Chapter 1:  
The evolving Internet governance landscape

This chapter identifies trends in IG. It aims to highlight the digital policy topics that are gaining importance and should be taken into consideration in capacity development initiatives, in order to prepare students for the emerging challenges. This analysis provides the background against which the strengths and gaps in existing capacity development initiatives will be assessed (chapter 3).

Since the World Summit on the Information Society, the term ‘Internet governance’ has been broadened beyond narrow technical concerns to include a wider range of Internet-related policy topics, ranging from legal to societal and cultural issues. At the same time, it is important to highlight that some topics which are considered technical also have a governance dimension. The importance of standards to policy development, for example, should not be downplayed. Different choices of standards may uphold or undermine certain values and rights. This holistic understanding of IG, which places equal weight of technical and non-technical aspects, underpins this report.

Terminology: Capacity development and training

While there is agreement about the importance of capacity development, there is little understanding about what it includes. Moreover, capacity development is often used as a buzzword. Our study shows that the way in which the terms capacity development and training are used, are often interchangeable. Capacity development is a broader concept, which goes beyond training. Capacity development is about change and transformation. Capacity also needs to be understood at various levels: while training often results exclusively in the building of individual competencies (skills and know-how), capacity development aims at creating a sustainable impact on organisations and networks. Logically, it requires more time, and greater resources and planning than training.

Capacity development or capacity building

Capacity development and capacity building are two terms often heard in development discussions. The former refers to developing existing endogenous capacities and skills that are present in all countries, while the latter is used more in reference to a process of starting from scratch and building something that has not existed previously. Capacity development is more widely used in current development parlance.

The various levels where capacities are developed and needed are visualised through the capacity development butterfly (Figure 2) (based on the methodology used by the Swiss Agency for Development and Cooperation).\(^5\)

---

The effectiveness and legitimacy of IG depend on the capacity of nations, organisations, and individuals to participate fully in IG policy processes. Capacities refer to their abilities ‘to define and solve problems, make informed choices, order their priorities, plan their futures, and to implement programmes and projects to sustain them’.

The need for capacity development has been an underlying feature in IG since the WSIS 2003–2005 outcome documents, which underscored capacity development as a priority for developing countries. Likewise, the 2015 WSIS+10 outcome document calls for further investment in capacity development.

Research on capacity development in general and experience from the IG field lead towards the following highlights:

- While the Internet is a global facility, Internet policy is often very local. It is shaped by local cultural and social specificities (e.g. cultural sensitivity for content, relevance of privacy protection). Thus, capacity development should follow local dynamics, taking into consideration local political, social, cultural, and other specific conditions in developing and
implementing capacity development programmes and activities.

- The urgency for capacity development could be addressed by providing just-in-time learning as a part of policy processes. The growing need for capacity in the digital policy field has to be addressed at a more systemic level, by including IG and related topics in the curriculum of academic post-graduate studies.
- Genuine and sustainable empowerment can be achieved through holistic capacity development on individual, organisational, system, and network levels, as visualised in the capacity development butterfly.

This study identified many training activities, but less programmes that provide additional elements of capacity development (e.g. institutional development, network creation, etc.).

**Figure 3. Internet Governance building in construction**
In order to conduct this analysis, IG topics have been clustered according to the IG taxonomy – into seven thematic baskets.\(^7\) The IG taxonomy has been evolving since 1997 when it consisted of 5 baskets: infrastructure, legal, economic, development and socio-cultural. In 2014, security and human rights baskets were added forming the current version of the IG taxonomy. These baskets have also been adopted in the report *Mapping of International Internet Public Policy Issues*,\(^8\) commissioned by the Working Group on Enhanced Cooperation, created under the auspices of the UN Commission on Science and Technology for Development, and was adopted by the Global Internet Policy Observatory (GIPO) of the European Commission.

IG issues are sorted into seven baskets based on their main policy characteristics. However, most issues are of a multidisciplinary nature. For example, the governance of data involves technological, economic, human rights, and security considerations. Data standards, set by the technical community, could impact the security, economic, and human rights aspects of data governance. The level of privacy protection could affect flexibility when it comes to processing user data, the core of the pillars of the Internet industry business model. Multidisciplinary aspects are numerous. The multidisciplinary approach is one of the main success factors for capacity development and training programmes in the IG field.

### 1. Infrastructure

The infrastructure basket includes three issue-areas that are concerned with the core functionality of the Internet. These are: a) the telecommunications infrastructure that facilitates digital communication; b) technical issues related to standards and critical Internet resources: technical and web standards, Internet Protocol (IP) numbers, the Domain Name System (DNS), and the root zone; and c) cross-cutting issues, including net neutrality, cloud computing and the Internet of Things.

In each of these areas, significant changes can be noticed, such as the emergence of new players in the provision of connectivity, an increasing number of attempts to tamper with Internet architecture in order to achieve policy and legal enforcement, and the rapid development of new technologies enabled by ubiquitous connectivity and big data, such as artificial intelligence and the Internet of Things, which are under scrutiny from legal, ethical, and human rights standpoints. Capacity development covering infrastructure aspects should introduce some reflection on the new actors, regulatory initiatives and societal challenges that these changes introduce.

The following trends can be identified in the fields of infrastructure:

**Major Internet companies, such as Google and Facebook, have started to play a key role in the deployment of Internet infrastructure.** These companies have been acquiring parts of the infrastructure or participating in the process of building new connections. Asian Telecom and Google, for example, have established a partnership to build one of the main cables connecting the

---

\(^7\) The term 'basket' was introduced into diplomatic practice during the Organization on Security and Cooperation in Europe (OSCE) negotiations.

United States and Japan. Many other projects are underway, such as a Google-sponsored cable between Florida and Brazil and a cable between Virginia, in the United States, and Bilbao, in Spain, a joint endeavour by Facebook and Microsoft. Internet companies have also started to provide connectivity using innovative technologies, such as drones and balloons.

**Concerted efforts are underway to facilitate 5G spectrum allocation, deployment and standardisation.** These faster and smarter networks will enable the computing power necessary for the development of the Internet of Things and interconnected smart cities. Milestones for the 5G standardisation process have been put forth by ITU. They inspired important policy processes, such as the European agreement on the use of the 700 MHz band, crucial in the deployment of 5G technology.\(^9\)

**Governments have increasingly intervened in the Internet infrastructure as part of law enforcement measures.** This included the imposition of restrictions on Internet infrastructure within their jurisdictions, with the possible negative impact on Internet functionality and availability. Domain name seizures are also growing in number.\(^10\) Such measures also lead to collateral unintended consequences, such as the disruption of connectivity and the accessibility of services in other jurisdictions, as well as the risk of Internet fragmentation.

**There is a clearer perception of the interrelation between technical standards, ethics and human rights.** For example, the Institute of Electrical and Electronics Engineers (IEEE), has published the draft guide ‘Ethically Aligned Design: A Vision for Prioritizing Human Wellbeing with Artificial Intelligence Autonomous Systems’ aimed at encouraging technologists to prioritise ethical considerations in the creation of autonomous and intelligent technologies. A Human Rights Protocol Considerations Research Group has been created in the Internet Research Task Force (IRTF) to research whether standards and protocols can enable, strengthen or threaten human rights. The breaking of silos between technical issues and societal considerations facilitates a transversal approach to human rights. Capacity development on technical aspects that have policy implications could benefit from the inclusion of an ethical and human rights analysis.

**Organisations are intensifying their efforts to encourage IPv6 adoption.** IPv6 adoption is important for many reasons, including enabling the development of the Internet of Things. The results of a survey that looks at how ISPs deploy IPv6 shows that there are certain regional leaders when it comes to IPv6 adoption: the United States in the ARIN region, Belgium in the RIPE NCC region, Brazil in LACNIC, and Japan in the APNIC region, while there seems to be almost no IPv6 deployment in AFRINIC. The global average level of IPv6 deployment is at around 7%, according to APNIC. Capacity development that fosters IPv6 deployment should be further encouraged.

**The implementation of the network neutrality principle remains under discussion.** Although more national and regional norms about network neutrality have been introduced, new price differentiation and zero rating practices trigger discussion. This is one of the most controversial IG policy and regulatory issues, because it involves a careful balance between preserving innovation


\(^10\) In November 2016, over 4500 domain names were seized for selling counterfeit products in a global operation coordinated by Europol, Interpol, and the US National Intellectual Property Rights Coordination Centre.
and the possibility to create new business models, while preserving competition and the rights to information and expression.

**Over-the-top services (OTTs) are being discussed in several regions from legal, economic and infrastructure standpoints.** On the one hand, messaging platforms such as Facebook, Viber and WhatsApp enable people to make free calls and send short messages, in a similar manner that telecommunications services do. In Europe, for example, the proposal of an EU Electronic Communications Code aims to introduce new legal obligations for providers of OTTs that use telephone numbers to allow end users to reach each other (i.e. to call phone numbers/be reachable via a phone number). They are to become subject to the same rules applicable to traditional Telecom operators, such as the obligation to provide contractual information to their customers and switching and emergency call rules. On the other hand, these platforms are responsible for a large amount of data traffic and there is mounting pressure for them to contribute to infrastructure development.

**The global cloud computing market is accelerating.** Companies are increasingly looking at cloud computing as a viable place to run their core business applications. Nevertheless, according to a study conducted by the IDC and sponsored by Cisco, most organisations (69%) do not have mature cloud strategies. Most of the growth will come from large cloud service providers such as Amazon, Microsoft, Google, and IBM, which are continuously opening new data centres, as they try to comply with data localisation requirements. Other aspects related to IG such as data sovereignty claims and the need to comply with data protection and security regulations are additional incentives for cloud service deployment. Capacity development in the area could help small and medium organisations develop their cloud strategies and could tackle the policy and legal issues raised with cloud computing.

**There is increasing interplay among three technology sectors – AI, IoT, and big data.** The elements of this triad re-enforce one another, and capacity development initiatives should take into account this emerging ecosystem. First, AI provides ‘thinking’ for IoT devices and gadgets. It is what transforms cars, for example, from simple vehicles operated by a driver to intelligent driverless vehicles. AI will empower a wide range of tools from vacuum cleaners to toothbrushes and even automated personal assistants. Second, smart devices and the IoT generate a lot of data, sometimes labelled as big data, which is used for data analysis. Insight from data generated by users is the cornerstone of the business model of the major Internet companies (Google, Facebook, Twitter). Third, the circle is closed by the verification of initial AI algorithms based on user-generated data gathered through smart devices. In addition, data analysis identifies new cognitive patterns that could be integrated into new AI algorithms.

**The implications of automation and artificial intelligence (AI) are being increasingly discussed.** The myriad of concerns includes: minimising the possibility of bias being accidentally built into AI systems; ensuring decision-making transparency for AI systems; instigating methods that can verify that AI technology is operating as intended and that unwanted, or unpredictable, behaviours are not produced and assessing the impact of automation and artificial intelligence on the job market.
The Internet of Things will continue its trajectory of growth. It is estimated that by 2020 the number of connected devices will reach 50 billion, causing a profound change in the global economy. This change will largely derive from the fact that the lines between the digital industries and industries that are primarily physical, such as agriculture, construction, transport and manufacturing will increasingly blur. IoT will bring the latter closer to the cyber world and will radically change their way of making business. At the same time, it will allow the largest software companies to make a shift to the physical world. The IoT creates the need for multidisciplinary capacity development in areas ranging from communications infrastructure, standards, security aspects and human rights.

2. Security

Security is among the main concerns of governments, Internet users, technical and business communities. Cyber-threats and cyber-attacks are on the increase, and so is the extent of the financial loss. Cybersecurity came into sharper focus with the Internet’s expansion beyond the circle of the Internet pioneers. The Internet reiterated the old truism that technology can be both enabling and threatening: what can be used to the advantage of society can also be used to its disadvantage. Security is an umbrella concept covering cybersecurity, critical information infrastructure protection, cybercrime, cyber conflict, child safety, spam, encryption and digital signatures. The following trends can be identified in the field of cybersecurity:

Security concerns related to the Internet of Things (IoT) connected devices are increasing. 
Governments are starting to consider developing regulation and companies are putting in place new strategies. Following the large-scale cyber-attacks involving the use of Internet-connected devices and routers that happened in the last trimester of 2016, the US Congress held a hearing on ‘Understanding the Role of Connected Devices in Recent Cyber Attacks’ and experts asked for governmental intervention, in the form of regulations and public policy to improve IoT security. The US Department of Justice (DoJ) created a threat analysis team tasked with studying potential national security challenges posed by Internet-connected devices, such as terrorist threats. The industry is also responding and Cisco, for example, plans to improve IoT security by adapting networks and certifying devices. A survey conducted in Europe revealed that, while most enterprises are aware of the business opportunity presented by the IoT, they also lack an understanding of how to adequately address the associated security risks.

Distributed Denial of Service (DDoS) attacks continue to increase in size, frequency, consistency and complexity. The largest attack size peaked at over 250Gbps, after two years of keeping at around 200Gbps. The majority of DDoS attacks now use multiple attack types, making them more sophisticated. While all the sectors seem to be targeted, IT services, cloud computing and software-as-a-service are the top targets, followed by financial services and the public sector.

National cybersecurity strategies are being developed or improved to face cyber threats. In Europe, the UK is an example of a country that has adopted a comprehensive National Cyber Security Strategy built around three main pillars: defending its infrastructure, deterring criminals and developing its cyber-capabilities.
At the international level, cyberspace is increasingly seen as the fourth military operational domain, in addition to air, land and sea. This comes as a recognition that most conflicts will have a cyber dimension, which is corroborated by the development of national cybersecurity strategies. Within NATO, the practical implications of this decision mean that a cyber-attack on a member state can trigger collective defence by any means (as in Article 5 of the NATO Treaty).

**Bilateral cooperation on cybersecurity is increasing between countries.** An interactive map of bilateral agreements and initiatives for cooperation on cybersecurity can be found here. At the margins of the 2016 BRICS Summit taking place in Goa, for example, India and Russia signed a cybersecurity agreement covering cybercrime cooperation but also matters of combating cyber-terrorism and protecting the critical infrastructure, as well as defence and national security cooperation.

**Cybersecurity laws are giving more power to law enforcement bodies.** Poland, for example, has passed a new anti-terrorism law, which gives its intelligence agency the right to 'order the blocking or demand that the electronic open source service administrator block access to information data,' and thereby allowing it to shut down online media outlets.

**Controls on exports of certain dual-use goods and technologies is being strengthened.** Dual-use technologies are those that ‘may be misused for human rights violations, terrorist acts or the development of weapons of mass destruction’. The European Commission, for example, has issued a proposal for a regulation which aims to strengthen control on the export of certain dual-use goods and technologies to prevent human rights violations associated with certain cyber-surveillance technologies. The export of encryption technologies also falls within the scope of this proposal.

**Concerns with the security of critical infrastructure is increasing.** The Network and Information Security (NIS) Directive, adopted by the European Parliament, for example, defines several categories of ‘operators of essential services’, such as energy, transport, banking, financial market infrastructures, health, water, and digital infrastructure (including Internet exchange points, DNS providers, and top level domain name registries). They are required to take appropriate security measures and notify serious incidents to the relevant national authority.

**The adoption of encryption by online platforms and the use of HTTPS is increasing.** According to Google: 97% of connections to Youtube are encrypted. Netflix moved towards using HTTPS to encrypt the transport of the video content it streams, in order to keep customer information, search queries, and other confidential data safe. Facebook introduced opt-in end-to-end encryption for Messenger chats. End-to-end encryption was also introduced in WhatsApp. At the same time, laws requiring encryption backdoors on messenger apps are being proposed in several countries.

**Extremist and criminal groups are using encrypted messaging and the dark web.** As a response, some governments – such as the German and French ministers of interior – are calling for a decryption legislation that would allow intelligence and law enforcement agencies to access encrypted data. The Apple/FBI case is emblematic of an ongoing discussion on whether - and to what extent - courts can compel manufacturers to assist in providing access to cryptographically protected data on their products, such as cell phones.
Stakeholders are increasingly collaborating on child safety measures. The private industry is developing new measures to identify illegal online child abuse content and identify the victims and perpetrators more quickly, such as the use of hashing technology. Stronger collaboration among governments, LEAs, the industry, educators, and civil society – on both national and international levels – is leading to improved efforts to minimise the online risks for children. At the same time, there is a stronger focus on a rights-based approach which aims at keeping children safe online while safeguarding their rights in the digital environment.

3. Human Rights

The understanding that the same rights that people have offline must also be protected online is the underlying principle for the discussion of human rights on the Internet. Human rights issues should also be understood as cross-cutting and interdependent. For example, the right to freedom of expression and information is related to access to the Internet and net neutrality, while ensuring the protection of privacy is important in dealing with cybersecurity. The following trends can be identified in the field of human rights:

International soft law is further defining states’ obligations when it comes to the protection of the right to privacy online. A UN resolution adopted in December 2016, for example, invites states to refrain from requiring companies to take steps that interfere with the right to privacy in an arbitrary and unlawful way, while specifically calling for informing users about company policies that may impact their right to privacy.

The adoption of national laws that expand investigative powers and data retention and that weaken encryption has been augmenting. Some of these measures have been considered disproportionate by the UN Special Rapporteur on the right to privacy in a report issued in 2016. In many cases, they have also been criticised by human rights activists and the private industry.

International courts decisions’ play an important role in establishing limits to national policies on personal data collection. The Court of Justice of the European Union (CJEU), for example, may pose a challenge to the UK’s Investigatory Powers Act, related to the bulk collection of communications data and set a new precedent for EU member states’ data retention regimes, stating that ‘general and indiscriminate retention’ of data is prohibited.

Human Rights are affected by private networks and platforms that are created, maintained, and operated by ICT sector companies and organisations. Several research initiatives, as well as a report published by the UN special Rapporteur on Freedom of Expression, have pointed out human rights violations, which frequently stem from companies’ terms of services.

Internet disruptions are on the rise, often for reasons related to security and the protection of local businesses. Studies estimate that the negative impact of these measures on economic growth account for USD 2.4 billion per year. The UN Human Rights Council has passed a draft resolution that condemns the intentional disruption of citizens' Internet access.
4. Legal issues

The legal basket includes six issues traditionally associated with the legal aspects of digital policy: copyright, trademark, jurisdiction, arbitration, Internet intermediaries, and labour law. A cross-cutting challenge, common to all topics included in the legal basket, is the application of existing legal mechanisms to Internet transactions, particularly in view of the transborder nature and speed of Internet activities. The following trends can be identified when it comes to legal issues:

Conflicts involving jurisdiction will become increasingly important. The transborder nature of the Internet has posed considerable challenges to the territorially based concept of national jurisdictions. There is a mismatch between the global Internet infrastructure, which naturally transcends borders, and the plurality of legal approaches that countries adopt with regard to issues such as content removal and access to personal data. Conflicts of jurisdiction could lead to the fragmentation of the Internet, as recognised by a 2016 report commissioned by the World Economic Forum.

The limits of intermediary liability are still being defined, especially when it comes to the protection of intellectual property rights. Operators of websites linking to materials that infringe copyright can be found guilty of copyright infringement, if the operators knew or could reasonably have known that the material was illegally distributed, according a CJEU ruling.

Social media platforms may be included within the framework of media companies. The role that social media plays in content distribution has been long emphasised. The attention given to the spread of fake news during the United States presidential campaign stirred up the debate. In response, Google and Facebook have announced to be working on changes to prevent ‘fake news’ websites to use their respective advertising networks. The Cyberspace Administration of China has announced in a statement that media will no longer be able to report news obtained from social media sites without approval.

Alternative models for collecting the revenues of authors for online distribution of their work are under discussion. Copyright reform proposals that address this issue, put forth by the European Commission, have raised concerns among Internet companies, like Google and Mozilla.

The rulings and guidelines are increasingly shaping the sharing economy, including labour law aspects. Court decisions have ruled that Uber drivers, for example, were employees of the company rather than independent contractors. The European Union has issued new guidelines on the sharing economy, which include labour-related issues.

5. Economic issues

Online economic activities have been among the main engines of Internet growth, and contribute to overall economic and social development. The economic basket includes a wide range of policy issues including: e-commerce, virtual currencies, consumer protection and taxation. Capacity
development on economic issues is necessary for all stakeholders in order to foster online businesses, improve legal frameworks and enhance consumer trust. The following trends can be identified when it comes to economic issues:

**E-commerce is being considered a key element to foster development and economic growth.** The digital revolution is expected to play an important role in fostering economic growth in the coming years.

Among the new business models enabled by ICTs, e-commerce has been considered key to fostering development. Business-to-business e-commerce is valued at over USD 19 trillion and business-to-consumer already accounts for over USD 2 trillion. If small companies in developing regions are connected to the Internet, they can enjoy access to the global market, fostering inclusion and development. Initiatives to boost e-commerce in developing countries are being launched, such as the eTrade for All initiative, put forth by UNCTAD.

**Traditional IG policy issues are being included in the multilateral trade agenda.** An exchange of views among WTO member countries mapped the trade-related aspects of e-commerce that would fall under the remit of the WTO, and included issues such as: network neutrality, data localisation, interoperability and encryption. Capacity development on trade policy and digital policy will be necessary to help actors participate in the discussions at the multilateral level.

**Free flow of data is key to the sustainability of trade and of a large number of ICT companies.** The Transatlantic flow of data is governed by a new framework – the EU-US Privacy Shield – which has replaced the Safe Harbour Agreement invalidated by a CJEU ruling.

**Adjustments are being proposed to taxation policies aimed at their application to e-commerce transactions.** This includes, in some cases, the sale of online content. New rules for the value added tax (VAT) are being discussed in the European Union, India and China, for example.

**Virtual currencies are starting to be introduced in monetary systems.** Tunisia and Senegal have adopted virtual currencies. In the latter case, there are plans to expand the use of the currency to the central African region. Blockchain technology is in the base of this development, increasing security and reliability of the virtual currency system. In parallel, there is a recognition that digital currencies pose a money laundering and terrorism financing threat. Europol, Interpol, and the Basel Institute on Governance have formalised the establishment of a tripartite partnership for a working group on money laundering with digital currencies.

**The importance of e-finance and e-banking is expected to grow.** E-finance includes investing, banking, mortgage lending, and it is a reflection of the spectacular growth of the Internet. One example is FinTechs. These technology startups will play a key role in mobile payments, money transfers, loans, fundraising and asset management. When it comes to e-banking, although many traditional brick-and-mortar banks offer online accounts, there are also web-only banks, such as NetBank. Besides convenience, these banks offer superior rates and lower fees.
6. Development issues

The development basket includes the following public policy issues: the digital divide, access, and capacity development. Development issues are cross-cutting affecting all other baskets, ranging from the telecommunications infrastructure in developing countries, through capacity building for cybersecurity protection, to questions related to broadening access to the Internet in the developing world. The following trends can be identified among development issues:

**Alternative platforms and technologies to provide access to the Internet in developing areas will proliferate.** Facebook, for example, is launching satellites that will enable the project Internet.org. It has also launched solar-powered drones that provide connectivity and OpenCellular, a device that allows users to set up their own local wireless networks. AT&T revealed plans to deliver low-cost, high-speed Internet access using power lines.

**The digital revolution is expected to play a key role in fostering economic growth and development in the coming years.** This has been recognised, for example, by the G20 Communiqué from the 2016 Hangzhou Summit. Affordable and universal access to ICTs and broadband connectivity has been also pointed out as a precondition for achieving the Sustainable Development Goals.

**Waves of migration and refugees will increase the pressure for affordable access.** According to the UN Refugee Agency (UNHCR), access to a mobile phone and the Internet is critical for the safety and security of refugees and essential for keeping in touch with loved ones. Refugees living in urban areas tend to have similar access to mobile networks as other urban populations, but in rural areas only one in six refugees have access to connectivity.

7. Socio-cultural issues

The socio-cultural basket includes policy issues triggered by the broad impact of the Internet on the social and cultural life of modern society. This basket covers a wide range of topics, such as content issues, promotion of cultural diversity and multilingualism. The following trends can be identified among socio-cultural issues:

**Pressure to counter terrorism and radicalisation online will increase.** Internet companies Facebook, Microsoft, Twitter, and YouTube have announced the creation of a common database to identify potential terrorist content, and curb its dissemination on multiple platforms, removing content when appropriate. This happens in parallel to lawsuits filed proposed by the families of the Orlando and Paris attacks victims, among other cases, suing Google, Twitter, and Facebook for contributing to radicalisation. Governments are also expressing concerns: the UK Home Secretary admitted that extremist material is spreading online at such a fast rate that UK security services are unable to keep up, while Denmark has announced a list of measures against growing radicalisation.
The right to be forgotten is being introduced in more countries; the delicate balance between the right to privacy and the right to freedom of expression is under focus. More countries have introduced the right to be delisted, although the actual content of laws proposed may vary. A recent law approved in Indonesia, for instance, covers not only search results, but also requests web administrators to remove the actual content. The latest request by the French data protection regulator for Google to apply its delisting across search results globally, drew criticism over the impact on freedom of expression.

Filter bubbles and the lack of transparency over algorithms will be a growing concern. German chancellor Angela Merkel argued that Internet users have a right to know on what basis they receive information through search engines. The lack of transparency over social engine algorithms may ‘lead to a distortion of our perception’ and ‘shrink our expanse of information’.

Barriers to content availability and distribution are among the issues that play an important role on slowing the pace of Internet adoption in developing regions. In Africa, for example, the importance of fostering locally created content, available in familiar languages (which are often different from the official national language), has been emphasised by recent researches. Fostering the diversity of content has always been an issue on the Internet governance agenda. Capacity development is necessary to empower individuals, so they become not only consumers, but also producers of online content.

8. Conclusion

IG is a highly dynamic field, which is undergoing significant changes. Some of them are prompted by the exponential increase in the power of computing and the arrival of a new wave of technological innovation. Big data and the Internet of Things will cause ripples in many policy areas, from security to legal and economic issues.

The second cause of change is the natural expansion and the increasingly complex nature of human activities online. The digital sphere is where most of the speech, interaction and commerce flourishes. The same kind of policy problems that existed offline – from hate speech, to radicalisation; from copyright to the challenges of taxation – need to be faced online. However, these challenges also present new characteristics, such as the viral scale with which they spread and the fact that these public policy issues so easily cut across jurisdictions.

This scenario of transformation takes place in parallel to a process of active digital policy-making. States are enacting national laws and reshaping the agenda of international institutions to deal with Internet related topics. Likewise, International Courts are increasingly called upon to adjudicate and solve emerging tensions. As a consequence, diplomacy and international law will be increasingly important in the years to come.

There is need for capacity development initiatives that are holistic enough to introduce actors to the trends comprised in each of the IG baskets, preparing them for the challenges they will be confronted with in everyday Internet use, and giving them the necessary information to
constructively take part in the governance processes that shape the digital policy agenda. At the same time, it is also necessary to provide a specialised kind of capacity development that will dive deep into specific issues, helping students acquire the knowledge and skills necessary to be fully integrated in the job market, in policy-making processes and in the production of original thought in the IG area. The mapping developed in chapter two sheds some light on the supply of capacity development in the global IG field.