GLOBAL CONFERENCE ON CYBERSPACE 2015

CHAIR'S STATEMENT

Introduction

1. On 16 and 17 April 2015 representatives of governments, international organisations, businesses, civil society, academia and the technical community gathered in The Hague, the Netherlands, to discuss key developments in the cyber domain with a view to presenting a forward-looking agenda to promote a free, open and secure cyberspace. The Conference built on the strong foundations laid by previous conferences in London (2011), Budapest (2012) and Seoul (2013), including the Seoul Framework for and Commitment to Open and Secure Cyberspace.

2. The use of ICTs, and in particular the Internet, has become a matter of strategic importance for governments, businesses and citizens alike. Governed through a partnership between all stakeholders concerned, the Internet is an engine for economic growth and social development that facilitates communication, innovation, research and business transformation.

3. This increased importance has also presented our global community with new challenges. As our societies become more interconnected and dependent on the Internet and ICT, we become more vulnerable to misuse of these technologies. We need to ensure that the security of our ICT infrastructure is continually improved in order to maintain its integrity as well as end users' trust in its reliability. We also need to be mindful that our own actions or inaction may impact on the security of others: security is a matter of collective responsibility. We need to foster a culture of collaborative security.

4. Similarly we need to ensure that human rights, including the freedom of expression and the right to privacy, are protected online as they are offline. Our commitment to protecting these rights must be unequivocal. As in the offline domain, violations of these rights must be addressed within the framework of the rule of law.

5. A free, open and secure Internet is a global resource which should be managed in the public interest. We need to ensure that the various stakeholders play an active role in the ongoing discussions about its governance, management and security. We must also ensure that those who do not yet have a voice in this debate are empowered to participate in these discussions – discussions which will also shape their future.

6. We believe capacity building in cyberspace, including the sharing of good practices, knowledge and expertise, is an essential component of international cooperation. The Global Forum on Cyber Expertise (GFCE), which was launched during the Conference in The Hague, is a key initiative for fostering international solidarity and providing political, technical and financial support for efforts to strengthen international cooperation among all stakeholders in the cyber domain. The GFCE will focus on capacity to safeguard cyber security, fight cyber crime, detect and counter cyber threats, and protect privacy and data security.

7. The Conference has taken stock of key developments in the various fields and has offered a platform for presenting and discussing important issues for the near future. It aims to be a catalyst for discussions on key aspects of the cyber domain, presenting an integrated strategic view of the issues. We welcome the general agreement that there is an urgent need for international cooperation on cyber issues among all stakeholders. We must continue to work

towards convergence of opinions to enable us to adapt to rapid technological developments and continue to shape our societies, making them more cyber capable, cyber aware and cyber secure.

8. At the same time, the Conference has offered a platform for presenting new ideas and practical tools that can be of use to various stakeholders. We welcome these contributions and encourage participants to make use of them. An overview of the contributions has been included in Annex A.

Economic growth and social development

9. The Internet has a major transformative influence on the global economy. The Conference discussed the economic impact of the Internet over the past few decades and explored future scenarios. The Internet-based economy has a bright future, provided that key conditions are in place, such as trust, education, and the right policy frameworks to promote participation, innovation, trade, competition and investment.

10. The importance of access to open, secure and resilient communication infrastructures around the world was stressed. It is equally important that developing countries can fully participate in the Internet economy. Delegates underlined the importance of including the need for Internet access for all and cyber-capacity building in the post-2015 Development Agenda. Particular attention was paid to the importance of implementing open Internet standards (e.g. IPv6 or DNSSEC). Businesses and governments were called upon to pay more attention to their respective roles in the maintenance and continuous development of the Internet as an infrastructure.

11. As the Internet economy develops, it will integrate more deeply into society, often with normative implications. The Internet economy has already changed our views on doing business in many economic sectors such as retail, banking and trade. Big data is expected to play an important role in digital innovation in the coming years. Innovation and economic growth will depend on various factors such as access to capital, a skilled workforce and, not least, trust of end users. Governments, businesses and civil society all have a role to play in creating a safe place to do business in which people's privacy is respected and their data are protected. The development of 'Privacy by Design' and cyber security solutions offers great business potential as well as social benefits.

Internet governance

12. The Conference reaffirmed its commitment to the multistakeholder model of Internet governance and called upon all stakeholders to further strengthen and encourage the sustainability of, participation in and evolution of this model.

13. With respect to the Internet Governance Forum (IGF), there was general support for the view that this global platform for multistakeholder policy dialogue on Internet governance issues should carry on and improve, including through enhanced and inclusive participation by all stakeholders not only at global level, but also at national and regional level. There was strong support for the renewal of the IGF's mandate beyond 2015, to be decided on by the UN General Assembly in December 2015.

14. The Conference acknowledged the efforts and progress made in utilising a multistakeholder mechanism to transfer the stewardship of the functions of the Internet Assigned Numbers Authority (IANA), operated by the Internet Corporation for Assigned Names and Numbers (ICANN), to the global Internet community. The Conference recommends future mechanisms to recognise the respective roles and responsibilities of all stakeholders. These mechanisms should preserve the current stability, security and good functioning of the Internet. The Conference

welcomed the ongoing work being done in the Internet community on enhancing the accountability of ICANN to the global Internet community.

Multistakeholder approach

15. From the beginning of the London process, through Budapest and Seoul, there has been a growing commitment to cooperation among stakeholders. Governments were urged to ensure that cyber policy at national, regional and international level is developed through multistakeholder approaches, including civil society, the technical community, businesses and governments across the globe. Only then can the increasingly complex cyber challenges be fully addressed. To ensure that the Conference reflected the above principles, the Netherlands facilitated the organisation of a civil society pre-conference. The participants encouraged future editions of the Global Conference on Cyberspace to include a civil society pre-event.

16. Similarly, throughout the London process reference has been made to the importance of human rights and the protection of fundamental rights online. At the same time there are concerns that certain cyber security measures could suppress the openness of the Internet and undermine users' rights. The Conference urged all stakeholders to work together proactively to ensure that cyber security policies are, from their inception, rights-respecting and consistent with international law and international human rights instruments, including the International Covenant on Civil and Political Rights and International Covenant on Economic, Social, and Cultural Rights.

17. The Conference recognised that the multistakeholder approach has also been key to facilitating the implementation and realisation of the goals of the World Summit on the Information Society (WSIS) and called for this year's concluding stages of the WSIS 10-year Review to be as open and inclusive as possible, ensuring the meaningful participation of all stakeholders.

Cyber Security

18. Raising awareness of cyber security in all areas of society is essential. New generations of skilled users and cyber security professionals are needed to safeguard the security of cyberspace and to unlock the economic and social potential it offers. Awareness and proficiency in the use of user security measures, as part of a digital literacy programme, can be achieved by educational programmes, including on Cyber Healthiness and Hygiene, for individuals from all age groups and educational and social backgrounds. People should be empowered with a basic understanding of cyber security and have an understanding of how to protect themselves. We hope this will motivate those with the aptitude to pursue a career in the field. During the Conference, examples of innovative and stimulating educational programmes were demonstrated.

19. Governments, businesses and citizens have a shared interest and responsibility for ensuring that cyberspace remains secure. As more and more products and services move online, the importance of good cyber security increases. Both users and suppliers have a role to play in improving the security of online products and services. Suppliers should understand and follow best security practices in hardware and software development to mitigate risks, and be open about problems that do arise. Users should be aware of the risks associated with their online activities and know how to manage these risks. This includes properly managing their ICT and patching and taking countermeasures to address ICT vulnerabilities. They should also be assertive in demanding secure products and services.

20. The Conference concluded that Public/Private Cooperation (PPC) has delivered a number of concrete results at international, regional and national level, such as the UK's Cyber-security Information Sharing Partnership (CISP) or the Triple Helix model of The Hague Security Delta. Delegates emphasised the importance of promoting the international exchange of PPC best practices and lessons learned.

21. Critical infrastructure is the backbone of our economies, security and health. The Internet has become fundamental for the functioning of critical sectors including energy, telecommunication, transport, health care and banking. Critical infrastructure sectors must ensure they are equipped to manage cyber security risks, thus protecting against social and economic disruption. The Conference called on senior executives to recognise the significance of cyber risk and to ensure they have robust cyber security measures and risk management in place. Governments and businesses that operate in the critical sectors are encouraged to develop a collective approach to the protection of critical infrastructure.

22. Computer Security Incident Response Teams (CSIRTs) have evolved from academic, private and public response teams into key players in national and international information exchanges for incident prevention, response and mitigation. Their capacity to provide early warnings of cyber threats, to coordinate responses to incidents and share expert knowledge is vital. CSIRTs worldwide have different levels of maturity. Improving the maturity of CSIRTs can boost cyber resilience and the response to cyber threats, and encourage information sharing to prevent the same threats from affecting large numbers of users. Delegates stressed the importance of strengthening global cooperation and capacity building to help emerging and existing CSIRTs enhance their capabilities.

23. Society's increased dependency on ICTs increases the potential impact of ICT vulnerabilities, such as security breaches, denial of service and loss of data. These vulnerabilities should be dealt with effectively. Increased attention for Coordinated Vulnerability Disclosure (CVD) and close cooperation with the ICT community, including ethical hackers, has resulted in many vulnerabilities being reported and mitigated. This shows that the multistakeholder approach works. Best practices, including possible ways to set up a national framework for CVD, will be shared through the GFCE.

24. Voluntary, consensus-based open standards are important to protect and improve the security and resilience of the global internet infrastructure. DNSSEC for securing the Internet Domain Name System, IETF Best Current Practice (BCP) 194 for routing security and BCP38/BCP84 for preventing Denial of Service attacks are some examples of these security solutions. The Conference underlined that the effective implementation of these solutions at international level requires collective action from all the relevant parties, public and private.

Cyber crime

25. In order to deny criminals a safe haven in cyberspace, it is important that all stakeholders work together. States, businesses and other non-governmental actors should all take measures to make it harder for criminals to commit illegal acts, both in their own countries and beyond their national borders, while preserving rights to privacy in accordance with international law. Up-to-date legislation is a primary requirement. Moreover, cooperation between government agencies and businesses is necessary to effectively counter online criminal threats and ensure the rule of law in cyberspace.

26. For law enforcement agencies and judicial authorities, the international nature of the Internet raises issues regarding jurisdiction in cyberspace. Participants, noting the work of the Cybercrime Convention Committee of the Council of Europe, shared their views on fighting cyber crime and on

the cross-border gathering of digital evidence. Although these issues will not be resolved easily, they remain urgent. The Conference discussed the various approaches that have been taken to these issues and identified new approaches that will be taken forward in the ongoing international discussions.

27. International cooperation and timely operational assistance are essential for law enforcement agencies and judicial authorities. Participants were provided with examples of international cooperation in cyber crime investigations. They stressed the value of 24/7 points of contact, such as the G7 24/7 Network and its 70 members and the partly overlapping network based on article 35 of the Convention on Cybercrime for securing digital evidence. It was noted that international cooperation in law enforcement can be facilitated through regional cooperation mechanisms, regional law enforcement organisations and INTERPOL. Capacity building initiatives concerning the fight against cybercrime will help support these effective forms of cooperation.

28. At the Conference, Europol shared its experience in addressing operational challenges and finding new forms of international cooperation. Earlier in the same week, INTERPOL opened the INTERPOL Global Complex for Innovation in Singapore, which aims to be a global hub for cooperation against cyber crime. The Conference discussed a number of other practical ways in which international cyber crime cooperation can be enhanced, building on the outcomes of the Law Enforcement and Prosecutors event held earlier in the week. Specifically it was agreed that:

    a. Despite the well known challenges of achieving timely acces to transborder data, there were incremental improvements that could be made within the current framework. These would be pursued.

    b. Further work would be undertaken to build on the success of operational coordination platforms (such as the J-CAT in EC3), to increase the geographic spread of such platforms, and to make them more accessible to a range of (public sector and private sector) participants.

    c. Recognising the fundamental importance of global capacity building, and the major step forward achieved through the launch of the IGCI, the Law enforcement community would play a strong and active part in the GFCE and related capacity building initiatives.

    A full set of recommendations will be published in the coming weeks. There will be an opportunity to review the progress made on the recommendations at the next Global Conference on Cyberspace.

International peace and security

29. While a peaceful cyberspace provides us with many opportunities, the potential for malicious cyber activities by State and non-state actors to create instability and mistrust in international relations is increasing.

30. The Conference emphasised the need for international cooperation to reduce these risks, with a view to doctrinal developments in various countries. It reaffirmed the applicability of existing international law to State behaviour in cyberspace, as well as its commitment to exploring the development of voluntary, non-legally-binding norms for responsible State behaviour in cyberspace during peacetime, and to developing and implementing confidence building measures to increase stability and prevent the risk of conflict as a result of misperceptions and miscalculations arising from the malicious use of ICTs.

31. The Conference reaffirmed the important role of the United Nations in maintaining international peace and security in cyberspace. The Conference welcomed the significant contribution of the 2012-2013 UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE). Among the UN GGE's many important conclusions, the Conference welcomed especially the agreement that international law, and in particular the UN Charter, is applicable to State behaviour in cyberspace. The Conference emphasized its strong support for the ongoing work of the UN GGE. It noted that complementary initiatives might also contribute to maintaining peace and security in cyberspace.

32. The need was stressed to reach shared understandings on how the principle of State sovereignty applies to State activities in cyberspace, consistent with States' international obligations and the law of State responsibility.

33. The Conference stressed the need for broad and inclusive engagement to enhance the shared understanding of how international law applies to State activities in cyberspace, for instance what legitimate responses are available when breaches of international law occur.

34. The Conference suggested that the ability of States to settle their international disputes peacefully, in accordance with their obligations under the UN Charter, would benefit from developing shared understandings of what might constitute a threat or use of force in cyberspace for the purposes of article 2 (4) of the UN Charter.

35. There is a clear, shared interest in strengthening not only technical but also legal, diplomatic and policy capacity and the exchange of best practices in the field of international peace and security in the cyber domain. Regional initiatives, such as the ASEAN Regional Forum, the Organization for Security and Cooperation in Europe, the African Union and the Organization of American States, provide an inclusive and cooperative approach to achieving this objective. Delegates reaffirmed their commitment to supporting these efforts and to increasing the coordination, cross-fertilisation and coherence of the various activities already taking place.

36. It was noted that existing regional processes should be expanded by increasing the number of states actively taking part in developing measures to promote peace and security in cyberspace. Mechanisms focusing on increasing transparency can be enhanced by including cooperative elements or by considering the development of stability measures.

37. A number of possible measures concerning responsible State behaviour relating to the protection of national critical infrastructures, the associated information systems, and critical components of the global Internet, both physical and logical, were discussed at the Conference, and could be taken forward in relevant processes of norm development:

    a. The Conference welcomed the debate on establishing normative protection for certain systems, including critical infrastructure providing essential civilian services, civilian incident response structures and certain critical components of the global Internet, both physical and logical. The Conference encouraged States to further explore how this might be taken forward most effectively.

    b. States should cooperate with and assist other States, in a manner consistent with their international obligations and domestic law, to defend against malicious cyber behaviour and protect the data of individuals and companies, especially those operating critical infrastructure.

c. States should support and enable the efforts of response mechanisms based in the wider technical cyber security community, not hinder them. In particular, States should not conduct or knowingly support any activities intended to prevent civilian CSIRTs from responding to cyber incidents.

d. States should have in place the relevant mechanisms – technical, policy-oriented, diplomatic and legislative – to increase their awareness of malicious cyber activities emanating from their territory.

e. States should consider how to mutually assist each other and exchange information, in a manner consistent with existing international obligations, with a view to preventing and countering the malicious use of cyberspace by non-state actors.

38. States were encouraged to be transparent about the roles and responsibilities of their defence forces and security services in the cyber domain. They were further encouraged to pursue dialogue and other measures related to cyber issues among their defence forces and security services to build confidence and ensure international stability.

39. Businesses, academia, the technical community and other civil society organisations can make an important contribution to enhancing ongoing processes for international peace and security in cyberspace. States should take into account the interests these actors have in international peace and security and include them in their respective roles.

Freedom and privacy

40. The Conference emphasised that our commitment to the protection of human rights must be unequivocal and that the protection of human rights and security online are complementary concepts. We must remain vigilant about those who use the Internet for incitement to (imminent) violence, and for the recruitment for or financing of terrorism, and ensure that such violations are countered within the framework of the rule of law without allowing ourselves to be governed by a climate of fear. We must also take full account of the need to protect the security and integrity of people, as well as their personal information, networks and devices, in ways that are fully compliant with international law, including human rights law.

41. The Conference recognised that international human rights law, as set forth in the International Covenant on Civil and Political Rights, provides a robust and universal framework for the promotion and protection of the right to privacy in international, regional and national frameworks. It was acknowledged, however, that we face increasing challenges to these rights in our modern societies. There is a need to improve the protection of the rights to privacy, freedom of expression and other relevant human rights, through appropriate national legislation, strong safeguards and effective oversight, consistent with international human rights law. It was emphasised in this regard that we need to ensure that the collection and analysis of information by government institutions and private companies is not arbitrary or unlawful.

42. The Conference affirmed that in the same way as people have a right to privacy offline, they have a right to privacy online. It further recognised that the individual’s right to privacy is important for the realisation of other human rights, including the freedom of expression and opinion and the freedom of assembly and association. Human rights and fundamental freedoms are the foundations of democratic, innovative and progressive societies and support economic and social development.

43. As an addition to this debate, the Conference welcomed the statement of the Global Commission on Internet Governance (GCIG). The statement calls on the global community to build a new social compact among citizens and their elected representatives, the judiciary, law enforcement and intelligence agencies, business, civil society and the Internet technical community, with the goal of restoring trust and enhancing confidence in the Internet. The Commission's recommendations can form the basis for further debate on protecting privacy and improving security in the digital age.

44. The Conference facilitated a constructive and forward-looking debate on these issues with all stakeholders, addressing their roles and responsibilities through policy recommendations. The objective of bringing together these experts and stakeholders is to build a future where security and freedom are protected; where citizens can retain control over their data, including private communications; and where we can safeguard a free and open Internet that generates economic growth and encourages social development. To this end, the Conference called upon stakeholders to take this debate further by drawing upon the policy recommendations made at the Conference. Encouragement was also given for the theme 'Freedom and Privacy' to be included in future editions of the Global Conference on Cyberspace.

45. The Conference also welcomed the ongoing debate within the United Nations on the right to privacy and looks forward to the important contribution of the newly-appointed Special Rapporteur.

46. The Conference noted that more data is collected and processed, and more and more decisions are taken by automated systems, which may have significant consequences for our human rights, in particular freedom of expression and privacy, and could also impact on anti-discrimination measures. It stressed the importance of raising awareness of the ethical dimension of such decisions and of further research in this field, and emphasised the need for greater transparency and the development of best practices in the public and private sector.

47. The Conference discussed international strategies to mitigate the potential risks associated with uncontrolled exports of ICT products that could be used in a manner that leads to human rights violations. It concluded that a flexible, effective and comprehensive solution could be found through a balanced approach, which might include a list-based regime, end-user controls and vendor due diligence (as required, for example, by the OECD Guidelines for Multinational Enterprises and the UN Guiding Principles on Business and Human Rights). The Netherlands committed itself to developing this approach in relevant fora and encouraged all relevant stakeholders to join this initiative.

Capacity building

48. To fully reap the benefits of information and communication technology, further investments are needed to ensure a free, open and secure cyberspace. Consequently, greater, more inclusive collaboration in the area of capacity building and the exchange of expertise on cyberspace is rapidly becoming one of the most important topics on the international cyber agenda, as was also noted in the 2013 Seoul Framework for and Commitment to Open and Secure Cyberspace.

49. The importance of capacity building in an interconnected cyberspace was highlighted as an overarching priority by governments, businesses, academia, the technical community and NGOs throughout the Conference. As was pointed out in the different sessions, building a truly resilient cyber domain requires international cooperation and better ways of working together. And while countries or regions face their own cyber challenges, we all benefit from sharing our experiences

and capacity building strategies. This Conference series gives us a major opportunity for global engagement in this endeavour.

50. Now is the time to put principles into practice and to address needs with solutions. The Conference welcomed the launch of the Global Forum on Cyber Expertise (GFCE) as a concrete effort to strengthen cyber capacity and expertise and to support and complement the existing international cooperative efforts in this field.

51. This capacity building forum aims to share knowledge and expertise, to take stock of ongoing efforts worldwide and to build international partnerships between countries, intergovernmental organisations and businesses, closely involving civil society, the technical community, think tanks and academia in the process. Nine joint initiatives were presented at the official launch of the GFCE on 16 April 2015. Other interested parties are invited and warmly welcomed to become active members of the GFCE.

Closing

52. In the coming year, debates on various aspects of cyberspace will continue in various fora. We hope that the work done and ideas generated by the Global Conference on Cyberspace, based on the vision of a free, open and secure Internet for the benefit of all, will resonate in future discussions.

53. The Global Conference on Cyberspace provides a unique multistakeholder platform for discussion at a strategic level of issues relevant to the cyber domain. We greatly welcome the fact that Mexico has expressed its willingness to host the fifth Global Conference on Cyberspace in 2016 or 2017.

54. ICTs and the Internet have become a key strategic aspect of our societies, and our societies have become increasingly dependent upon them. ICTs affects us all on a daily basis and has the potential to transform people's lives for the better. Yet we struggle with the complexities of finding mutually acceptable ways of cooperating globally to deal effectively with the implications. The Global Conference on Cyberspace has contributed to fostering this cooperation and to moving the debate further in several areas. We look forward to continuing our work together following this Conference.