2
Information and Communications Technology (ICT)

General overview

In the first ever issue of *PC Magazine* published in January 1982, Bill Gates predicted that computers and related technologies would change the way people worked. Twenty-five years later in the same publication, Gates reflected that this technology had indeed changed the way we worked but, more importantly, it was changing how we lived.[1]

Information and communications technology (ICT), more specifically digital ICT, is a central part of this change. ICT includes some of the most important technological innovations of the twentieth century.[2] A broad term, ICT and related services span the entire range of the production, consumption and distribution of information in all media, ranging from the Internet and satellites to radio and television.[3] They also include all technologies that collect, distribute, produce, consume and store information.[4] In recent decades no technology has had a global impact on the same level as ICT. Improvements in ICT have transformed the nature of production, communication, and dissemination of information and have expanded their reach. The increasing availability of information and the growth of communications networks have contributed greatly to the process of globalization.[5] Overall, rapidly evolving ICT makes it possible for us to live in a more globalized and interconnected world, and it is directly influencing everything from business to health to global discussions on politics, culture and religion.

The global ICT industry

ICT is an increasingly prevalent facet of modern life, with a strong and growing presence in the daily routines of businesses, governments and

N. R. F. Al-Rodhan, *The Politics of Emerging Strategic Technologies*

private households around the world. In June 2008, nearly 1.5 billion people worldwide were accessing the Internet, an increase of over 300 per cent since 2000.[6] Overall, the global ICT marketplace was estimated to be worth approximately USD 3.7 trillion in 2008, and by 2011 it is expected to have exceeded four trillion USD, even in spite of the global economic slowdown.[7] The United States, Japan and China are the world's largest spending countries on ICT.[8] In total, countries outside the Organization for Economic Cooperation and Development (OECD) make up over 20 per cent of world investment in ICT, and they are responsible for about 50 per cent of all the ICT products manufactured.[9]

While the United States is currently the world's largest user of the Internet and related services, it is likely that this will change over the next decade. Internet usage in China, India and parts of Africa is expected to grow especially quickly, as are these countries' international Internet revenue streams.[10] Some of the major technologies and innovations driving ICT are outlined below.

Relevant technologies

The Internet

First it was the telegraph, then the telephone, the radio and the computer. All these communications technologies laid the groundwork for what is now regarded as one of the most significant technological revolutions of modern times: the Internet.[11] Essentially a widespread information infrastructure, the Internet first made its public debut at the 1972 International Computer Communication Conference. Designed to allow networked computers to communicate transparently across numerous linked packet networks,[12] the Internet is a 'network of networks', capable of delivering information and data to any part of the global network, often in just a matter of seconds.[13] The development of the World Wide Web in 1992 made accessing information over the Internet dramatically easier.[14] Defined by its creator Tim Berners-Lee, as 'an abstract (imaginary) space of information',[15] the World Wide Web was one of the major catalysts that made the Internet more user-friendly and a central part of daily life.

The other major component that helped transform the Internet to mainstream usage was the development of user-friendly web browsers such as Netscape Navigator, Internet Explorer and Firefox. Without the simplicity of design of these browsers, the Internet would never have taken off. Indeed, as J.R. Okin notes, the most remarkable thing about the Internet is how its engineering makes it simple, usable and able to be

customized to a variety of needs.[16] Browsers in particular keep the technical components of the Internet 'hidden from view', making it accessible and user-friendly for those without a highly technical background.[17] Without the advent of these browsers, it is unlikely that the Internet would have become the widespread commercial force it is today.

The Internet constitutes a major shift in the communications realm, largely because of its interactivity and accessibility.[18] Combining computers and telephony, the Information Revolution – as it has been called – makes it possible to create, store, exchange and use information at any time and from anywhere.[19] Moreover, the Internet and related technologies represent 'the sum of all the private and public investment, activities, decisions, inventions and creativity of a billion users, over 23,000 autonomous systems, and countless creators and innovators'.[20] In short, the Internet is the fastest growing communication tool in human history. Since its inception, it has had a profound impact on the global political, economic and social structure. It has changed the way we communicate, the way we educate and the way we access and exchange information.[21]

Broadband

Broadband refers to telecommunications that benefit from a wide band of frequencies with which to transmit information. High-speed Internet is one of the most prevalent forms of broadband, and it allows for faster transmission of data, higher quality services such as streaming video and interactive services, and constant Internet access that is not dependent on a phone line.[22] As broadband becomes more widely available, it is leading to greater economic opportunities, better distribution of Internet services to populations regardless of income or geographical location, and more reliable Internet access.[23] Broadband is largely responsible for the deeper integration of the Internet and related services into our daily lives, as well as for the growing convergence between technology and lifestyle. Broadband is also interesting as an example of technology that was initially designed for a restricted group of users – the military and scientists – that was later extended to the general public. This is a theme that is often seen in cases of emerging strategic technologies.

Web 2.0

Web 2.0 is a term that was coined in the early 2000s for what was perceived to be a new era of the Internet. It was introduced by the Vice-President of O'Reilly Media Inc. Dale Dougherty, as he and other

Internet executives sought to assess the future potential of the Internet in the wake of the 2000 bursting of the 'dot-com bubble'.[24] Web 2.0 is associated with collaboration among users, and a high degree of participation, networking and creativity. Tim O'Reilly defines Web 2.0 as:

> The network as platform, spanning all connected devices; Web 2.0 applications are those that make the most of the intrinsic advantages of that platform: delivering software as a continually updated service that gets better the more people use it, consuming and remixing data from multiple sources, including individual users, while providing their own data and services in a form that allows remixing by others, creating network effects through an 'architecture of participation,' and going beyond the page metaphor of Web 1.0 to deliver rich user experiences.[25]

Sometimes called the 'living' or 'active' Web,[26] Web 2.0 is focused on collaborating, sharing, socializing and connecting. In many ways, Web 2.0 makes the Internet more personal as it offers a space where people have a chance to express themselves and to share their experiences with people around the world. The highly diverse applications and services include social networking, photograph- and video-sharing sites, weblogs (blogs), wikis, podcasts, tagging and social book marking. The use of Facebook, Twitter, YouTube, eBay and so on, is expanding exponentially. In 2009, Facebook directed 13 per cent of traffic to portals such as Yahoo or MSN, while Google and eBay accounted for about 7 per cent.[27]

While the term 'Web 2.0' has been dismissed in some circles as meaningless, it is still one of the best, most concise ways to summarize the changing role the Internet is playing in people's social lives. Web 2.0 is not an all-encompassing summary of the Internet's significance to modern lives, but in terms of social networking and helping people connect with each other at the individual and community levels, the term is quite useful. A more participatory, social Internet has the potential to promote better mutual understanding and positive empowerment, as well as to develop respect and forgiveness among and within cultures. At its best, Web 2.0 could promote the adoption of a set of shared values and, as a result, the creation of a more secure world.

Blogs

Blogs are a key component of Web 2.0, and they are so important that they merit going into with some additional detail. In a previous work,

I designated blogs as the 'fifth estate' after the other modern estates that influence policy: the executive, legislative, and judicial branches of the government and the media as a whole.[28] Blogs are regularly updated online resources reporting about topics and events of interest to the writer. Other key components of a blog include the use of the Really Simple Syndication (RSS)-feed file format, which permits readers to see new content automatically; reverse chronological organization; links to other interesting blogs; and the option for readers to comment on individual blog postings, thus making blogs a very interactive form of media.[29] Blogs have a number of features that make them important for issues of international security. For example, their content often lacks any editorial oversight, which contributes to openness and freedom of speech but also undermines quality control and makes it easier to spread false information.[30] Blogs tend to be difficult to censor and are often reflective of the opinion of the 'masses' as opposed to the elites of a society.[31] As is outlined below, blogs have demonstrated that they are capable of effecting social change and contributing to peaceful dissidence. However, blogs, the Internet, the growing ease of communication and the ability of rogue groups to connect with one another are also increasing risks of terrorism, and contributing to organized crime and manipulation by extremist political groups or cults.

Mobile Internet

Mobile computing refers to the 'ability to use technology that is not physically connected to a static network'.[32] Wi-Fi, a wireless technology using radio waves to offer Internet access, is one of the most popular and important technologies driving this mobile computing revolution.[33]

Mobile Internet technology has become more widespread and accessible through innovations like the Blackberry and the iPhone, and mobile Internet is expected to grow into 'a thriving, low-cost network of billions of devices by 2020'.[34] According to the Research Consultancy Mobile World, about 140 million new mobile subscribers were registered in the first quarter of 2009.[35] Trends in this area point to more 'location-aware' mobile devices that may offer personalized shopping suggestions as you walk down the street, or chances for parents to monitor their child's location.[36] As the technology is refined, mobile Internet will look increasingly like fixed line Internet, offering similar but not completely equal services, speed and accessibility. Overall, mobile Internet will mean increased Internet accessibility and faster, more varied communications. At the same time, more location-aware

mobile devices have the potential to dramatically reduce privacy and heighten vulnerabilities to cyber attacks.

An extension of the mobile computing phenomenon involves technology known as 'augmented reality', a cousin of the once much-vaunted 'virtual reality'. Augmented reality works by starting with a real environment and then adding to it, overlaying digital information over the real world.[37] For example, a person looking at a mountain landscape with augmented reality might see the names of each mountain imposed over the actual mountain. Augmented reality essentially provides a way to blend data available online with the physical world; it is a bridge between the real and the virtual.[38] Although augmented reality has been around conceptually for some time, the rise of mobile computing and mobile phones equipped with features like satellite-positioning systems, fast Internet connectivity, and a digital compass are making augmented reality much more possible.[39] For now, augmented reality mostly helps a person contextualize their surroundings but, eventually, it may help to make advertisements and other media more interactive.[40] As *The Economist* notes, 'the building blocks of [augmented reality] have arrived and are starting to become more widely available. Now it is up to programmers and users to decide how to use them'.[41]

Cloud computing

Cloud computing designs the delivery of hosted services over the Internet. The three categories of service included in cloud computing are Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-a-Service. Unlike traditional Internet hosting, a cloud is sold on demand by the minute or the hour, and it is elastic.[42] In other words, a user can have as much or as little of a service as they want at any given time. In slightly more technical terms, cloud computing refers to a style of computing that allows providers to deliver a variety of IT-enabled capabilities to consumers. What makes cloud computing unique and important is the delivery of capabilities as a service, the delivery of services in a highly elastic and scalable fashion, the use of Internet technologies and techniques to develop and deliver services, and designing for delivery to external customers.[43] Because of its elasticity and scalability, the barriers to entering the cloud computing arena are low, and this allows small companies to grow quickly. Overall, cloud computing promises to make accessing the Internet easier and more cost-effective. This is because cloud computing allows businesses a way to increase their IT capacity and capabilities without the expense, time and uncertainty

of adding new infrastructure, training personnel or acquiring software licences.[44]

HashCache

In many parts of the developing world, a major barrier to using ICT is not the lack of computers but the difficulties in obtaining reliable, fast Internet access. Often, in the developing world only low band-width Internet connections are available, and individual users receive a fraction of the speed of the notoriously slow dial-up connections.[45] US computer scientists are working to develop HashCache, a more efficient method of storing frequently accessed web content on a hard drive rather than using bandwidth to repeatedly retrieve the same information. HashCache reduces Random Access Memory (RAM) and electricity requirements by a factor of ten by using a novel hash function that eliminates the need for a RAM-hungry cache index.[46] Although this technology is still in the early stages of development, it is being field tested in Africa and represents a major move forward in the previously stagnant field of caching. As Jim Gettys, the co-author of the Internet's HTTP specification, has noted, HashCache would allow even the poorest schools and most basic computers to cheaply access one terabyte of web content, roughly equivalent to all the coursework that is freely available from colleges such as MIT.[47]

Computational technology and the rise of supercomputing

Computers are becoming increasingly fast, breaking previous performance records at lightning quick speeds. The world's leading supercomputers can now process information and make calculations at a rate of 1105 quadrillion calculations per second.[48] Since 1961, computers have become faster and the timeline between each increase in speed has become shorter.[49] Two principles in particular highlight this fact: Moore's Law, which states that thanks to ongoing technological advances, computer processing power has been doubling every 18 months for the past three decades (a trend that is likely to continue for at least another decade),[50] and Kryder's Law, which observes that disc memory doubles every 12 months.[51]

Overall, the trend in computational technology is for more functionality to fit into the same amount of space, allowing for more and more powerful computers in smaller and smaller sizes. Smaller dies can also mean less need for power, which in some cases translates to more energy-efficient computers.[52]

In everyday life, faster processors can help process data faster and ensure smooth operations of everything from photo editing to 3D video game playing.[53] However, the real significance of improving computational technology is for science and research. For example, faster computer processors will help astronomers and those searching the universe for extraterrestrial life to measure and process frequencies in space at a much faster rate, allowing more efficient detection of unusual patterns.[54]

Improved computational power will also help in longer range weather forecasting (beyond the current limitations of approximately ten days), better 3D-modelling and, perhaps most importantly, a processor with infinite speed could allow scientists to have a purely numerical and computational model of the universe as opposed to one that relies on rough approximations of continuum mechanics.[55] Some of these latter developments are still hypothetical and may be decades away, but the increasing power of computational technology is already playing an important role in our abilities to process, understand and model information.

Nano-memory storage

Information storage is a key challenge of the Information Age. New memory chips based on nanotubes and iron particles may be capable of storing electronic data for a billion years. Researchers at the University of California in Berkeley have designed a memory cell by taking a particle of iron and placing it in a carbon nanotube.[56] (For more information on nanotubes, see Chapter 8.) The researchers then placed electrodes at each end of the tube, and when they applied an electrical current, the iron particle shuttled back and forth. In this way, the researchers created a '1' and '0,' the signs required for digital representation.[57] What makes this method of memory storage so durable is the fact that the repeated movement of the iron particle does not damage the walls of the carbon nanotube, meaning the process can be repeated almost infinitely. Researchers still need to design a platform that will exploit millions of these memory storage units instead of just one, but this technology could revolutionize how we store electronic data.[58]

Regulatory structures

It should come as no surprise that in a multifaceted industry like ICT, there are numerous regulatory structures and competing visions of who should govern what and how. The Internet is a transnational network of

networks, basically accessible to anyone with a computer, and its regulation and governance are particularly thorny subjects, but even more basic forms of ICT such as telephones are subject to some form of international monitoring and standards setting. An overview of some of the dominant ICT institutions, issues, and controversies is provided below.

The Internet

Internet governance is a contested concept,[59] but perhaps the best starting definition is that of the United Nations Working Group on Internet Governance (WGIG). WGIG has defined Internet governance as 'the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet'.[60] While this is a generally accepted definition of Internet governance, it is by no means the final word on the debate. Some have dismissed WGIG's implied calls for a single Internet regulatory structure, arguing that there is more of a need for 'a heterogeneous and highly distributed array of prescriptions and processes that reflects the Internet's core features, rather than centralized "one-size-fits-all" control over a singular system'.[61] According to William J. Drake, a heterogeneous approach will help policymakers to 'evaluate the full diversity of public and private sector practices' relating to the governance of the Internet and to reflect whether there are cross-cutting issues, gaps or tensions which have not been properly tackled.[62]

The 'world's most visible Internet governance body' is the US-based Internet Corporation for Assigned Names and Numbers (ICANN).[63] Founded in 1998 at the request of the US Government,[64] ICANN is a non-profit public benefit corporation that coordinates Internet domain names and address assignments.[65] Due to its history and the fact that it is based in the United States, ICANN's overall legitimacy has often been questioned. Yet in 2009, ICANN took a step towards becoming more internationally accessible and democratic by allowing the creation of domain names in non-Latin scripts, such as Arabic, Chinese, Russian or other languages.[66] While ICANN still remains US-centric, this step opened up Internet access to a range of people who had previously been restricted in their web usage because of their unfamiliarity with the Western alphabet.[67]

Overall, the Internet today is managed in a generally ad hoc fashion with input from both public and private actors. Private management of the Internet infrastructure is focused on active coordination among private providers.[68] Meanwhile, multiple Internet industry groups are

currently involved in the development of protocols and technical standards and in improving network interconnection and inter-operability.[69] Many industry organizations participate in the global management of the Internet by establishing sets of rules and regulations on issues such as network security, electronic contracting and digital signatures.[70] Noteworthy structures include non-governmental organizations such as the World Wide Web Consortium (W3C) led by Tim Berners-Lee and the Internet Engineering Task Force (IETF). Some have suggested that this ad hoc regulation and the lack of strong global governance of the Internet have allowed creativity and entrepreneurship to play a central role in the development of the Internet. According to them, it is precisely because the Internet was so open and fluid that new modes of business and operation thrived, thus empowering the Internet to fundamentally change the world and our communication with it.

Yet, this type of regulation has not yet succeeded to the resolve the issue of cyber security. Cyber security refers to 'measures to protect information technology; the information it contains, processes, and transmits, and associated physical and virtual elements (which together comprise *cyberspace*); the degree of protection resulting from application of those measures; and the associated field of professional endeavour'.[71] The main challenge for Internet regulation guaranteeing cyber security stems from the fact that, in order to have the truly transnational cooperation necessary to design and implement effective, global regulations, countries have to be willing to share information about their perceived cyber vulnerabilities and threats. Only by doing this will it be possible to clearly define what the biggest risks are and to establish legal guidelines on how to combat those threats most effectively.[72] Unfortunately, such information is often extremely sensitive and is usually deeply connected with a country's intelligence-gathering capabilities and resources.[73] Thus, when it comes to sharing vulnerabilities and information about a country's cyber infrastructure weaknesses – even if this sharing is purportedly done in order to improve global Internet security – countries rightfully fear that sharing such details could increase their vulnerability. This would be especially true if an enemy country exploited the information that was supposedly shared for the greater good and then used it to attack its rival. Trust between countries is a fundamental requirement if better regulation and security of the Internet is going to be established, but the nature of geopolitics means that such widespread trust is far from realistic.[74]

In an editorial published in 2006, I outlined several other key policy challenges relating to the Internet. These include civil liberties versus

surveillance; balancing the potential use of technology by terrorists with the use of technology by governments; and the dissemination of harmful, radicalizing messages versus the spread of positive, peaceful ones.[75] Striking the correct balance between civil liberties and privacy with government monitoring of the Internet for potentially harmful activities is perhaps the most salient Internet regulatory challenge of all, for which the best solution is balanced policies and responsible oversight.[76] Similarly, in trying to ensure freedom of speech, states should look towards the creation of international regulations and organizations that monitor the creation of websites and the types of information they propagate.[77] Even on the Internet, hate-filled rhetoric and messages that incite violence should not be tolerated. Most European countries regulate and aim to eradicate any truly violent or hateful sites.

For its part, the Progressive Policy Institute (PPI) frames the challenge of commercial Internet regulation in terms of jurisdiction and sovereignty, arguing that, at least in commercial transactions, a jurisdiction must be created in which sellers are not subjected to the laws of other countries in their application of new technologies and information systems. The PPI stresses that international rules must protect consumers and create an environment of trust.[78] In terms of sovereignty, PPI maintains that the ideal regulatory framework will 'not let individual nations reach beyond their own borders to control content in cyberspace' but will allow them to 'control both users and Internet hosts within their borders as long as the content controlled is not governed by trade agreements'.[79] Finding a balance between these regulatory recommendations should be a top priority for global policymakers.

The International Telecommunications Union and the global alliance for ICT Development

The International Telecommunications Union (ITU) is the main UN agency overseeing issues related to ICT. As the second oldest international organization still in existence, the ITU has a history dating back to the advent of the telegraph.[80] Its modern day activities focus on coordinating the shared use of the radio spectrum, assigning satellite orbits, improving the communications infrastructure across the developing world, and establishing worldwide standards to encourage seamless interconnection of a multitude of communications system. Additionally, the ITU aspires to address and ameliorate the effects ICT have on the environment and to contribute to improving global cyber security.[81] Based in Geneva, Switzerland, the ITU's membership includes 191 member states and more than 700 sector members and

associates.[82] Since its creation, the ITU has had a foundation in public-private partnerships, and that is one of the key reasons for its longevity and success.

One of the ITU's top priorities is bridging the digital divide, a topic outlined in greater detail below. To this end, the ITU seeks to build information and communications infrastructures and to promote capacity building in the developing world.[83]

The Global Alliance for ICT Development (UN-GAID) is a UN organization that focuses specifically on achieving the ICT-related Millennium Development Goals (MDGs).[84] A platform for policy-dialogue, UN-GAID is committed to improving the accessibility, content, connectivity and educational value of ICT-related technologies.[85]

National regulation

ICT governance on a national level is a highly complex and challenging task. Although the responsibility for ICT networks lies mostly with governments, these networks are often privately owned.[86] In addition, even if governments adopt national legislation to regulate cyber criminality, prosecution, privacy issues and the like, the transnational nature of the challenge often transcends national borders and therefore eludes the reach of individual governments.[87]

China is a particular case in the sense that it attempts to strictly regulate the Internet in multiple ways. For instance, there are currently 12 government agencies working on censoring the Internet.[88] In 2010, the introduction of new legislation requiring Internet providers and telecommunications companies to inform the Chinese Governments about leaks of state secrets was announced.[89] It is also worth mentioning the ongoing dispute between the Chinese Government and Google. Following Google's decision that it would no longer comply with the censorship rules imposed by the Chinese Government, searches conducted on google.cn were automatically redirected to Google's Hong Kong address, google.com.hk, in order to avoid censorship.[90]

As for the United States, a 2008 report by the Center for Strategic and International Studies acknowledges the importance and the transnational nature of the potential threats posed by the Internet as well as the urgent need to react. More specifically, it finds that: 'cybersecurity is a major national security problem', 'decisions and actions must respect privacy and civil liberties' and 'a comprehensive national security strategy must embrace both the domestic and the international aspects of cybersecurity'.[91] So far, the approach adopted by the United States has

been to reinforce collaboration between law enforcement agencies of different countries[92]

In a nutshell, governance requested to face online threats goes beyond national reach. As Buckland et al. argue, private–public collaboration, trans-national collaboration and harmonization of national legislation are key to establishing effective frameworks.[93]

Other regulatory structures

Outside the realm of the Internet, other ICT-related governance mechanisms have been established in the form of legally-binding agreements within the framework of international organizations as well as informal agreements and consultations.[94] Organizations involved are the OECD, the European Conference of Postal and Telecommunications Administrations, the European Union, Asia-Pacific Economic Cooperation, the Asia-Pacific Telecommunity, the Inter-American Communication Commission, Australian Technology United and the European Telecommunications Network Operators Association.[95]

The United Nations is taking the lead on the creation of an international computer security treaty. In July 2010, a team of cyber security specialist and diplomats addressed a number of recommendations for the creation of such a treaty to the Secretary General. Signed by countries such as the United States, China, Russia, India, Brazil and South Africa, the document produced by this task force can be summarized in five points:

Having more discussions about the ways different nations view and protect their computer networks, including the Internet; discussing the use of computer and communications technologies during warfare; sharing national approaches on legislation about computer security; finding ways to improve the Internet capacity of less-developed countries; and negotiating to establish common terminology to improve the communications about computer networks.[96]

The role of the private sector

One of the major characteristics of the ICT revolution is that it has pushed the private sector to engage more directly in public policy making. As new technological opportunities in telecommunications merged with computing, multiple facets of the private sector became deeply and irreversibly intertwined, from banking services to commodity markets, and from capital flows to data systems.[97] Because of the increasing levels of global integration, multinational corporations (MNCs) received a new impetus to pressure governments to liberalize domestic

and international markets.[98] In fact, the human and financial resources of some MNCs exceed the capacities of many governments and allow them to exercise considerable influence.[99]

Compared to governments, industry has very different priorities in terms of the types of regulation it would like to see over ICT and the reasons for engaging in such regulation. While governments routinely emphasize the risk of cyber warfare and the idea that critical infrastructures could be attacked by a rogue or enemy government, businesses and industry tend to be much more focused on their bottom lines, and they structure their approach to regulation accordingly.[100] In particular, the entertainment industry is concerned with the growing phenomenon of copyright piracy, peer-to-peer file sharing, and illegal downloading of music or films. In general, industry groups will be more willing than government agencies to cooperate with other businesses, the government and in some cases even competitors in order to identify vulnerabilities and to create ways to protect their ICT infrastructures from hackers and other malicious parties.[101]

The question of to whom it is that MNCs ultimately report still arises. It is one thing to say that MNCs and industry in general will look to secure their own Internet and ICT infrastructures as a means of preserving their bottom lines. The questions of who will prevent MNCs with a truly international presence from breaching the security of others and who has the jurisdiction to enforce MNCs adherence to any international guidelines, however, remain sticky ones.[102]

Unlike MNCs, small- and medium-sized firms often lack the means to participate effectively in the public policymaking process. In addition, governments can be selective about which firms they will consult or allow to participate in multilateral forums.[103] Thus, private sector regulatory efforts on ICT are by no means clear-cut.

Challenges

Time compression

In the past, the rate of scientific progress has been so predictable that it is treated almost as a law of nature. For example, in scientific research the number of papers published has generally doubled every 15 years, and in astronomy the distance to the furthest galaxy that can be seen from Earth has doubled around every ten years.[104] The ICT revolution has also proceeded at a regular, albeit much faster pace, as evidenced by Moore's and Kryder's Laws, which are mentioned above.

Coupled with the global spread of information through communications networks and the media, this creates what has been called the 'time compression phenomenon'. Essentially, this is a reference to the fact that ICT enables more information to spread more rapidly, which generates pressure for business and policy leaders to react increasingly quickly to new developments. Even if policymakers would prefer to have time for contemplation or analysis of unfolding events, the Internet, blogs, 24-hour news stations and other public forums often create pressure for a quick decision, leaving little time for deep analysis and reflection.[105] Such a situation is made even more dangerous by the potential unreliability of information on the Internet and by the public's tendency to react before all the facts are known.[106]

Time compression is also evident in the economic and financial sectors, where the emergence of a global, active, around-the-clock financial market has resulted in the creation of a trading system that requires computer-dependent decisions and computerized evaluations of market developments for its daily operations.[107] In this environment, businesses and governments alike are forced to react faster to changing developments than they would in the absence of ICT.[108]

People have more access to information and to each other than ever before and, in this context, issues of security and privacy in dynamic wireless networks present themselves. It is important to address the issue of insufficient and sometimes unreliable security infrastructures, as well as the problems related to the security evaluation techniques necessary in the context of emerging wireless networks.[109]

Death of distance

The Internet allows us to identify, relate to and work with other people, regardless of where in the world they are based. Social networking, business matters or research benefit from these developments since physical proximity is no longer required for interaction. This has important consequences for geopolitics, and not all of them are beneficial. For example, it means that cyber attacks can be launched from any part of the world. Often, the origins of attacks cannot be traced back. For instance, although it is heavily suspected that Russia was responsible for a series of cyber attacks on Estonia in May 2007 (discussed below), there is no conclusive evidence.[110]

Privacy issues

Privacy issues are a central concern in today's interconnected societies. One possible definition of privacy, as opposed to security, has

been proposed by Biggs: privacy refers to 'unwarranted access to private information, but not necessarily breaches in security', whereas security refers to the 'access by non-authorised people to protected sites'.[111] The social networking site Facebook is probably the most prominent case of privacy concerns. In 2009, Facebook changed its terms of service, noting that going forward, Facebook would have ownership of all information and material uploaded to its site forever – even after its users cancelled their accounts. Following uproar from consumer groups, Facebook users and the media, Facebook quickly had to at least temporarily reverse its policy change, but the incident touched the heart of the debate over privacy and who controls personal data in the Information Age. In addition, gaps in privacy resulting in the display of protected information are repeatedly being discovered.[112]

Similarly, Google's recently launched social networking service Google Buzz has been heavily criticized. At the time of launching, Buzz drew on contact information stored in Gmail and used it to automatically create a network of friends. Following public outcry, Google had to change its settings.[113]

As the Internet becomes more and more ubiquitous, the trail of information that individuals leave on the web is growing. Much of this trail comes from search engines, where users' searches are saved, often revealing personal identity clues or information.[114] Other concerns relate to how the government or employers might track or monitor personal emails.[115] For as common as the Internet and other ICT outlets are in everyday life, few consumers have a clear understanding of how websites or companies collect, collate and share data about their personal details or habits. Data collected through different ICTs could be used in a number of ways, from more targeted advertising to potentially tracking individuals and sharing information with third parties (the government, insurance companies or future employers).[116]

With regard to Internet privacy, the distinction between personally identifiable information (PII) and non-PII is important. As is indicated by the name, the tracking, storage and use of the former type of information poses a much greater risk to individual privacy than the latter. Unfortunately, consumers are often naive about the distinction, and the potential for the abuse of PII is strong.

Generally speaking, concerns over Internet privacy are two-fold. On the one hand, there are issues of private companies like Internet search engines or web browsers gathering the information provided by consumers and either using it to better market their products or selling it to third parties to use for unspecified purposes. More menacingly,

there are also considerations over governments using ICT as a means to monitor and track their citizens. Information that could once simply be collected can now be digitized and stored on huge interconnected databases, making it easier to build highly detailed profiles of people, their preferences and their behaviour.[117] In order to protect individual privacy in the face of emerging and rapidly evolving ICT, governments must enact strict privacy regulations and rules protecting personal information and regulating how such information can be used.[118] Initially, it seemed as though the dominant paradigm for Internet regulation was going to be industry self-regulation, but such efforts have fallen short and it is becoming increasingly apparent that the government will need to play a bigger role.[119] Priorities for regulation include websites providing notice before collecting information, allowing users' choice over how their information is used, providing consumers with access to collected data, with the ability to contest how such data is used, and the assurance of information security and protection of information from unauthorized use.[120] Companies with privacy policies should not be confused with companies with policies that protect privacy.[121]

Again, such efforts must be broadly multinational, as even if one country protects its citizens' data and Internet privacy, another country may be ready and willing to exploit or sell the same information.[122] Transborder flows of information must be protected, and purely national legislation and guidelines will not suffice on this front.[123] Adding an additional layer of complexity, different nations value privacy and the importance of personal information differently. Indeed, many companies complain about lack of clarity amid competing local, national and international regulatory frameworks.[124] Moreover, many government and private sector leaders worry that overly stringent privacy regulations on the Internet would limit the Internet's commercial potential.[125] Thus, it will be challenging but nonetheless necessary to develop a set of global best practices on this front.[126]

ICT and the environment

The ICT sector is responsible for about 2 per cent of global greenhouse emissions, meaning there is an increasing impetus to improve the greenness of the industry by introducing power-saving features into the various computing platforms, as well as other, more expansive, initiatives.[127] Green ICT firms are gaining more attention for their potential to both reduce their industry's emissions and help offset overall global carbon emissions.[128] In fact, the Climate Group estimates that reductions in the ICT industry's emissions could reduce total global

greenhouse gas emissions by 7.8 billion tons of CO_2 by 2020 – more than five times the ICT sectors own carbon footprint.[129] However, the ITU expresses concern about the effects of the financial crisis on eco-ECTs or energy-efficient ICT, warning that there is a risk that the global downturn may affect the investment needed to change to alternative energy sources as well as research and development efforts.[130]

Geopolitical implications of ICT

Social implications

ICT is one of the key drivers of social change and plays a key role in empowering global civil society; and new information technologies can affect political systems and stimulate political change. This is especially valid in countries where the print and broadcast media are under state control. New forms of ICT outlets such as blogs or mobile phone text messaging, photography, and video are difficult for governments to control and are therefore accessible platforms for citizens to express dissent. By overcoming the information bottlenecks of state-owned media and bypassing censorship rules, bloggers have the capacity to influence the media and the public at large, and the potential to generate positive and negative change in their home countries.

One prime example of this trend is Iran, where the number of bloggers has increased dramatically in recent years. According to the NITLE Weblog Census, Farsi is the fourth most widely used language in the world of blogging.[131]

In April 2009, the power of the new media and ICT was demonstrated in very high-profile ways in the former Soviet republic of Moldova. In the wake of elections that many people perceived as being rigged in favour of the incumbent Communist party, journalists and young people organized an impromptu protest against the government and the elections. What made this protest unique was the fact that it was organized entirely via social media, in particular through Twitter, a micro-blogging service that allows users to post updates on their activities and whereabouts. Moldovan journalist Natalia Morar, the mastermind of the so-called Twitter Revolution, explained to the BBC how simply and quickly the protests came together: 'It just happened through Twitter, the blogosphere, the Internet, SMS, websites and all this stuff', she said. 'We brainstormed for 15 minutes and decided to make a flash mob' in order to protest the elections.[132] Within several hours, over 10,000 people had come on to the streets. The events in Moldova show the ways in which technology is increasing the speed and efficiency with

which people can respond to events, an extension of the previously described time compression phenomenon. The Moldovan protesters took advantage of new technologies that allowed them to act when their anger and frustration were still fresh, and because of the organic nature of Twitter and other tools used to rally people, the protests were organized and enacted so quickly that the Moldovan authorities did not have time to clamp down on the demonstrations until they were already in full-swing. Although the protests ultimately did not result in a regime change, Moldova did receive a visit from European Union (EU) foreign policy chief Javier Solana who promised to begin EU dialogue and engagement with Moldova's opposition parties.[133]

Impoverished populations may also stand to benefit from ICT developments. For example, a United Nations Economic, Social and Cultural Organization (UNESCO) initiative seeks to provide women in rural parts of the world's least developed countries with access to ICT to improve their information resources and to offset a perceived gender imbalance in the distribution of ICT-related technologies.[134] Through chat rooms and other social networking services like message boards and information sharing websites, isolated or marginalized women now have greater opportunities to share and discuss their experiences in health, agriculture and family-planning and, importantly, they are doing so in their own languages.[135] Initiatives like these are especially important because the gender divide for ICT is quite dramatic. In general, and especially in poor, developing countries, women have much less access to the Internet and communications tools than men. This can reinforce women's marginalization in a culture, which can make it harder for women to get jobs or to access educational resources.

More ominously, new forms of ICT are, in some instances, enabling the news media to perpetuate xenophobia and cultural stereotypes. These discourses, which are often one-sided and separated from fact, can fuel aggression and violence against ethnic and cultural minorities.[136] Governments need to work to establish policies that allow for freedom of speech while still clearly outlining guidelines for responsible journalism.[137] In the short-term, it is important to make sure that journalists can operate independently from government or special interests. In the long run, measures should be taken to promote more inclusive societies via ICT. For example, 'peace radios' should be created and promoted in order to offset the influence of 'hate radios'.[138] Above all, cultural respect should be maximized and xenophobia should be minimized.[139] Governments can help in this process by encouraging media programmes about other cultures, their specific sensitivities, and

methods for promoting mutual understanding of different cultures and religions.[140]

Overall, ICT presents great opportunities to generate new scenarios for social relations. New agents from civil society in the field of ICT can have a significant influence on technological, social and political relations on local, national and global scales.[141]

Military applications of ICT

Information technologies have been widely used in military and national security applications. Not only do militaries use ICT in their day-to-day operations, it is also increasingly likely that, in the future, they will use cyber attacks as a way to weaken their enemies during a more traditional military attack.

According to Michael Vatis, the then Director of the Institute for Security Technology Studies at Dartmouth College in the United States, cyber attacks can be defined as 'computer-to-computer attacks to steal, erase, or alter information, or to destroy or impede the functionality of the victim computer systems'.[142] In terms of 'aggressors' initiating the attack, it is important to distinguish between cyber attacks conducted by private criminals and attacks conducted by governments. Ventre suggests distinguishing between 'cyber criminality type attacks', and what he calls 'information warfare type attacks'. Cyber crimes include tools used by criminals which can be dealt with by national legislation while information warfare attacks, or the use of force and armed attacks, refers to states attacking other states or their own citizens.[143] Yet, not all cyber attacks can be as easily categorized. There are also certain grey zones where an attack may not be conducted by a Government, but where a private agency may have been commissioned to do so, on its behalf.[144]

Cyber attacks may put at risk critical infrastructures, such as telecommunications; government and public health records; food and water supply; agriculture and many areas of production.[145] As the World Economic Forum explains, an attack on or a system failure in one part of a critical information infrastructure 'creates a domino effect, shutting down IT-dependent applications in power, water, transport, banking and finance, and emergency management'.[146]

An enemy government could also use cyber attacks to alter information in order to spread misinformation or propaganda. Such actions could provoke anger or fear, or damage morale among target populations and could contribute to undermining public support for a military campaign. Similarly, such misinformation could cause panic in global financial markets and undermine the economic strength of

an adversary.[147] For many smaller countries, cyber attacks are a way of addressing imbalances of power in terms of conventional military strength.[148] Nye, from a geostrategic power point of view, argues that ICT allows smaller actors on the word scene to acquire a disproportionately large share of power. Although resources and geography are still crucial for cyber power, smaller actors do have greater access to ICT power tools than to traditional means. Nye calls this phenomenon a 'diffusion of power', whereby larger powers will dominate the domain less than they dominate areas such as the sea or the air.[149]

Perhaps the most striking case of governments using cyber attacks as part of a more traditional military strategy was in May 2007 when Estonia became the victim of a cyber attack. Although it was difficult to determine exactly who was responsible for this attack, it is widely suspected that the Russian Government played at least an indirect role in the denial of service that wreaked havoc on Estonian businesses and government offices for several days.[150] The attack was initiated in the form of botnets, which are malicious automated computer programs that 'take root undetected in far-flung computers and barrage their targets with useless data'.[151] As a result of the attack, many government and bank websites in Estonia were disabled.[152] The Estonian Government responded calmly and quickly. Although the attacks were disruptive, most sites restored their services in between one and two days. This type of attack – a so-called denial of service – is not the most damaging.[153] Although the Estonian case was very serious, the country's territorial integrity was not compromised, and all damage from the attack was apparently short-term.

The July–August 2008 conflict between Russia and Georgia reflected an escalation of the type of tactics used in Estonia a year earlier. This time, in the conflict over the status of South Ossetia, cyber weapons were openly used as part of Russia's conventional military attack on Georgia.[154] Many government websites, including that of Georgian President Mikheil Saakashvili, were attacked as Russia sought to assert its authority over the former Soviet Republic. Because of this denial of service cyber attack, Georgia's ability to disseminate information to the public during the conflict was severely compromised.[155]

Estonia and Georgia are not the only countries to suffer attacks. In 2007 and 2008 for instance, the United States, Germany, France, the United Kingdom, New Zealand, India, Belgium, China and Russia declared themselves the victim of cyber attacks.[156]

Hopefully, these recent developments will encourage governments to focus more on cyber security laws and policies. So far, most of

the victims seem to have been surprised by and unprepared for the attacks. According to Ventre, 'that our security leaders or our governments admit to the world that they were victims [...] is a confession of helplessness, an acknowledgement of vulnerability and a lack of control'.[157]

As is shown by these cases, cyber war can be used as a part of traditional military strategy. There is also an ongoing debate over whether cyber attacks even have the potential to entirely replace the traditional military in the future.[158] Some argue that cyber war will bring a 'second wave of revolution in military affairs'.[159] Cyber warfare presents multiple policy and legal problems that need to be tackled urgently but, even in the light of recent examples, governments seem slow to respond to this emerging challenge. As a case in point, after being a victim of the cyber attack in 2007, Estonia asked the North Atlantic Treaty Organization (NATO) for help with cyber defence. In response, NATO put a renewed focus on improving its common approach to cyber security.[160] The 2008 NATO cyber security policy sets out the general principles underlying the importance of the issue of cyber defence and asking various NATO agencies to create a coordinated and unified approach for resolving the outstanding issues.[161] However, that policy does not tackle important policy issues such as those related to NATO retaliation in case of an attack.[162] A new 'strategic concept' for NATO was to be agreed in 2010.[163]

There are several policy possibilities for tackling weaknesses in cyber security, including improved education and training, improved risk management, adopting the necessary standards and certification, and using benchmarks, checklists and metrics.[164] To successfully address the issue of cyber security, it is important to create global and national cyber security frameworks.

In terms of securing cyberspace, various initiatives have been undertaken at the national and international levels. The European Union has created the European Network and Information Security Agency, a cyber security agency. The G8 has launched a cyber crime response network.[165] In addition, various private organizations deal with cyber security at the national level, including: the Cyber Security Industry Alliance, the Business Software Alliance, the Information Technology Industry Council and the Software & Information Industry Association. Most recently, the United States has established a national cyber command (CYBERCOM) at the US Department of Defense to protect military networks against cyber attacks and provide the Pentagon with offensive cyber weapons.[166]

Connectivity is crucial in this technologically advanced world, which is why the need to protect cyberspace and assets is so important. The rapid advances in ICT require well-defined strategies for tackling potential cyber threats at the national and global levels. Cyber security is a cross-cutting issue across all types of infrastructure, and it is a foundation for many public and private sector operations. Cyber security threats can change very quickly, so they require protective measures to be as rapid. In this context, it is important to establish global and national cyber security response systems as well as awareness-raising and training programmes. It is also important to develop a strong international cyber security cooperation programme.

Interestingly, many states have been reluctant to improve their cyber security. Many potential initiatives are a hard-sell from a political perspective because they can be costly and long term, and many of the end results are invisible to everyday users.[167] Unfortunately, this means that states and international and regional groups often resort to patchwork proposals in response to imminent or just passed threats. A more comprehensive approach is crucial.

Threats to international cyber security

The US Federal Bureau of Investigation (FBI) has ranked cyber attacks as the third greatest threat facing the United States, second only to nuclear war and weapons of mass destruction.[168] Whether it is the launch of a new virus, an attempt to break into computer systems containing valuable information or something even more sinister, the Internet has many traits that make it both vulnerable and appealing to hackers, terrorists and criminals. The fact that the traits that make the Internet so susceptible to attacks – its interconnectedness and its wealth of information – are the same traits that make it so invaluable to daily life is one of the greatest challenges of Internet security.

Cyber security is extremely difficult to implement, especially in a comprehensive fashion. The Internet has developed at a rapid pace with the constant addition of new systems, and the truth is that the Internet is only as strong as its weakest link. Even a seemingly simple virus can spread rapidly around the world.[169] Adding to the complexity of the threat is the fact that an attack can be launched from anywhere in the world, with surprisingly minimal technical skill or financing required. Moreover, cyber attacks are often difficult to trace to their origin, making it more difficult to prosecute cyber criminals.[170]

Cyber attacks can vary in intention, scope and motive. As is mentioned above, threats may come from individuals, states or even as a

result of accidents or infrastructure-damaging natural disasters such as earthquakes.[171] Although the latter factor is a risk, James Lewis stresses that any large-scale cyber catastrophe will have a human element. 'Could a crisis in cyberspace happen without human intervention? This sort of scenario is very doubtful [...] Cyberspace is a human construct and will most likely require human intervention for it to fail.'[172] The motives for cyber attacks can be equally various. From malicious dissidents who unleash a virus to damage the key infrastructures of their enemies to thrill-seeking pranksters simply looking to wreak havoc or even to international criminal groups looking for financial gain, the range of cyber crimes is almost as broad as the Internet itself.[173] Furthermore, new viruses or worms can be released across a wide variety of platforms, facilitating their spread and making it even more difficult to stop them.[174] As we as a society become more dependent on the Internet, the chance that cyber attacks and Internet viruses will move beyond having only a financial impact to having human costs will increase dramatically.[175] In fact, some cyber security experts argue that the main cyber threats come not from attacks that debilitate critical infrastructure such as power grids but from cyber attacks carried out in conjunction with physical terrorist attacks.[176] For example, a cyber attack could debilitate emergency responders' communications tools at the same time as terrorists set off a bomb. Such a coordinated attack would have the dual impact of having a high human cost and a high financial cost. Although the main motive for cyber attacks until now has been financial profit, such technological uses could well be prompted by political, criminal or terrorist motives.

Cyber threats can take different forms, such as hacking, espionage, identity theft or terrorism, spamming, phishing, data leaks, intrusions, site defacements and denial of service attacks.[177] Commonly used strategies include information warfare, stimergy, swarming, open source models as a guerrilla warfare model and psychological manoeuvres such as the propagation of rumours, using blogs, semantic attacks and the use of web applications by insurgents.[178] They might also include attacks on the information infrastructure, conducting hostile information operations or performing reconnaissance for physical attacks. Cyber experts agree that the United States is a prime target.[179] In 2007, the US Department of Homeland Security logged over 80,000 attacks on Pentagon systems and about 37,000 attempted breaches of private sector and US Government computer systems.[180]

The complexity of cyberspace and its related components makes it difficult to predict how different systems would behave in unexpected

circumstances, thus making it hard to adequately prepare for a potential cyber attack.[181] The major channels of potential attacks are 'through cyberspace [...] by direct destruction or alteration of physical structure, such as buildings or telecommunications lines, or through intentional or inadvertent actions by a trusted insider'.[182] Various combinations of attacks are possible, and they are not mutually exclusive.[183] Conficker, a malicious software programme or botnet thought to have been designed by criminal gangs in Eastern Europe, is among the more recent, high profile examples of the Internet's enormous vulnerabilities. On its release, Conficker easily infiltrated millions of computers worldwide, often without the computer's owner even being aware of the attack.[184] At the time of its launch, Conficker was quickly identified but its potential ramifications were a mystery. It could send spam from infected computers; capture information typed by users or any other number of possibilities. The uncertainty surrounding Conficker underscores the ambiguity of many cyber threats and, more importantly, the difficulty authorities have in successfully combating them.

Potential improvements of cyber security include: approving the necessary standards and certifications, promoting best practices and guidelines, using risk management, improving training and education, using benchmarks and checklists, building a high degree of security into enterprise architecture and adjusting metrics.[185] More aggressive solutions call for a redesign of the entire Internet, possibly having users give up their anonymity in exchange for more security.[186] In fact, researchers at Stanford University are studying options for ways to introduce a more secure Internet structure without disrupting the Internet we are so accustomed to in our day-to-day lives.[187] Such a structure would have improved security capabilities and the ability to support new, complex, and not-yet-created Internet applications. Security measures would be a much more integral part of this system. While the introduction of a universal redesign to the Internet is far from being fully implemented, the fact remains that most cyber security threats are currently dealt with in a piecemeal fashion that neglects the overall security challenges of the Internet's infrastructure and architecture.[188]

Cyber security, like other forms of security, is a public good, but the Internet is unique because of the high level of private sector involvement. 'In a perfect market, the private sector would purchase adequate security and firms would offer the products needed for it. This has not been the case. While some industry sectors, such as financial services, have moved to increase security, other sectors may not improve without further incentives.'[189] In such a situation, the benefits of government

intervention would be great. As both the public and the private sectors become more and more dependent on the Internet and ICT for key day-to-day functions,[190] the need for a comprehensive and coherent policy approach is increasingly apparent. Unfortunately, government regulation of the Internet would be difficult, because the private sector owns many components of the Internet. Additionally, on the Internet, physical jurisdiction is separate from governance.[191] In an ideal world, countries would act to govern the Internet in a more coordinated fashion but, unfortunately, issues of sovereignty are a hindrance in this endeavour.[192]

The digital divide

The digital divide refers to the global gap between the ICT 'haves and have-nots'.[193] According to the United Nations Conference on Trade and Development (UNCTAD), a person in a high-income country is 22 times more likely to have Internet access than a person in a low-income country.[194] Secure Internet servers are 100 times more likely in rich countries.[195] In 2007, less than 5 per cent of people living in low-income countries had access to broadband networks.[196] Moreover, Internet access in developed, rich countries is much faster and relatively much cheaper than the Internet available to people in poorer countries.[197] As ICT develops and evolves, advances in the technologies tend to be to the benefit of wealthier populations, a trend that has been dubbed the '80/20 factor' (80 per cent of ICT profit is made from serving the richest 20 per cent of the population).[198] Even when the poor do get access to ICT, it is generally a modified version of what was originally designed for the affluent, thus many of the poor's ICT needs end up being ignored or neglected.[199]Although it was once hoped that ICT would help leapfrog developing countries to better technological parity with developed countries, the opposite has been the case. Even as the developing world increases the number of computers per capita and other indicators of ICT progress, the differences in quality and relative price and what is available in the developed world far surpass the developing world's progress. Today, the digital divide acts as 'a potential threat to political stability and economic progress' in countries such as China and India.[200] That is not to say that ICT has not brought any benefits to developing countries; in fact, between 1993 and 2001, spending on IT grew twice as fast in developing nations as in developed ones, and such expenditures have improved the productivity of developing economies – China's in particular.[201] To the extent that digital and ICT technologies have infiltrated the developing world, they have

had a positive economic effect. Nonetheless, a gap in the quality and availability of such technologies still exists between the developing and developed worlds.

There are a number of international initiatives under way to shrink the digital divide, including providing Internet kiosks to rural communities, recycling computers, designing affordable computers and providing economic incentives for Internet service providers to operate in poor, rural areas. In spite of these efforts, the digital divide remains a major geostrategic challenge. The United Nations hopes that international efforts to widen access to cell phones, the Internet and other ICT will help to eradicate poverty, and WSIS has increased its calls for donations in order to facilitate reaching this objective.[202]

Advances in mobile technology are also promising on this front. Mobile telecommunications offer the opportunity to avoid the cost and hassle of having to purchase a computer and to pay an Internet service provider for Internet access, a prospect that can be especially costly if Internet services are bundled with telephone landlines and television access.[203] Many people in the developing world already have mobile phones, so now it is just a matter of upgrading that device to a device that is capable of web browsing and adding the Internet plan to that account.[204] In other words, mobile technology is showing promise in areas where other ICT developments have fallen short, specifically in helping developing countries to leapfrog stages of technological advancement in order to be fully connected to the world and the Internet. Admittedly, mobile phones are not a perfect solution to bridging the digital divide, and the challenge of getting Internet-capable mobile phones into the hands of the world's poorer populations should not be understated. Nonetheless, mobile telecommunications do have more potential than earlier forms of ICT to lessen the divide as opposed to expanding it.

Blogs

For all they offer in terms of freedom of speech and freedom of expression, blogs present a number of geopolitical and geostrategic challenges. They provide easier methods for terrorists to communicate and to develop transnational networks, for example. Furthermore, they can undermine overall security by allowing for the promotion of criminal, violent, racist or dangerous ideas and philosophies.[205] Blogs enable extremist groups to spread their messages more effectively and, importantly, they can make it hard to trace the source of the information or to locate the person spreading such information.[206] Blogs run by

military personnel in operations may spread sensitive information.[207] Extensive blogrolls and linking between blogs reinforces this tendency, as it makes it easier to cross-reference and access information related to topics of interest. Case studies on the significance of blogs to geostrategy are touched on in the 'social implications' section of this chapter, but it is nonetheless worthwhile to reiterate their unique importance to global security.

Additionally, there are some blog-specific policy recommendations worth taking into account. For example, it is imperative that anonymous bloggers be discouraged because if bloggers are not willing to take responsibility for their thoughts and postings, the chances of immoral postings or the posting of illegal information will increase.[208] Similarly, it is important to introduce criminal prosecution and liability laws for use against bloggers that incite hatred, violence, criminality, terrorism or other forms of insecurity as well as for bloggers who make unsubstantiated personal allegations or use character assassination.[209] A web of anonymous writers, potentially with connections to terrorists or organized crime, will inevitably undermine global security.

From a geostrategic perspective, the key point is that bloggers need to be held accountable for their writing and actions, and governments need to move to implement the structures that would make such accountability possible. As blogs gain prominence and increasingly play a role in social revolution and political dissidence, it will also be necessary to introduce more quality controls by peers and ethical guidelines for responsible blogging, along with legal remedies in case of unjustified prosecution by authorities or slander and libel.[210] Special priority and preference should be given to blogs that promote peace and transcultural harmony.[211] As blogs become more advanced, technically sophisticated and mainstream, more harmonization and collaboration with the traditional media is also desirable.[212]

An overview of key trends and developments in ICT

From the Internet to social media to faster processors, ICT has revolutionized our daily lives, the way we access and share information, contemporary business models and even how governments respond to and interact with their populations. Social media and Web 2.0 have facilitated protests against governments from Iran to Moldova, and they have also increased the frequency and quality of dialogues between diverse populations. Faster Internet access through broadband technology and the increasing prevalence of the mobile Internet have also encouraged

this trend. Unfortunately, many of the benefits of ICT disproportionately favour the developed world, and poorer countries remain somewhat marginalized from the Internet revolution and other ICT-related developments. Although some initiatives are under way to ameliorate this imbalance, much work still needs to be done. In the end, the hope is that the beneficiaries of the ICT revolution will be developing and developed country populations and industry alike.

Developments in ICT also mean new geopolitical challenges and dangers. Hackers, criminals and even governments are using ICT for malicious reasons, including theft of financial information, denial of service attacks against political enemies and, in some instances, widespread disruptions of Internet servers and Internet access. Even though cyber terrorism is a growing threat to geopolitics, we as a global community are almost universally unprepared to address it. Similar inadequacies exist with regard to ICT regulatory frameworks, and fixing these shortcomings should be a top priority for global policymakers and private sector leaders. Developing appropriate responses to these governance challenges is made even more difficult by the fact that new developments and innovations in ICT happen so quickly that it is difficult, if not impossible, for the slow and often unwieldy policy-making process to keep pace. Multilateral frameworks and an emphasis on global standards and regulation of ICT innovations and applications should be a priority.