Budapest Conference on Cyberspace, 4-5 October 2012

Summary by the Chairman
János Martonyi, Minister of Foreign Affairs of Hungary

Plenary Sessions

Opening Addresses

As Host of the Budapest Conference on Cyberspace I pointed out that the aim is to carry on the work started in London in 2011 and to further discuss some of the most important and difficult policy issues related to the use of the cyberspace. The Internet has revolutionised our everyday lives, driving sustainable growth, giving access to knowledge and providing a platform for the exchange of ideas. To preserve this, we need openness, sound policies and the cooperation of the international community. A safe, resilient and trusted digital environment must be shaped by the interests of civil society, industry and governments across the globe, therefore inclusive and co-operative partnerships are needed. The global challenges of cyber space must be addressed through global cooperation.

Viktor Orbán, Prime Minister of Hungary stressed that the international community is facing the beginning of a new era. He urged countries around the world to step up efforts and cooperate in creating a secure cyberspace. We must prepare to fight against cyber threats, knowing that the possibility exists to launch an attack at a relatively low cost from a simple computer disrupting the operation of an entire country. Day by day, 1 million Internet users become victim of cyber-attacks. To secure the safety and privacy of users and to tackle cybercrime and hostile attacks, the international community has to find the right solutions to manage behaviour in this borderless online space. Hungary’s IT sector has a promising future, as Hungarians have always been at the forefront of information and communication technologies. While the ICT sector is rather capital intensive, past experiences show that a country the size of Hungary, even if capital-poor, is capable of producing serious achievements, contributing to development with their innovative ideas.

William Hague, Secretary of State for Foreign and Commonwealth Affairs of the United Kingdom underlined that Hungary has provided an important leadership to maintain the momentum from the London Conference on Cyberspace. The aim is to address one of the greatest global and strategic challenges of our time: how to preserve and expand the benefits of the digital age? The Internet has been an unprecedented engine for growth, social progress and innovation across the globe. But we also need to shine a strong light on
the darker side of the cyber age. The United Kingdom called for a new international consensus on rules of the road to guide future behaviour in cyberspace, and to tackle the abuses of it. The cyberspace is emerging as a new dimension of future conflicts, and the threat posed by organised cybercrime is growing. There is a divergence of opinion and action between those countries seeking an open future for the Internet and those who are inching down the path of state control.

The UK is determined to remain a world leader in cyber security, to be a pre-eminent safe space for e-commerce and intellectual property online. But, like cyberspace itself, the threat does not recognise borders, and standards of cyber-security need to be improved worldwide. For this purpose the UK is developing a new Centre for Global Cyber-Security Capacity Building, and will be investing £2m a year to offer countries independent advice on how to build secure and resilient cyberspace, improving co-ordination and promoting good governance online.

Kim Sung Han, Vice Minister of Foreign Affairs and Trade of the Republic of Korea also urged the international community to make further efforts to preserve and increase opportunities and benefits of the cyberspace while reducing the risks and challenges. To continue to be an engine for growth, innovation, democracy and cultural diversity, the Internet must be an open and free space. If there is a need to regulate the cyberspace it should be kept at a necessary minimum. Since the Internet has become essential for business, it is imperative for cyberspace to be a safe, secure and trusted domain. In order to effectively tackle borderless cybercrime it is necessary for law enforcement agencies to cooperate with each other. The international community should develop confidence-building measures and explore norms of behaviour in cyberspace in order to avoid potential conflicts between states. Korea will host the next follow-up conference on 17-18 October 2013 in Seoul with special focus on e-government and e-commerce. This series of events should develop into a framework for a comprehensive view on the state of play and a forum representing related interests. Next year’s gathering will be another good opportunity to explore constructive ways to develop a safer cyberspace.
Plenary Session I - Cyberspace: Dynamics and Perspectives

Markus Kummer, Vice-President of the Internet Society pointed out in his introductory remarks the importance of safeguarding the openness and the availability of the Internet for everyone and the need to increase the number of Internet users. The Internet’s organic relationship with freedom of expression and freedom of association is the result of specific design choices – the decentralised nature of the network is a fundamental characteristic. He presented four main scenarios of how the Internet might develop in the future:

- The Common Pool scenario is based on interoperability, open access, open standards and light regulation. It is decentralized, distributed and highly generative, allowing for innovation and competition, based on trust.

- The Boutique Networks Scenario is also generative and allows for innovation and competition, but it is based on exclusive standards and heavy regulation. Its key characteristics are closed devices, client capture and sticky services and it tends towards a command and control approach.

- The Moats and Drawbridges Scenario falls also under the command and control approach, with exclusive standards and heavy regulation. It is a reductive model with a focus on security, risk mitigation and control through rules. Its key characteristics are tight regulation, censorship and content control.

- The Porous Garden Scenario, finally, is a decentralized and distributed model, based on open standards and light regulation. However, at the same time it is reductive with an emphasis on security, risk mitigation and control through rules. Its key characteristics are fragmentation, no consensus and multiple roots.

Lady Ashton, Vice-President of the European Commission and High Representative of the European Union for Foreign Affairs and Security Policy called for maintaining the momentum from the meeting in London last year. Everyone engaged - governments, private companies and civil society – share a common goal of ensuring a free, safe and secure use of cyberspace. Open and free cyberspace has brought unprecedented opportunities to all societies for economic and social progress. Global connectivity also serves as a catalyst, particularly in the developing world, promoting social and democratic reform and protecting human rights. We need to protect the cyberspace from attacks, intensify global efforts to fight cybercrime – but also must resist attempts to use security concerns as an excuse to suppress the Internet. The protection of fundamental rights online is as important as offline. Europe must stand united on this principle. Norms of behaviour in cyberspace between countries must be agreed, existing international laws must be respected in cyberspace; conflicts extending to cyberspace must follow the Geneva Conventions. Principles of commonly accepted laws must also apply in this new domain. The principles of the Budapest Convention are the most efficient international instruments to address cybercrime. Transnational cyber threats should be countered by building global capacity programmes.
and by better coordination of existing initiatives. The initiative announced by the UK Foreign Secretary was welcome. The current multi-stakeholder model of Internet governance has to be strengthened: freedom and creativity have made the Internet flourish. The EU strategy on cyber security to be launched in a few months’ time is expected to bring together different parts of EU policy in the field.

Toomas Hendrik Ilves, President of Estonia highlighted how information technology has changed paradigms concerning a nation's size, wealth, power and military force. Non-state actors can wreak havoc on nation states, aggression need not even be directed on standing militaries – they can be bypassed to cripple a country’s economy. Rolling back the clock is no solution. In cyberspace, oppressive regimes are faced with the import of potentially disruptive liberal aspects of open societies. He further stressed the strategic importance of the processes and decision-making on international level, specifically the upcoming ITU Plenipotentiary in December 2012.

Carl Bildt, Minister for Foreign Affairs of Sweden welcomed the UN Human Rights Council’s resolution affirming that the same rights that people have offline must also be protected online and described the opening of previously closed societies as the most important feature and consequence of the Internet. The socio-political implications of this new “hyper-connectivity” generate challenges to the authorities worldwide. The open and multi-governance nature of the Internet must be safeguarded and preserved, but this requires global efforts and cooperation.

Hillary Clinton, U.S. Secretary of State recalled in her video message the United States’ efforts aimed at tackling the full range of cyber policy issues, which represents a new foreign policy imperative. The U.S. is working to help build an environment in which norms of responsible behaviour guide states’ actions, sustain partnerships, and support the rule of law in cyberspace. The United States has launched new whole-of-government cyber dialogues with Brazil, India and South Africa, has had productive cyber conversations with Russia and China, and continues to work closely with its like-minded partners. The Government is actively working with key international and multilateral partners to find common ground, and is supporting capacity-building in the developing world. It was particularly important to examine how non-governmental actors can help harness the power of the Internet to promote more inclusive government and greater democratic values. She closed by saying “as you look for new solutions and continue these conversations from Budapest to Seoul and beyond, consider the United States a partner every step of the way.” The U.S. Ambassador to Hungary added that freedom should not be sacrificed for security; we must and can have them both.

Amy Adams, New Zealand Minister for Communications and Information Technology emphasised the joint responsibility of business, the IT industry, individual users and state actors in preserving and protecting the freedom of the Internet. Governments around the world are increasingly focused on the need for global collaboration to improve cyber security. As we increasingly move into a fibre world, we must make sure that we get the
balance right between ensuring information, innovation and ideas can continue to flow freely and making cyber space safer and more secure. New instruments to support the security of cyberspace need to be based on existing ones.

Cornelia Rogall-Grothe, Government Commissioner for Information Technology of the Federal Ministry of the Interior of Germany recalled the necessity of finding global answers on both the political and technical level to the challenges and recommended moving forward on the basis of the largest common denominator, promoting soft law approach to customising national approaches to the security of cyberspace. She stated that despite ideological differences a global response has started to emerge. Cyber cooperation is essential in order to find broad consensus. Germany aims to ensure the Internet is an area of freedom, security and justice, working with France, UK and the USA on the elaboration of a code of conduct and confidence-building measures. Germany is in favour of soft laws which are politically binding, and the establishment of norms of behaviour as soon as possible.

Huang Huikang, Legal Advisor of the Ministry of Foreign Affairs of the People’s Republic of China highlighted the challenges presented by the Internet and called on the entire international community to discuss how to meet these challenges effectively, stressing the need to balance the human rights and security aspects related to cyberspace. He pointed out the growth and economic significance of the Internet in China. Domestic legislation still needs improvement and China is exploring a path of Internet management suitable to its national conditions and compatible with international common practices. Cyberspace rules and norms should be elaborated within the United Nations as the most universal and representative international organisation.

China proposed five principles to be observed in strengthening international cooperation: 1) Sovereignty 2) Balance 3) Peaceful use of cyberspace 4) Equitable development and 5) International cooperation, based on equality and mutual-benefit, increased mutual understanding and trust.

Osamu Imai, Ambassador for Cyber Policy of Japan described international cooperation and the full and efficient implementation of the Budapest Convention as the most pressing issue in the short-term. Japan, as the only state party to the Convention from Asia, considers combating cybercrime as the highest priority. Developing the norms of “responsible state behaviour” should also appear high on the international agenda. Japan participates in the international community’s efforts to elaborate norms of behaviour without legally binding nature. Existing international law can be applied to the cyberspace taking into account its special characteristics.

Richard Boucher, Deputy Secretary-General of the OECD focused on the correlation of economic growth and the spread of the Internet. He presented the “OECD Internet Economy Outlook 2012” underlining the growing importance of the IT industry in the global economy, especially in the recovery from the crisis. The Internet is now a fundamental infrastructure
supporting the economy and will continue to expand. This requires, however, that the multi-stakeholder and open nature of the Internet be preserved.

**Plenary Session II - Capacity-Building: Policy Implications and Drivers**

Speakers in this plenary were Cheri McGuire, Vice President of Global Government Affairs & Cyber-security Policy, Symantec (*Introductory remarks*); Sachin Pilot, Minister of Information and Communication Technologies of India; Krista Kiuru, Minister of Housing and Communications of Finland; Genc Pollo, Minister for Information and Communications of Albania; Michal Boni, Minister of Administration and Digitisation of Poland; Vladislav Sherstyuk, Deputy Secretary of the Russian Security Council; Jean-Francois Blarel, Deputy Secretary General, Ministry of Foreign Affairs, France and Francis Maude, Minister for the Cabinet Office of the United Kingdom.

The Internet has yielded fundamental changes in our everyday lives, affecting our social and technological environment. It contributes as a **driving force to economic growth**, it reduces barriers in connection with our trade relations across the world and, at the same time, it enables people to establish closer relations, to communicate and to co-operate.

The Internet opens the door for the unheard to be heard and it can hold governments to account. Its role in supporting sustainable development should not be underestimated either. It is becoming a tool as essential as air, water, food and shelter. Even the basic driving forces of our society are “being transposed” to cyberspace: business, war and love. However, this opportunity accompanied by an increasing interdependence and dependence on cyberspace has brought new **challenges**.

The need to protect information and communication technologies against **potential threats** has risen drastically. It is vital in order to safeguard the smooth functioning of the states and even to reduce the vulnerability of our citizens. Key systems and data on which we rely can be compromised or damaged in ways that are hard to detect or defend against.

Cyber-attacks can disrupt economic and social activities, thus can retard the development of individual states. There were 5.5 billion cyber-attacks in 2011, an 81% increase over 2010. Attacks and malware are becoming ever more sophisticated. The **Budapest Convention on Cybercrime** is the first international treaty for combatting the negative effects of the phenomenon by promoting international cooperation, harmonising national laws and improving investigation techniques.

Nations can only be sure of achieving the economic and social benefits that the cyberspace can offer if they are able to build security and confidence in their systems. Such capacity-building requires institutions, technical tools and skills. National efforts to strengthen cyber-
security are important, nevertheless not sufficient. The characteristic of cyberspace is that it is global, the challenges and threats do not respect borders.

**Capacity-building** can be considered a complex, **multi-layer exercise**. For a long time it was considered technical, but this is not the case anymore. It is a global issue claiming for a global approach. The basic idea can be summarised in three words: **create, cooperate and reach out**. The responsibility is shared; the strengthening of security in the information society requires the concerted effort of all stakeholders, i.e. governments, international organisations, the private sector and civil society.

**States** need first and foremost resources to achieve the capabilities and the level of security and confidence necessary in order to enjoy the full potential of cyberspace. According to the figures, 25% of the cyber-attacks target the governments and the public sector. The approach cannot be limited to risk management; a pro-active attitude is necessary.

The first step a state can take is that of the creation of the legal basis that empowers her to punish and pursue the wrong-doers. States can promote the adoption of procedural and technical cyber-security measures. The establishment of the institutional framework and the organisational structure is also indispensable. Threats require response from states, although views differ on the extent to which this defence can touch upon the rights of the citizens.

The transnational nature of cybercrimes and cyber-threat can only be met through **international cooperation**. There is no state in the world that could possess all the relevant means to fight the former. We depend on each other, and we need to cooperate at national, regional and international level. The challenge to cyberspace is global; however we do not yet have the sufficient capacities to improve the use of cyberspace.

Cooperation is a key word from another perspective as well. **Public-private partnership** must be ensured to guarantee the desired result. Innovative ways have to be found to make sure that the government and public sector, the regulators as well as the technical community and the IT industry synergize properly.

The “**outreach element**” can result in responsible cyber-citizens by empowering end-users to adopt safe behaviour. The end-users and the small and medium enterprises can be called the weakest links in the system. There are 1.5 million “on-line consumer victims” every day. Security awareness programmes should be elaborated, targeting the end-users. The basic aim of such a programme can be to build a stakeholder commitment and at the same time to promote collaboration on cyber-security issues.

All of the above requires a much **greater investment by all players to build cyber-security capacity across the globe**. There are many good programmes out there, but supply is not meeting demand. What is out there needs to be made more accessible and more
accountable. The comments from both governments and the private sector to do more were welcomed.

**Plenary session III - Sharing Knowledge for Global Challenges – the Role of International and Regional Organisations**

Speakers in this plenary were: Neil Klopfenstein, Executive Secretary, Inter-American Committee against Terrorism (CICTE), Organization of American States (*Introductory remarks*); Morris Rosenberg, Deputy Minister of Foreign Affairs of Canada; Guy Berger, Director for Freedom of Expression and Media Development, UNESCO; Jan Kleijssen, Director of Information Society and Action against Crime, Council of Europe; Alexey Lyzhenkov, Director of the Transnational Threats Department of the OSCE; Timothy Unwin, Chief Executive Officer of the Commonwealth Telecommunications Organisation (CTO); Andrew W. Wyckoff, Director for Science, Technology and Industry, OECD and Malcolm Johnson, Director of the ITU Telecommunication Standardization Bureau.

High-level representatives of international and regional organisations and key personalities of cyberspace shared their vision on the evolution of the respective roles played by industry, governments and international organisations in the future of cyberspace, and of their overlapping and complementary responsibilities. Participants heard about the all-important role of international and regional organisations in standard-setting, and their contribution to security. Speakers elaborated on the role of these organisations in human and institutional capacity-building, in exploring and furthering confidence-building measures, and in organising international cooperation to fight cybercrime. The aim of the session was to use this opportunity to share visions and exchange experience to prepare new understandings, and to provide a platform for more, deeper cooperation for an open, free and secure Internet in the service of progress.

The **Organization of American States** has had a cyber-security strategy since 2004. It helps its member states to fulfil the commitments they have undertaken. OAS focuses on three particular areas: (1) technical training, (2) assistance in drafting national cyber strategies, legislation and the establishment of CERTs (3) conducting Crisis Management Exercises. The number of countries that have developed a national strategy, and have established national CERTs, has increased considerably. Regional organisations are well placed to assist the efforts of the international community as it is easier to build consensus on a regional level, they can rely on existing networks and are in a position to provide expertise and tools.

In **Canada** the Internet plays an important role in the social and economic development of the country in areas such as e-health, e-learning and open government. Canada works with other countries to share their national experiences. Sharing experience and improving access to the Internet in the developing world are the two main areas of their work. While there are pressures that are moving certain countries to enhance their control over the Internet, it is important to maintain its openness. In this respect it is necessary to preserve the diversity of
voices and the multi-stakeholder nature of the governance of the Internet. There are already a large number of international organisations dealing with cyberspace. It is therefore important that they bring added value to the process as for example the work of the UN, ASEAN and the OSCE.

**UNESCO** promotes the free flow of ideas and the preservation of the freedom of expression online. Limitation to freedom of speech should be an exception and it is the responsibility of governments to protect freedoms online as it is the case offline. Government action limiting freedoms should be based on proportionality; according to a 2011 UNESCO publication many governments violate this principle. If public morality can limit freedom of expression, it is more important to educate people than to prohibit content.

The **Council of Europe** emphasises the importance of human rights for cyberspace and the crucial role the freedom of expression and the rule of law play in the functioning of the Internet. However freedom comes with responsibilities online as well. Concerning the fight against cybercrime, the importance of acceding and ratifying the Budapest Convention of the Council of Europe was highlighted, and advantages of the document were stressed.

The **OSCE** is active in the field of confidence-building measures. While it is becoming easier for non-state actors to launch attacks, states have even more resources, therefore it is becoming more important to prevent escalation, promote confidence, clarify intentions and enhance predictability in cyberspace. Possible agreed new measures could include clarifying terminology, establishing communication channels that could be used in times of crisis, joint exercises, capacity building, establishing contacts and developing guidelines. It is important to take a step-by-step approach in order to build confidence among participants.

The **Commonwealth Telecommunication Organisation** focused on the criteria that could be important for international cooperation. While international cooperation was crucial it is important to avoid duplication of efforts. The best mechanism is sharing knowledge. Cybersecurity is not just a technical issue, and needs a comprehensive approach from government. Public debate was necessary to discuss the ethical, social and economic challenges and the possibility of putting human responsibility in the centre.

The **OECD** is focusing on the future of the Internet from an economic perspective, and the organisation could provide added value through its existing knowledge-base and analytical work. The data and research in the OECD Internet Economy Outlook 2012 highlight the spread of the Internet’s influence throughout the economy and help support empirically-based policy making.

The **International Telecommunication Union** (ITU) is contributing in this area by bringing together all stakeholders, with such initiatives as the Global Cyber-security Agenda. ITU’s standardization work is particularly important in the design of future networks. The World Conference on International Telecommunications (WCIT) will amend the global treaty on
international telecommunications, known as the International Telecommunication Regulations (ITRs). This new treaty will hopefully further the efforts that are being made to make cyberspace a safer place for everyone.

**Joint Plenary with Youth Forum**

The session provided an opportunity to listen to views on topics of particular interest to young people related to the big themes of the Budapest Conference. Within the framework of the Youth Forum organised on 4th October in parallel with the work of the main conference, a hundred young people aged 17 to 25, coming from Hungary as well as European and other countries gathered to discuss how the Internet and the use of cyberspace can contribute to employment, growth and development; how to reap its social benefits and assert human rights promoting participation; how to handle their digital footprint, and what to do for their own safety on the net. The interaction between the generations in a debate including the participants of both the main conference and the Youth Forum at the end of the day provided an opportunity to channel the ideas stemming from the discussion in the Youth Forum and stimulate further action.

During the session the rapporteurs of the three panels of the main conference provided short outlines of the discussions of the afternoon. The responses came from the five rapporteurs of the sessions of the Youth Forum.

The rapporteur of Panel A on Economic Growth and Development highlighted the fact that the majority of the members of that particular panel were „doers“, representatives of enterprises that make the Internet a reality. He pointed to the importance of broadband availability to the further development of the industry and provided a brief overview of the strategies of the OECD and the World Bank in this field, underlining the importance of preserving the open, dynamic, multi-stakeholder approach that was crucial for success in the past.

The rapporteur from the Youth Panel pointed to the major changes that have taken place in the labour market, and highlighted that formal schooling was not enough. While experience is now considered more important, young people face difficulties in acquiring the necessary expertise to get a job. She also pointed to the lack of coordination between universities and enterprises looking for employees.

In the view of the rapporteur from Panel B on Social Benefits and Human Rights, the panel indicated the major positive developments that have taken place in the past year. Preserving the decentralised nature of the Internet was important to ensuring human rights online. There was no need to create a new framework for the regulation of the Internet, but existing agreements should be applied to cyberspace. The importance of transparency and corporate responsibility was also highlighted, together with the need for governments to take appropriate action to protect human rights in the digital age.
The first rapporteur from the relevant Youth Panel also underlined the importance of human rights for the development of the Internet and the need to preserve the freedom of the Internet. Instead of censorship, the emphasis should be on educating future generations. The role of national governments should be to analyse developments, ensure that younger generations are “cyber literate” and promote their participation in the drawing up of legislation and the implementation process. On the international level, more efforts should be made to support computer literacy in the developing world, to strengthen cyber security and the protection of personal data, while taking resolute action against those perpetrating crimes on the Internet, and involving the youth in the decision-making processes. The second rapporteur from this Youth Panel focused on the definition of e-participation, and pointed to the changes brought by the digital age, such as global reach and the emergence of a common language, that have made it easier for people to influence events. While there are differences in which issues could be influenced, the Internet can be an important tool that should be used to advance the common good.

The rapporteur of the Panel on Cyber Security indicated that further work is needed to come up with a joint understanding of what cyber security is. While there are good examples for strategies to counter security threats, solutions should be adapted to fit local needs. It was important to engage civil society in the dialogue. He also pointed to case studies on how security could be increased, such as in the case of mobile phones in one particular country.

Both rapporteurs from the Youth Forum focused on the importance of education in countering threats to cyber security. Governments should develop guidelines for schools and should follow up on their implementation. Cyber security education should be compulsory. There should be better cooperation between NGOs and schools, and specialists should be invited. Parents also need to be educated on the subject.
Panel Discussions

Panel A - Economic Growth and Development

The main issues covered the importance of broadband access; the proper role and level of the regulatory framework; the significance of background infrastructure, including education; the factors of privacy and security; issues related to intellectual property; the effect of the growing social networks and the expanding network of mobile communication; the relationship between security and development; the connection between technological development, and its acceptance by society; as well as the importance of ICT growth targeting vulnerable groups. Panellists highlighted that the entire economy is subject to the Internet economy these days.

Panellists cited several surveys demonstrating that an open and accessible Web and ICT-related growth has a tangible contribution to economic growth as well as a significant social impact. Participants agreed that outdated regulation can have negative effects on innovation and growth. According to the recent OECD Conference on the Economic Impact of ICT the sector is responsible for 50% of productivity growth in Europe, whereas each job replaced by the Internet sector creates 2.6 new jobs.

Panellists highlighted the importance of cyberspace in international development through presenting a programme that uses mobile technology to provide agricultural and risk-related information (floods, frost, etc.) to rural communities in developing areas from Armenia to Cambodia, with particular focus on targeting (and thus empowering) women. Oxfam gave a number of examples where simple, practical initiatives could empower individuals and make an economy contribute to their life choices. Panellists agreed governments are increasingly acknowledging the role ICT plays in accelerating development.

Participants gave an overview on new trends in ICT-related business (e-books, social networks, online video and gaming, cloud computing), highlighting their impact on ‘traditional’ e-commerce and m-commerce. The focus is shifting towards u-commerce (ubiquitous commerce), based on continuous wireless communication between retailers and customers.

The Chairman of Hungarian software developer Graphisoft gave examples of different patterns of large companies setting global standards and emerging companies in small countries adjusting to the diversity represented by the global market. Taking Hungary as an example, he stressed the importance of scientific education as the most important component of the ICT infrastructure.

The World Bank representative presented the institution’s 2012 Strategy for Information and Communication Technology with its three priority areas: connectivity (contributing to wider access); innovation (fostering ICT-related technical innovation); and transformation
(making development more open and accountable). Three quarters of active World Bank projects have an ICT component and the focus on increasing broadband infrastructure in developing countries contributes to the democratisation of Internet access.

**ICANN** (Internet Corporation for Assigned Names and Numbers), the organisation responsible for coordinating the Domain Name System (DNS) and Internet Protocol (IP) addresses, presented the background work they perform. The new leadership of ICANN aims to ensure the Internet works in a synchronised way, while **enabling wider access for participation to all stakeholders**, thus enhancing legitimacy around the globe.

New initiatives were presented regarding the important, but challenging task of measuring the impact of the web, such as **WebIndex**, a new annual global ranking of countries on the progress and social utility of the web, measuring three attributes: web readiness (quality and extent of communications infrastructure), web use (percentage of individuals online and the quality of content available to users in their language), and the impact of the web (political social and economic effects).

**Panel B - Social Benefits and Human Rights**

The need for a single high level document containing an agreed set of principles governing the use of Internet was raised. Today there are around 30 documents with different principles produced in various forums such as OECD, Council of Europe, WIPO and the Internet Governance Forum. This situation allows „principles shopping”, i.e. countries recognising only those principles that best suit their interests. One speaker argued that the best venue for the negotiations could be the Internet Governance Forum.

The **Norwegian Government**’s efforts to develop online public sector services were presented, highlighting how online services help citizens keep in touch with government institutions, while saving public money. Despite the positive results there are still several difficulties such as the need to review legislation and safeguard privacy.

The role of individual players in cyber space to produce social benefits was discussed. How companies handle official requests for sharing data was cited as a possible example. While international legal norms are fairly clear in such cases, there are many countries in the world where the legal environment is ambiguous and legal procedures lack transparency and accountability. Speakers argued that private companies need to cooperate and decide the appropriate response to such government demands.

Participants highlighted that countries with wider Internet access and freedom of speech have much better development opportunities (and achievements) compared to those that restrict Internet use. Yet, currently 43 states restrict or partly block Internet access compared to only four countries a decade ago. There was agreement on the importance of
transparency reports highlighting government conduct, but also corporate responsibility to keep the Internet as free as possible worldwide.

There was agreement that the Internet provides previously unimaginable development opportunities. The key points of the Netherlands’ cyber strategy were presented underlining the different roles the state, NGOs, and private companies play in achieving its aims.

The discussion highlighted the contradiction between the borderless nature of the Internet and the differing approaches of sovereign states trying to regulate it within their borders. Participants agreed that protecting human rights online is necessary and maintaining freedom of expression on the Internet is a daily struggle, requiring permanent attention. Some argued that countries with overregulation should be confronted with evidence of the better economic results of states not restricting access to the Internet. One participant cited historic examples of efforts to restrain freedom of speech, which were eventually pointless and argued that these efforts will prove fruitless in the near future as well.

Questions were raised about what governments can do to prevent the misuse of cyberspace (such as propagation of false news, etc.). A consensus emerged that Internet providers should not be made responsible for the content, and clear norms should guide companies on the need to delete malicious contents from the Internet. These decisions, however, should be made on a case-by-case basis to prevent unjustified restrictions. Participants commented that in countries where the judiciary is not independent from the government, this issue remains problematic.

Speakers agreed that private companies (and users) should be aware of the dangers; yet they should keep pushing for more openness on the Internet. Balancing between security and freedom of expression is a delicate task; therefore human rights will likely remain a complicated issue for the foreseeable future.

**Panel C - Cyber Security: Building Frameworks for Prevention, Response and Resilience**

Panellists remarked that the safeguarding of resources is a fundamental aim of foreign policy. Today, the Internet, the mobile networks and telecommunication infrastructure are indispensable resources. Participants agreed on the difficulty of finding the right balance between security and freedom in cyberspace. There was general agreement that cyberspace cannot be ruled and controlled by governments alone; other actors in the field need to be involved as well. One panellist outlined the need for a comprehensive strategy for cyber security, and pointed out that the European Union is currently working on a new strategy, building on the discussions of the London Conference last year. The speaker stressed that cyber security is important not only on the EU level, but on the national level as well; therefore Member States must have the necessary capabilities to tackle challenges.
Participants pointed out that the term cyber security is not clearly defined. Further work needs to be done in this area to help define a set of common terms and definitions that will clarify the extent and scope of the different aspects of cyber security. Improving international cooperation in the field is made more difficult by the different approaches within each country. There is no unified solution that suits everyone. Solutions that have proved effective on the national level have taken into account the local culture and way of life, and while they have been successful they will need to be significantly reviewed and adapted if intended to be used in other countries, or on an international level. There was consensus on the need to intensify international cooperation, as well as to involve the private sector in the fight against cybercrime. The protection of critical infrastructure has to be part of cyber security.

Panellists highlighted that the evolving cyber security landscape creates a new set of economic (networks becoming borderless), demographic and geopolitical (access to global markets, global supply chain) challenges. The new generation (“Millennium generation”) is very comfortable with using new technology and has different expectations about the nature of their future work. Participants highlighted that rapid developments in technology render existing solutions obsolete. Smartphone information security needs to be addressed as well. A case study on Smartphone Security was presented with three main lessons: maintaining the operating system constantly updated, ensuring an anti-virus solution is present on the device, ensuring that the operator has a role in scrutinising applications.

The pace of technical innovation has created new challenges concerning information security. Panellists pointed out that cyber security is equivalent to national security in some countries. Societies are getting more concerned about cyber security which is by now a global challenge that requires enhanced international cooperation and sharing of responsibilities. Some countries have done great work in the field which can form the basis for discussions, but these national solutions are not sufficient on the global stage. National strategies can serve as the basis for global co-operation and sharing of information. However, the sharing of security-related information can create risks to privacy which will need to be taken into account. The importance of sharing information and leveraging best practices is essential. It was also felt that a pragmatic approach is needed as overprotection can stifle innovation and can prove to be too expensive. Some delegates pointed out that while we may not be able to reach consensus on everything, there is a need to find a common way forward that is acceptable to all.

**Panel D - International Security: State on State Behaviour and National Security**

This panel dealt with the international security aspects of cyber security and, in particular issues relating to the possibility of state on state conflict. Panellists recognised that discussion concerning this issue is still in its early stages.
Participants noted that, increasingly, cyberspace is being looked at as a venue for military activities. The lack of strong attribution and the potential of State and non-State actors, coupled with countries’ increasing dependence on cyberspace, contribute to a growing potential of miscalculation and misperception between states. Panellists noted countries use differing terms with different connotations in this area and highlighted the distinctions between “cyber security” and “information security”. Some talked of the need to create a document – be it a declaration, a resolution, a guidebook – where consensus is reached on basic definitions. Others stressed the importance of building a consensus around norms and basic principles, rather than spend a large amount of time trying to agree on common definitions. There is a need to apply the existing international law to cyberspace such as International Humanitarian Law. Panellists pointed out that all countries have the right to enjoy the benefits of cyberspace.

**International law applies to cyberspace already** – this is not a “lawless space”, we already have the binding legal framework. Participants agreed on the importance of confidence-building measures as a concrete and practical way to avoid misperception, miscalculation and possible escalation. It was agreed that increasing transparency was crucial in establishing trust and strengthening stability in cyber space. It was established that transparency is essential both on bilateral and multilateral level. Establishing as much cross-connection as possible by exchanging points of contacts was also thought to be essential. Possible additional confidence-building measures could focus on cooperative measures, such as between States against third party criminal threats. The OSCE and the Asian Regional Forum are both doing important work in articulating confidence-building measures.

Panellists pointed out that the developing world needs to be better integrated into cyberspace for the dynamic growth of the ICT sector to continue, as well as to spread the economic and social benefits the Internet can provide. Participants underlined that the benefits of the Internet and the openness of cyberspace are unequivocal. Cyberspace however, can also be a zone of conflict. It was agreed that there was a clear need for a multi-stakeholder engagement with a common responsibility to preserve important elements of cyberspace.

Certain participants highlighted the central role States must play in cyber security, with an important role for international organisations. Panellists agreed that the private sector is nonetheless an important actor that the governments should partner with in addressing security issues. Security needed a holistic approach; we have to respond to the vulnerability and to the threats as well. Panellists pointed out that the practice of private ICT companies in responding to global cyber challenges can serve as a model to be followed when addressing global cyber security threats, with companies such as Microsoft supporting the creation of cyberspace norms.

There were expressions of concern that we are witnessing a militarisation of cyberspace. A clear consensus emerged that transparency, confidence-building measures, capacity-building
and public-private partnership were crucial to make cyberspace more stable and to avoid unnecessary confrontations. Some participants suggested working on cyber issues within the framework of the UN as it is the only organisation that brings together most countries allowing for a comprehensive discussion. Others noted that some work is already occurring in the UN, such as in the GGE, and that the UN, by its nature, is not a multi-stakeholder institution. Instead, it is important now for regional and other organizations and states to discuss and build a consensus around appropriate norms. Some panellists cited the Code of Conduct introduced as a discussion paper in the UN last year as the basis for further discussions. Others noted that the proposed Code undercut the multi-stakeholder approach to the Internet, focused on State control of information, and did not provide a good basis for discussion. Panellists agreed that we do not need an explosion of duplicative activities but that many forums have particular strengths that can be leveraged. Setting norms is important, however, the development of cyberspace is extremely dynamic and norms cannot be put in a single institutional framework.

Panel E - Cybercrime

Panellists agreed that the international battle against cybercrime has become increasingly effective and sophisticated over the last two decades, and there are numerous examples of successful initiatives – including the Budapest Convention on Cybercrime, the G8 24/7 Network, the cybercrime centres being created by INTERPOL and EUROPOL, and an increasing focus on capacity building in the developing world – that should be reinforced and expanded. In addition, these successful cybercrime initiatives can inform and guide efforts to address other emerging cyber issues.

Panellists highlighted a number of attributes of cybercrime, including its borderless and global nature, the ability of criminals to leverage and exploit dynamic and evolving technologies, the increasing role of transnational crime groups, and its increasing impact on both the developed and the developing world.

Panellists highlighted a number of steps that must be taken to successfully combat cybercrime, including: eliminating safe havens for cybercriminals, increasing international cooperation, promoting adoption of compatible legal frameworks based on the Budapest Convention, educating citizens around the world about the dangers of cybercrime, ensuring appropriate prioritization and resource allocation by governments to cybercrime enforcement efforts, and enhancing cooperation and collaboration with the private sector and civil society.

Panellists agreed on the importance of international cooperation in fighting cybercrime, and pointed out that affected states are not always willing to cooperate. Numerous international law enforcement organisations try to counter the lack of political will and offer new, innovative solutions and know-how for countries that lack the technological capacities and
resources in the fight against cybercrime. Participants welcomed the launch in January 2013 of the European Cybercrime Centre to be established at EUROPOL. The new centre will help EU Member States investigate cybercrime issues and share relevant technical data while offering best practices for those in need of solutions and protection on the ground.

Some participants pointed out that responses to cybercrime should include:

- New legislative measures to address cybercrime, with a focus on flexible, technology neutral laws.
- A focus on capacity building and training for law enforcement, prosecutors, and judicial officials.
- Introducing new and sustainable mechanisms for international cooperation.
- Awareness-raising among end-users for preventive purposes.
- Focus on human rights in line with the principles of rule of law.

Panellists concluded with the observation that significant progress is being made in the international battle against cybercrime, and, while many challenges remain, it is important to remain focused on promoting and expanding existing approaches that have proven successful, such as the Budapest Cybercrime Convention, the G8 24/7 Network, the new centres being created by INTERPOL and EUROPOL, and capacity-building in the developing world.

**Workshops**

**Workshop 1: Children on the Internet**

The workshop focused on how to prevent children from becoming hackers/criminals. A former hacker highlighted the importance of education and the role of the parents in providing a solid moral background for their children. Parents and teachers should explain the negative consequences of hacking and/or using malware. The parents themselves should follow developments of the Internet in order to warn their children of the potential negative consequences. A good example was Estonia’s cyber security strategy which advises school curricula to contain IT skills.

Participants agreed that these efforts need to be multiplied and that they will eventually become regular. Continuous dialogue between all parties is needed. Some speakers underlined that companies can provide new technologies to prevent Internet attacks but they cannot solve social problems.

According to research data parents do not wish to block access to the Internet but want to monitor what their children watch online. Information on the dangers of the Internet should
be provided to both parents and children, especially through awareness-raising lectures in schools. This is a shared responsibility of the state and the private sector. The overriding consensus was that Governments need to do much more by way of an education strategy starting in the school with young children and embedding Internet security through the school syllabus.

**Workshop 2: International Law Enforcement Cooperation in Cyberspace**

When dealing with cybercrime one of the biggest challenges is how to obtain adequate evidence for law enforcement agencies and courts. In most cases physical evidence concerning misuse and/or abuse of digital data is located on servers in other (overseas) countries. These being under the jurisdiction of another state, law enforcement agencies and prosecutors have to go through long and complex bureaucratic processes to retrieve digital evidence. Even after evidence is (somehow) obtained another challenge arises in judicial proceedings with the domestic courts accepting or refusing evidence obtained from other countries (in most cases from developing countries with weak domestic regulations on cybercrime). To this end a new concept of reconciled state sovereignty should be introduced that allows for a more effective and flexible approach in combating cross-border cybercrime.

Due to its highly technical nature training is of the utmost importance. Besides law enforcement agencies emphasis should be given to the training of prosecutors and judges involved in cybercrime cases. Improving investigative capacity for law enforcement units and overall raising of public awareness shall be a priority for countries most affected by cybercrime.

Fast and effective data sharing, exchange of vital information, sharing of experiences and best practices among states and their law enforcement agencies is of crucial importance. Law enforcement agencies tend to develop informal networks among specialists on cybercrime, and these peer-to-peer contacts tend to make a huge difference in results. Participants shared the idea to establish in their domestic law enforcement agencies 24/7 cyber units connected with each other.

Global social networks are excellent training grounds to raise awareness concerning threats in cyberspace. User-friendly reporting mechanisms make vigilance in cyberspace an effective tool to identify and counter criminal activities, making data protection everybody’s business.

Participants agreed that international cooperation should be and could be further enhanced on a practical level; at the same time capacities should be provided for units on a local or national level, also to be able to take part effectively in international cooperation.
**Workshop 3: Critical Infrastructure Protection**

The aim of the workshop was to give an overview of the cyber-relevant aspects of Critical Infrastructure Protection.

Presentations touched upon basic definitions for security. The **threat to industrial control systems** is increasing and the number of intrusions detected continues to rise. Also, it was commonly shared and agreed that infrastructure elements – whether physical, technical, or virtual – are all interdependent, and present all modern societies.

Therefore, co-operation among different sectors is a must, as 90% of infrastructure systems considered critical from the point of view of states, industry, and the public are managed jointly by states and private industry. CIP is impossible without co-operation between these two sectors. Related costs must be shared as well. Cyber security is a cross-border topic, thus related costs affect service providers globally.

Governments and societies must set up legal frames like the Hungarian CIP Bill discussed in Parliament. Another global challenge in CIP is the exchange of valuable, useful information, necessitating trusted channels and trusted relations. The human factor is crucial in relation to cyber security of CI – information security awareness has to rise dramatically in all layers. Finally, public media has to be more cautious about publicising cyber attacks – there has to be a balance between raising awareness and avoiding threatening the public.

**Workshop 4: Perspectives on International Security in Cyberspace**

The term “cyber security” potentially spans a very broad spectrum from cyber warfare to passports; and it is easy for the discussions to become too diffuse. Often the conceptual difference of technical and national security embedded in the concept of “cyber security” is not acknowledged the same way by actors with different expertise and experience background. It is therefore important to focus increasingly on the core issues of State behaviour.

There was wide endorsement of the **multi-stakeholder model** and recognition that this is a truly multidisciplinary area and that we need to effectively utilise expertise; Governments do not have all the answers.

Civil society and the private sector need to be creative in getting their messages across, engaging at the national, regional and international level. There is also the need for the more general dissemination of information and for transparency.

There was a general feeling that facts on the ground are likely to dictate the pace of progress and also the direction in which the debate moves. There were several comments on the need
to make early and practical progress; the risks are real and growing.

A common set of norms to which all members of the international community can subscribe may be achievable; continued, inclusive dialogue was essential to this.

The application of international humanitarian law is possible in the cyber military context; the existing international law on the conduct of armed conflicts applies and established principles such as distinction and proportionality are as relevant in a cyber context as they are in the traditional, kinetic context.

**Workshop 5: Security and Privacy Challenges: Digital Trust**

The importance of digital trust was uniformly acknowledged. Every user has the right to rely on the integrity of his data on-line, but also on the safety of the net. Security and trust are inseparable: trust can only exist when equipment and net structures are secure. Privacy has to be secured in the context of growing threats. It is not only a technical concept but a political priority and also a business requirement.

Security and privacy have to be included into data handling from the beginning: this can be described as “privacy by design”. Security and privacy serve the same goal. There is no basic conflict in/between them, but balances have to be struck, compromises found based on strong principles. Data protection is becoming increasingly complex and is marked by diversity.

A couple of challenges and tasks were highlighted. As sound legal bases are already available in most places, or are being elaborated, the accent now has to be on effective implementation of data protection. Effective implementation requires effective supervision and strong enforcement powers; procedures have to be simplified, standardised, and made more cost-effective. The rights of users to control their data, including the “right to erase” have to be strengthened in practice. Protective technologies have to be developed further and harmonized.

Trust is built slowly, gradually, with inputs from identifiable groups. In order to strengthen it and to build trust networks, one should not forge ahead too fast. On the threat side, among the many risk factors, botnets are to be brought to attention as they posing the major danger to privacy. In conclusion, not only are aggregate responses to threats to both security and privacy required, but beyond that a common culture embracing both is to be developed.
**Workshop 6: Cyber Research & Development**

The workshop analysed the security aspects of large research and development infrastructures. All speakers pointed to the increasing need for **enhanced security of large complex systems** where the amount of data is rapidly increasing. They emphasised the complexity of the systems that leads to more components, thus larger interfaces of interaction, and larger interfaces of security hazards.

Large infrastructure examples were the LHC of CERN, used for high energy physics experiments, and Helix Nebula, a Europe-wide cloud initiative, as examples for large intergovernmental collaborations, and the Japanese R&D data networks and their major security challenges. All speakers pointed to the need for collaboration among the key stakeholders of large infrastructures: a good cooperation among academia, industry, and the government sector is a must.

The users' trust in the infrastructure should be improved in the future, not only in technical terms but also on the organisational level. The latter was referred to as "human trust", meaning that the infrastructure works as expected. The Internet of Things also enhances network complexity, thus security issues.

The speakers outlined some **future trends** to be expected: the level of virtualisation will increase in R&D infrastructures; the role of identity management will face serious expansion; there will be more and more data produced that need a treatment different from before; the convergence of supercomputing, grid technology and clouds will be more straightforward.

**Workshop 7: Human Rights Online**

Main issues included international coordination among stakeholders, finding the right balance between legitimate security concerns and the full respect for human rights; and the way to ensure that technologies are used to serve the purpose for which they were initially designed.

There is a risk of laws losing relevance with technological innovations, thus leading to a new phenomenon of companies taking over roles from governments/lawmakers when it comes to ‘policing’ the web.

The representative of the European External Action Service presented their work concerning human rights online, including protection of media freedom, while utilising export controls on technologies and equipment that could be used against human rights defenders and bloggers. There is a need for stronger coordination even among EU institutions, as well as with like-minded organisations and institutions.
The coordinator of the Council of Europe stressed the important role of legal instruments in the field, with special regard to the Budapest Convention of Cybercrime. Implementation is crucial to an effective protection of human rights online.

Civil society representatives highlighted the importance of the work of NGOs in promoting freedom of expression and privacy online, while making sure that the legislative framework put in place by states does not overregulate the cyber framework, leading to Internet censorship. There seems to be an understanding that ‘offline’ rules and principles should also apply online regarding human rights.

**Side events**

**Youth Forum**

The Youth Forum was organised within the framework of the Budapest Conference on Cyberspace. Engaging young people in such a high-level event was important as they would shape the future of Internet, and they already have a huge responsibility at present. As the latest “Facebook revolutions” have shown vividly, online communication in cyberspace is one of the most powerful tools of today.

Since the event on October 4 several participants have already sent positive feedback, confirming that the Forum gave real added value and that they would be happy to take part in a similar event again in the future. One of the participants, a Polish girl, wrote in her e-mail that this Forum was so inspiring for her that she decided to work on projects on Internet literacy and the use of cyberspace.

The main purpose of the event was to provide an open forum for discussion for the youth where they can express their opinions about the opportunities and dangers of cyberspace. The organisers invited a geographically diverse group of participants. In spite of the distances and high travel costs, many foreign youth thought the Forum offered a great opportunity to widen their knowledge on the subject. The participants came from countries as far as Australia, Kenya, Ethiopia, Nigeria, the Russian Federation and the United States.

This global element of attendance made for a great contribution to a comprehensive international discussion. Before the forum young participants shared their cyberspace experiences in their own countries with each other. Thus, they could get first-hand information on the current situation in other countries and get acquainted each other and the trainers of the workshops as well, which made the collective work much easier.

The young participants attended the opening addresses of the conference, which made them felt for the first time, that they are part of a high-level international conference. After the speeches, the Youth Forum got off to an official start: international experts gave their lead-up presentations about the four topics of the Forum (Jobs and Youth, E-participation,
Social problems on the net, Cybercrime and Youth). The thought-provoking and well-prepared presentations provided a special view, and some of them even additional information on national cyber legislation and cyber security issues. The presentations raised a multitude of questions and comments from the participants, including what young people could do against online hate speech; why some videos were not available on the Internet in certain countries, who decided on these matters and why this question divided the global community.

After the lead-up presentations, the young participants regrouped into four smaller workshops. These were led by facilitators and supported by resource persons, the latter being government representatives/experts of certain topics. At the end of day, the Youth Forum participants compiled their suggestions and recommendations, presented by their rapporteurs to the participants of the main conference at a joint session. Conclusions are available on the official website of the conference.

Innovation Showcase

On the first full day of the conference, an interactive exhibition of Hungarian innovative ICT prototypes and products was organised on the premises. The exhibition provided a platform for the Hungarian digital industry – and in particular its start-up ecosystem – to present its main achievements, and to interact with the international participants of the conference. The 23 exhibitors were selected by an independent jury of successful entrepreneurs, investors, and policy-makers. To add to the excitement and engaging power of the event, the exhibitors also presented their projects at a pitch competition.

Three prizes were awarded to the exhibitors. An independent on-site jury picked the winner of the special jury award, while the audience voted on the most innovative project and on the best presentation. The special award of the jury went to Optoforce, a new and low-cost 3D force sensor, impressing the jury with its wide range of potential industrial applications. EasyLing, an innovative, crowdsourcing solution for 1-click website translation received the audience prize for the most innovative IT solution, and the remarkable efficiency-enhancing workforce management system JobCTRL was chosen by the audience for best presentation at the pitch rally. The Institute for Technical Physics and Materials Science of the Hungarian Academy of Sciences received an Honourable Mention from the jury for its exciting research on graphene nano-membranes.

Closing Session

Following the presentation of rapporteurs of two panels and seven workshops I highlighted in my Chair’s Closing Statement that the Budapest Conference, bringing together leaders from governments and industry, the Internet technical community, civil society and youth from around the globe, served well the global dialogue. With over 600 participants from...
over 60 countries, international organisations, companies, NGOs, representatives of the academia, this high-level event attracted wide interest.

The Internet is an unrivalled source of creativity, economic opportunity and dynamism globally. But we also have to be aware of the serious threat posed by cybercrime and the abuse of cyberspace. True to our motto: “With Trust and Security for Freedom and Prosperity”, the aim of this conference was to find consensus along shared principles and to set out the agenda for how to build a secure, resilient and trusted global digital environment as defined in London.

We must share the benefits of the digital age – striving to minimise threats without undermining our commitment to fundamental freedoms. It is a general understanding that stronger co-operation and collaboration is needed to build confidence and trust, and to avoid problems arising from misunderstandings. Government actions need to be measured and existing rules of international law and the traditional norms governing interstate relations apply to cyberspace.

There is a clear consensus that the Internet is a crucial contributor to economic growth and a key driver of gains in productivity globally. New and increasingly affordable technologies such as mobile Internet are opening up new possibilities, narrowing the digital divide. In developing countries these new technologies are driving progress in, and access to, education, healthcare and financial services helping us reducing poverty and achieving the Millennium Development Goals. OECD presented a study highlighting the significant contribution Internet companies continue to make to growth and job creation. We now have to broaden access to e-communication. It is our joint responsibility to ensure that the Internet remains open; and people can use services and applications, can decide on the ways to get connected, the only restrictions being those for their safety and privacy. Several delegates noted that the Internet is also a tool of good governance, promoting transparency and accountability, serving democracy. I welcomed the announcement by the President of ICANN to more fully engage with their global stakeholder base and to encourage greater participation across the world.

Many expressed support for the principle confirmed by a UNHRC resolution that rights to freedom of expression and association apply with equal force in cyberspace. Digital space cannot really be dissociated from real space. Transparency is needed in our handling of privacy and data protection issues. Many participants noted that freedom and security in cyberspace are not incompatible.

Delegates agreed on the urgent need to protect users against abuse. The number of cyber-attacks is reaching levels never seen before. Participants pointed out that the victims are governments, businesses, but most often ordinary users. We should be particularly aware of the need to protect our children. Delegates agreed that we need mechanisms to protect the integrity of online transactions from fraud. They have expressed their sentiment that in
order to benefit from the opportunities presented by cyberspace more needs to be done on global cyber security capacity-building to help countries derive all the potential benefits offered by the Internet. I welcomed the new UK Centre of Excellence to advance international cooperation and capacity-building.

There is a need for humility on the part of governments and an acceptance that there are limits to state power. We must also be flexible: overprotection is both too costly and wasteful. There was overwhelming support that setting standards and norms for the future of cyberspace is the joint responsibility of all stakeholders. All governments must conduct themselves in a manner which does not hinder international peace, security and justice. International and regional organisations provide good forums for continued cooperation. I welcomed the on-going work of the UN, OSCE and ASEAN Regional Forum on norms of behaviour. I welcomed Korea’s initiative for increased cooperation in establishing crisis communication channels and supporting capacity-building. There was general agreement that all stakeholders, users, companies as well as governments share responsibility in preventive actions on cybercrime. We need to recognise the important contribution from industry and civil society. Industry has a key role in developing products, standards and systems with improved security. Academia also has an important contribution to make.

The conference has reinforced the willingness and readiness to focus on creating and safeguarding a reliable and secure cyberspace. We need to continue promoting greater collaboration between states to fight cyber-crime, which affects all of us, and does not respect borders. I welcomed the creation of the new Europol and Interpol centres on cyber security.

There were some generally accepted points:

- The Internet is for everyone, and everyone is a stakeholder.
- Broadband and capacity-building are keys to economic and social usefulness. Several important initiatives were identified and new ones launched here.
- Openness is a key to further progress.
- International cooperation is needed, and offline laws and norms must apply.
- We should continue our dialogue and make it even more inclusive. I encouraged more countries to engage in the lead-up to next year’s conference.
- We should include the next generations, which is why I was particularly happy about the great contribution the Youth Forum has provided to our work.