www.digicert.com/ssl.htm	A standard security technology for establishing an encrypted link between a server and a client - typically a web server (website) and a browser; or a mail server and a mail client (e.g. Outlook).
TCP/IP	Transmission Control Protocol/ Internet Protocol	http://compnetworking.about.com/od/tcpip/TCPIP_Transmission_Control_Protocol_Internet_Protocol.htm	Arguably the single most important computer networking technology. The Internet and most home networks support TCP/IP as the 'language' computers use to find and connect with each other.
TLD	Top Level Domain	http://archive.icann.org/en/tlds/	The Internet's domain-name system (DNS) allows users to refer to websites and other resources using easier-to-remember domain names (such as www.icann.org) rather than the all-numeric IP addresses (such as 192.0.34.65) assigned to each computer on the Internet. Each domain name is made up of a series of character strings (called labels) separated by dots. The right-most label in a domain name is referred to as its top-level domain (TLD).
ToS	Terms of service		Terms and conditions that users need to read and formally accept (by clicking 'I agree') when using most online services.
TRIPS	Trade Related Aspects of Intellectual Property Rights	http://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm	The WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), negotiated in the 1986-1994 Uruguay Round, introduced intellectual property rules into the multilateral trading system for the first time.
UCLA	University of California, Los Angeles	http://www.ucla.edu/	A public research university in Los Angeles, CA, USA.
UCSB	University of California, Santa Barbara	http://www.ucsb.edu/	A public university in Santa Barbara, CA, USA.
UDHR	Universal Declaration of Human Rights	http://www.un.org/en/documents/udhr/	Basic UN declaration of Human Rights adopted by the UN General aSsemby in 1948.
UDRP	Uniform Domain-Name Dispute-Resolution Policy	http://www.icann.org/en/help/dndr/udrp	Policy whereby most types of trademark-based domain-name disputes must be resolved by agreement, court action, or arbitration before a registrar will cancel, suspend, or transfer a domain name.

Abbreviation	Full term	Link	Short definition
UN	United Nations	http://www.un.org/en/	International organisation with 193 member states, founded in 1945 to replace the League of Nations.
UNCITRAL	United Nations Commission on International Trade Law	http://www.uncitral.org/	The core legal body of the UN system in the field of international trade law. A legal body with universal membership specialising in commercial law reform worldwide for over 40 years. UNCITRAL's business is the modernisation and harmonisation of rules on international business.
UNESCO	United Nations Educational Scientific and Cultural Organisation	https://en.unesco.org/	A specialised agency of the United Nations (UN) with five major programs: education, natural sciences, social and human sciences, culture, and communication and information. It replaced the League of Nations' International Commission on Intellectual Cooperation.
UNIX	Not an acronym, but an Open Group brand for a computer operating system, based on a play on words for MULTICS multi-tasking, multi-user computer operating system	http://www.unix.org/	Today the definition of UNIX ® takes the form of the worldwide Single UNIX Specification integrating X/Open Company's XPG4, IEEE's POSIX Standards and ISO C.
UNODC	United Nations Office on Drugs and Crime	http://www.unodc.org/	United Nations (UN) body, established in 1997 to deal with illicit trafficking in and abuse of drugs, crime prevention and criminal justice, international terrorism, and political corruption.
USENET	Slang for 'use the Net'	http://en.wikipedia.org/wiki/Usenet	Usenet is a worldwide distributed Internet discussion system. It was developed from the general purpose UUCP dial-up network architecture.
UUCP	Unix-to-Unix Copy	http://en.wikipedia.org/wiki/UUCP	The term generally refers to a suite of computer programs and protocols allowing remote execution of commands and transfer of files, e-mail, and netnews between computers.
VoIP	Voice over Internet Protocol	http://www.cisco.com/en/US/prod/voicesw/networking_solutions_products_content0900aecd804f00ce.html	A way to carry phone calls over an Internet Protocol (IP) data network, whether on the Internet or your own internal network. A primary attraction of VoIP is its ability to help reduce expenses because telephone calls travel over the data network rather than the phone company's network.
W3C	World Wide Web Consortium	http://www.w3.org/	An international community where member organisations, a full-time staff, and the public work together to develop Web standards. Led by Web inventor Tim Berners-Lee and CEO Jeffrey Jaffe, W3C's mission is to lead the Web to its full potential.

Abbreviation	Full term	Link	Short definition
WCIT	World Conference on International telecommunications	http://www.itu.int/en/wcit-12/Pages/default.aspx	The ITU convened the World Conference on International Telecommunications (WCIT) in Dubai, United Arab Emirates, from 3-14 December 2012. This landmark conference reviewed the International Telecommunication Regulations (ITRs),
WELL	Whole Earth 'Lectronic Link	http://www.well.com/aboutwell.html	One of the oldest virtual communities founded more than two decades ago in association with the Whole Earth Review. The service was recently purchased to be run by a group of its own long-term active members.
WGIG	Working Group on Internet Governance	http://en.wikipedia.org/wiki/Working_Group_on_Internet_Governance	Working group on Internet governance (IG) set up by the Secretary General of the United Nations (UN) to investigate and make proposals for action on the governance of the Internet by 2005.
WIPO	World Intellectual Property Organisation	http://www.wipo.int/about-wipo/en/	United Nations (UN) agency dedicated to the use of intellectual property (patents, copyright, trademarks, designs, etc.) as a means of stimulating innovation and creativity.
WSIS	World Summit on the Information Society	http://www.itu.int/wsis/index.html	Held in two phases. The first phase took place in Geneva hosted by the government of Switzerland from 10 to 12 December 2003; the second phase took place in Tunis hosted by the government of Tunisia, from 16 to 18 November 2005.
WTO	World Trade Organisation	http://www.wto.org/	International organisation runs by its member governments whose primary purpose is to open trade for the benefit of all.
WTPF	World Telecom and ICT Policy Forum of the International Telecommunication Union (ITU)	http://www.itu.int/en/wtpf-13/Pages/default.aspx	A high-level international event to exchange views on the key policy issues arising from today's fast changing information and communication technology (ICT) environment. The Fifth WTPF took place in Geneva, Switzerland, from 14 May to 16 May 2013.
www	World Wide Web	http://en.wikipedia.org/wiki/World_Wide_Web	Not to be confused with the Internet, the world wide web is a system of interlinked hypertext documents accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia and navigate between them via hyperlinks.
XML	eXtensible Markup Language	http://www.w3.org/XML/	A simple, very flexible text format derived from SGML (ISO 8879). Originally designed to meet the challenges of large-scale electronic publishing, XML is also playing an increasingly important role in the exchange of a wide variety of data on the Web and elsewhere.

Endnotes

[1] Boston Consulting Group (2012) *The connected world: the Internet economy in the G-20.* Available at http://www.bcg.com/documents/file100409.pdf [accessed 26 August 2013].

[2] OECD (2012) *Internet Economy Outlook.* Available at http://www.oecd.org/sti/ieconomy/ieoutlook.htm [accessed 26 August 2013].

[3] Facebook (no date) Facebook users as a percentage of Internet users. Available at http://en.wikipedia.org/wiki/ Facebook_statistics [accessed 26 August 2013].

[4] ComScore (2013) *Facebook and Google capture the majority of time spent online in Switzerland.* Available at http://www.comscore.com/ger/Insights/Data-Mine/Facebook-and-Google-Capture-Majority-of-Time-Spent-Online-in-Switzerland [accessed 26 August 2013].

[5] Newman M (2012) Interactive: Mapping the world's friendships. Available at http://www.facebookstories.com/stories/1574/interactive-mapping-the-world-s-friendships#/h [accessed 26 August 2013].

[6] Centre for Retail Research (2013). *Online retailing: Britain and Europe 2012*. Available at http://www.retailresearch.org/onlineretailing.php [accessed 20 August 2013].

[7] Dübendorfer T, Wagner A, and Plattner B (2004) An economic damage model for large-scale Internet attacks. Available at http://tansi.info/papers/eco_damage04.pdf [accessed 20 August 2013].

[8] For more information consult ICANN's *Educational material to assist ICANN in deciding what status the corporation should aim for as a private international entity in its host country*. Available at https://archive.icann.org/en/psc/corell-24aug06.html [accessed 30 September 2013].

[9] Members of the online privacy coalition include Austria, Brazil, Germany, Liechtenstein, Mexico, Norway, and Switzerland.

[10] The Annex is an adapted excerpt from material in Kurbalija J (2013) *An Introduction to Internet Governance, 6th edition*. Malta: DiploFoundation and Paque V (2013) *Internet governance (IG) as a diplomatic priority.* Malta: DiploFoundation and University of Malta. MA Dissertation.

[11] This is a simplified version of the seven Open Systems Interconnection (*OSI*) model layers: physical, data link, network, transport, session, presentation, and application layer. For non-engineers, the three-layer model outlined here is sufficient yet fundamental for understanding both how Internet works and what its policy challenges are.

[12] Technical facilities that enable direct connection between various local or regional Internet providers, thereby cutting the costs and latency of traffic flow within the region.

[13] gTLD are domains like .com, .edu, and .org. The announced expansion of the domain space with thousands of new domains, under the guidance of ICANN, would include gTLD like .book, .berlin, .bank, .google, .apple and other.

[14] Root zone file is an original copy of the 'Internet address book' linking TLD with IP addresses. Copies of the file are preserved in and used by 13 Root Zone Servers, most of which are administered by the institutions in the USA.

[15] Due to its format, the old version, IPv4, is limited to about 4 billion addresses (2^{32}) - a global pool that has been formally exhausted in 2011. The pool of the IPv6 format addresses contains practically almost unlimited number of addresses - 340 undecilion (2^{32}).

[16] Kurbalija J'International inviolability for the root zone file?' *Diplo* (Geneva, 13 June 2013). Available at http://www.diplomacy.edu/blog/international-inviolability-root-zone accessed 09 November 2013.

[17] XYZ For a detailed discussion on cyber terrorism (including a definition), please consult the report of the UN Office on Drugs and Crime http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

[18] Gallagher R (2013) After Snowden leaks, countries want digital privacy enshrined in Human Rights treaty. Available at http://www.slate.com/blogs/future_tense/2013/09/26/article_17_surveillance_update_countries_want_digital_privacy_in_the_iccpr.html [accessed 30 September 2013].

[19] Swiss Government (2012) *National strategy for the protection of Switzerland against cyber risks.* Available at http://www.isb.admin.ch/themen/strategien/01583/index.html?download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1ad1IZn4Z2qZpnO2Yuq2Z6gpJCEeX9,fGym162epYbg2c_JjKbNoKSn6A--&lang=en [accessed 12 September 2013].

[20] EU Commission (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Available at http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-on-line-freedom-and-opportunity-cyber-security [accessed 12 September 2013].

[21] Also referred to as the over-the-top providers (OTTs).

[22] Also referred to as Internet access providers (IAPs).

[23] Also referred to as TelCos and Internet Broadband Providers (IBPs).

[24] European Dialogue on Internet Governance (EuroDIG): www.eurodig.org

[25] Open sea is often used as a potential analogy for Internet regulation, especially for proponents of the view that the Internet is beyond national jurisdiction. However, it is not a useful analogy. While the sea is open for navigation, ships and other entities on the open sea are part of national jurisdiction. For example, if the Internet servers are set on the ship or platform on the open sea (as was suggested by some proposal), they will be still under the national jurisdiction of the state where the ship or platform was registered ('flag state').

[26] The first version of GIGI was prepared for the study commissioned by the EDA: *The role of Geneva as an Internet governance hub: A policy study* (Geneva, April 2012).