

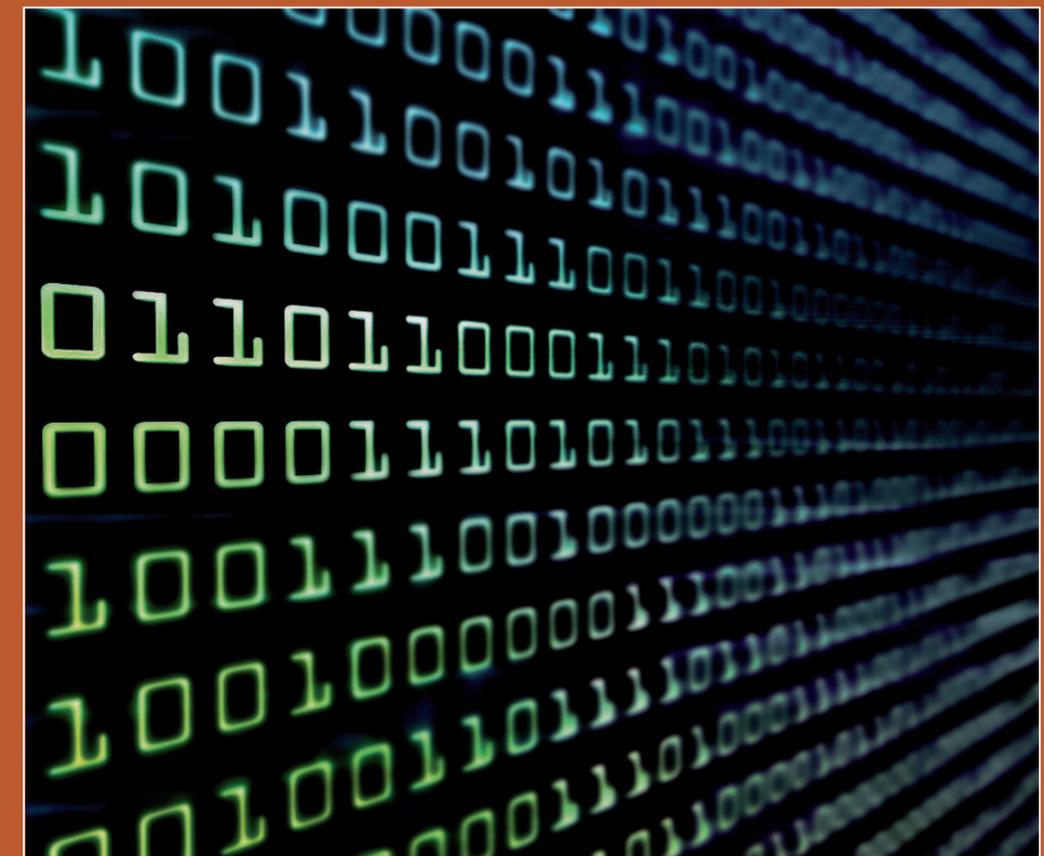


Conference Report

Institute for Peace Research and Security Policy
at the University of Hamburg

Challenges in Cybersecurity

Risks, Strategies, and Confidence-Building



© Flávo Takemoto - www.takemoto.com.br



© Auswärtiges Amt

Conference organizing Institutions:



Institute for Peace Research and Security Policy
at the University of Hamburg
Beim Schlump 83 · D-20144 Hamburg
Tel: +49 40 866077-0 · Fax: +49 40 8663615
e-mail: ifsh@ifsh.de
www.ifsh.de

13 and 14 December 2011
Conference Venue:
Federal Foreign Office in Berlin

Conference Report
Institute for Peace Research and Security Policy
at the University of Hamburg

Challenges in Cybersecurity

**Risks, Strategies, and Confidence-Building
International Conference**

13 and 14 December 2011
Conference Venue
Federal Foreign Office in Berlin

NOTE

This report represents a summary of the conference. The conference was held under the Chatham House Rule. Views expressed at this conference are the sole responsibility of the individuals concerned. They do not necessarily reflect the views or opinions of the organizing bodies, their staff members or sponsors, the Rapporteurs or the individuals' respective organizations or governments.

CONTENTS

Foreword	5
Acknowledgements	5
Conference Overview	7
Background	8
Opening Sessions: German Cyber Policy	
Werner Hoyer	9
Cornelia Rogall-Grothe	10
Introductory Talks: National Perspectives	10
Short Panel Summaries	12
Track 1.1	
Cybersecurity and Society	12
Track 1.2	
Cybersecurity Dilemmas	13
Track 1.3	
Introducing Transparency and Confidence-building	13
Track 2.1	
Understanding Computer Network Activities	17
Track 2.2	
High-End Hacking	18
Track 2.3	
Regulating Cybersecurity	19
Conference Result: Food for Thought	21
Abbreviations	22
Conference documents	
1 Speech by Werner Hoyer, Minister of State at the Federal Foreign Office	23
2 Speech by Cornelia Rogall-Grothe, State Secretary, Federal Ministry of the Interior	28

FOREWORD

The idea of a major conference on cybersecurity was initially proposed by the Freie Universität (FU) Berlin and the Policy Planning Staff at the German Federal Foreign Office. At the same time, the United Nations Institute for Disarmament Research (UNIDIR) and the Institute for Peace Research and Security Policy at the University of Hamburg (IFSH) were also planning to hold an international workshop as part of their project on “Legal Frameworks and Constraints and Perspectives for Transparency and Confidence Building”. The conference “Challenges in Cybersecurity – Risks, Strategies, and Confidence-Building” was made possible by merging these two projects. Both projects were sponsored by the German Federal Foreign Office which agreed to host this ambitious event at its conference facilities in Berlin.

A Scientific Board drawn from the four institutions – consisting of Sandro Gaycken, Theresa Hitchens, Heike Krieger, and Götz Neuneck – was established to plan the two-day conference. We are grateful to the speakers and delegations from the United States, Russia, China, and the European Union for their presentations. The broad participation and lively discussions underline the necessity of further national and international debates.

The conference consisted of six parallel tracks on specific issues related to the overall topic of cybersecurity: the nexus of “Cybersecurity and Society” (Track 1.1) was illuminated, focusing on the German legal and cultural situation; the most crucial “Cybersecurity Dilemmas” (Track 1.2), such as the problems of complexity and attribution and economic and regulatory dilemmas, were covered; an attempt was made to identify a basis for international consensus and “Introducing Transparency and Confidence-building” (Track 1.3); the strategic military interest in “Computer Network Activities” (Track 2.1) was investigated by senior representatives of western and eastern militaries; in the track on “High-End Hacking” (Track 2.2), technical details and tactics of sophisticated cyberattacks were discussed and the inefficiency of IT-security products in the light of such attacks was assessed; and finally, “Regulating Cybersecurity” (Track 2.3) debated the problems of attribution and assessing the applicability of international law in cyberspace.

The design of these six tracks proved to be of particular benefit to the conference. They were conceptualized using a content-focused approach. This approach helped to first identify topics of high scientific and political relevance in the cybersecurity debate. Potential contributors were then assigned by fittingness of their background. Each contributor was committed to a very specific topic and given additional notes on the ground they should cover.

ACKNOWLEDGEMENTS

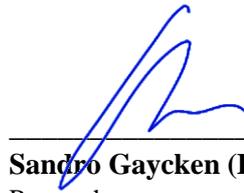
The remarkable success of the conference resulted from its unique genesis and the fruitful collaboration of the four institutions with the Federal Foreign Office. Different ideas, concepts and plans were brought together as best suited to international cybersecurity, a multi-stakeholder challenge. UNIDIR and the IFSH are grateful to have been able to join efforts with the Freie Universität Berlin and the Federal Foreign Office in preparing and implementing the ambitious conference concept. Particular thanks go to Jürgen Schnappertz of the Federal Foreign Office’s Policy Planning Staff, the Office’s Deputy Political Director Herbert Salber, and Detlev Wolter of the Office’s Conventional Arms Control and CSBM division. We are also thankful to the conference team, especially to Jürgen Scheller, Susanne Rack, Jörg Barandat,

Andrea Wagner, Kerstin Pertermann, Tobias Hosenfeld, Christine Schulz, and Regina Craja for their organizational help and personal commitment. The smooth running of the conference would have been impossible without the on-site support provided by students from the FU Berlin and trainee diplomats from the Foreign Affairs Academy.

This report was written largely by Kerstin Pertermann based on summary reports provided by rapporteurs in the various workshops. The conclusion was contributed by Götz Neuneck. We are especially grateful for substantive feedback and input by Ben Baseley-Walker (UNIDIR), Michael Brzoska (IFSH), Oliver Meier (IFSH), and Graeme Currie (IFSH).



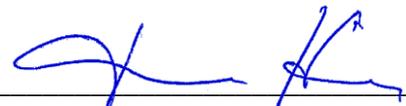
Martin Fleischer (FFO)
Head of International Cyber Policy Coordination Staff



Sandro Gaycken (FU Berlin)
Researcher



Götz Neuneck (IFSH)
Deputy Director and Head of IFAR²



Theresa Hitchens (UNIDIR)
Director

CONFERENCE OVERVIEW

“Challenges in Cybersecurity – Risks, Strategies, and Confidence-Building” took place on December 13 and 14, 2011, at the Federal Foreign Office, Berlin, Germany. The conference focused on addressing the challenges and issues revolving around the emerging domain of cybersecurity. It brought together key stakeholders and decision-makers from civil society, industry, multiple academic disciplines, and governments. They took part in an in-depth assessment and discussion of fundamental problems, evolving issues, future national or international regulatory regimes, and technical and non-technical approaches to cybersecurity. Exploring options for confidence- and transparency-building measures in cyberspace was a key goal.

In particular, the two-day meeting aimed to:

- (1) develop joint approaches to keep the internet as an unrestricted global commons and a forum for free speech and commerce,
- (2) understand existing and planned strategies, measures and approaches to protect cyberspace,
- (3) identify emerging risks and vulnerabilities in the cybersphere, ranging from disruptions of critical infrastructures to economical and military espionage and sabotage and addressing technical and regulatory steps to measure and confront these risks,
- (4) explore the best ways to develop principles, norms and rules for appropriate and responsible state behavior in cyberspace, including existing and future international norms, laws, and measures to regulate state behavior in times of conflict,
- (5) examine the need to adapt international humanitarian law to deal specifically with cyberwarfare,
- (6) strengthen international efforts to keep cyberspace open and safe for all via enhanced transparency, confidence-building and security, including via the Organization for Security and Co-operation in Europe (OSCE), the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF) and the United Nations (UN).

These issues were addressed in six *Track* sessions. Following the *Opening Keynotes* and *Introductory Talks* by panelists, who gave details of the “cyberstrategies” of various governments, the meeting broke down into several “tracks”. On the first day, sessions dealt with questions regarding “Cybersecurity and Society”, “Cybersecurity Dilemmas”, and “Introducing Transparency and Confidence-building”. The second day of the event focused on “Computer Network Activities”, “High-End Hacking”, and “Regulating Cybersecurity”.

The conference closed with a session that brought together the track chairs, who summed up the results of the conference. All meetings except for the *Opening Session* were held under the Chatham House Rule.

Participants came from the United States, Russia, China, Canada, Australia, Mexico, Georgia, Japan, Korea, Bahrain, the Emirates, and various European countries, making this event a truly international forum for candid and productive multi-stakeholder discussions. Over 220 individuals took part in total. It was not the intention of the organizers that the conference would generate consensual recommendations.

BACKGROUND

As cyberattacks grow in number and sophistication, and states, as well as non-state actors such as private hackers and organized criminals, appear to be becoming involved, the threat is increasingly perceived as a problem in both a national and an international security context. Yet assessments of how real the threat is, where the danger lies, who is best suited to respond to it, and what kind of international measures and strategies are appropriate to protect information societies against malicious actors – in short, how best to safeguard the long-term stability and peaceful use of the internet – vary widely.

States are increasingly aware of the need to seriously address the daunting challenges of protecting their information networks – especially those related to national security and critical infrastructures – from any attacker. Recent developments have shown that there is more to this endeavor than answering technical questions, particularly since many technical problems do not necessarily seem to have solutions. The cybersecurity question needs to be placed within a larger framework of international cooperation, norms, and rules for appropriate and responsible state behavior that will ensure the peaceful use of cyberspace. To make such a framework possible, a variety of questions have to be addressed:

- The potential impact of the actions of newly emerging, sophisticated cyberattackers, state as well as non-state actors, their motivations, tactics, and procedures.
- The costs and benefits to national and international security of military doctrines incorporating offensive cyber operations have yet to be fully understood. Due to the nature of this type of technology, it is very difficult to attribute cyberattacks. Offensive uses of such technologies in the cyber domain could lead to geo-strategic instability and raise the risk of miscalculations in times of crisis. This in turn could lead to escalation and serious conflicts. It is important to understand current trends and developments regarding the potential of cyberattacks for conflict and war, and the possible effects on civilian infrastructure, economies, and human security.
- Open questions regarding the application of international laws and norms have to be addressed, as there is still no multilateral understanding about how to apply these to the cyber realm, or even about why doing so is important for the future. For example, how should national militaries apply the laws of armed conflict and humanitarian law to cyberwarfare in the lead up to or in actual times of armed conflict? How does one apply the principle of proportional response to “cyberwar”? What level of cyber disruption constitutes “unacceptable harm” to civilians? Even more fundamentally, what constitutes a *casus belli* in cyberspace with possible effects on other domains causing a conventional response?
- The question of what constraints can and should be put upon offensive cyber operations given their technical conditions and the current legal regimes needs to be further investigated. Is it possible to control various kinds of cyber operations and confine their impact? What are the strengths and weaknesses of major strategies to prevent the misuse of cyberspace? An effective response to the threat of cyberattacks will have to involve a variety of stakeholders. But what are the respective roles of non-state and transnational actors such as civil society and industry? What role can national governments play? How can global cybersecurity be strengthened through international norms of behavior,

transparency, and confidence-building measures* (CBMs)? What potential is there for international organizations such as the European Union (EU), the OSCE, the North Atlantic Treaty Organization (NATO), and the UN to contribute to cybersecurity regulation?

- The relative value of potential international regulatory regimes in preventing the hostile use of information technology needs to be determined. The lessons learned from other efforts to regulate other dual-use technologies and apply them to the special case of cyberwarfare need to be evaluated.

OPENING SESSIONS

After the representatives of the organizing institutions – the German Federal Foreign Office, the FU Berlin, UNIDIR, and the IFSH – welcomed the participants and thanked them for their attendance, the conference opened with speeches by two German officials, who outlined German views on cyber matters. *Introductory Talks* then highlighted various national perspectives on cybersecurity before the participants attended their chosen *Track* sessions. Herbert Salber, the Deputy Political Director of the Federal Foreign Office, chaired the *Opening Sessions* on the first day.

Werner Hoyer

Minister of State at the Federal Foreign Office, Germany

In the first *Opening Keynote*, Werner Hoyer stressed the importance of securing the availability, openness, and integrity of the internet through international cooperation at the level of the state, the private sector, and civil society. The Minister noted that the internet and IT infrastructures have brought a wealth of opportunities to the global community by facilitating trade and communication. He emphasized that, from the start, cyberspace has been a global, open network that has reinforced education, technological innovation, and the exchange of knowledge and ideas. Moreover, he argued that this space of freedom, personal development, and economic progress warrants protection. According to Mr. Hoyer, security and freedom are complementary – without freedom, security could become repressive, and without security, freedom would cease to thrive. Cooperation between international stakeholders is required to manage and preserve a secure and free cyberspace. Consequently, “cyber-diplomacy” – discussing and negotiating internationally accepted rules of behavior – is taking place in various international forums and regional organizations which accords with the complexity of the subject. However, Mr. Hoyer pointed out that the current focus should be on areas where the consensus for cooperating internationally is the strongest and hence could lead to politically binding rules of conduct. This could generate trust which is the basis for further steps in global cybersecurity. Transparency and CBMs, as seen in conventional arms control, may provide a useful platform for the development of measures specific to cyberspace. “Soft law” – political commitments that may help build trust in areas where the striving for global cooperation is strongest – could lead to a “cyber code of conduct” for states. This could lead to further international cybersecurity developments.

The Minister of State noted that Germany is strongly in favor of creating an obligation on states to ensure security in the cyber realm, and that this should be anchored in international

* During the conference, experts talked about confidence-building measures (CBMs), confidence- and security-building measures (CSBMs) as well as transparency- and confidence-building measures (TCBMs). In order to simplify matters, this report uses the term CBM exclusively.

humanitarian law (IHL). He emphasized that efforts are needed to reach a common understanding of how existing international norms can be applied to the cyber realm.

Cornelia Rogall-Grothe

State Secretary at the Federal Ministry of the Interior, Germany

Cornelia Rogall-Grothe gave the second *Opening Keynote* of the conference entitled “International Cooperation in Developing Norms of State Behaviour for Cyberspace”. Because the internet and IT infrastructures cross borders and national legal systems alike, she argued, almost every state has a vital interest in ensuring their resilience, security, and stability for economic reasons as well as for the security of the public. Ms. Rogall-Grothe therefore stressed that it is not only necessary for individual states to protect cyberspace on their own territory but to also cooperate internationally to eliminate vulnerabilities in the cybersphere. Focusing on views shared in common by the international community of states would help to overcome differences and could lead to the cooperative development of an international code of conduct in cyberspace. She emphasized that a first step for this soft law codex would be to agree on which of the existing internationally recognized principles and norms could also be applied to the cyber domain. Once agreed, general principles for cyberspace, such as peaceful use, an obligation to secure critical infrastructures, cooperation among states in attributing cyberattacks could then be implemented. CBMs that would reduce the risk of cyberattacks could be developed on the basis of these principles. However, states should be responsible for preventing cyberattacks originating from their territory; otherwise they should expect a reasonable response, such as sanctions.

INTRODUCTORY TALKS: NATIONAL PERSPECTIVES

The United States attaches importance to building a shared international consensus on norms of conduct in cyberspace. According to the *International Strategy for Cyberspace*, which was drawn up by the United States, shared understandings and norms should focus on the physical and cyber worlds alike. These should include fundamental online and offline freedoms, property rights, public privacy, protection against cybercrime, a right of self-defense, technical stability, reliable access, and national resilience. It was argued that the Group of Eight (G8), the OSCE, and the Organisation for Economic Co-operation and Development (OECD) are appropriate forums for articulating these norms. In the US view, military CBMs should be based on the principles of proportionality and distinction, while other CBMs should aim to prevent escalation. The need for a more global conversation, which began at the London conference in November 2011, was emphasized. After all, cyberspace is inseparable and integral to the daily life of citizens, industry, and states. The internet impacts upon so many aspects of life – social, economic, etc. – it is not possible to treat the individual domains separately. The panelist concluded that the international community should act as a “steward” of cyberspace and enhance its openness through security as this domain grows in importance.

The second *Introductory Talk* of the day focused on **Russian initiatives for international cybersecurity**. These are based on the assumption that the main threats to information security are found in cybercrime, cyber-terrorism, and the military use of cyberspace as a tool for aggressive purposes. However, it was also argued that the dominance of the internet by a group of states was leading to a “digital disparity” and information technology (IT) monopolies. The

speaker stressed both that the global information network is a new domain of political confrontation and that the global community was ready to combat information security threats. The point was made that every actor – cyber-terrorists, criminals, militaries, as well as civil society and the private sector – is operating in the same environment, with the same tools, domains, and targets. Attention was drawn to the draft concept of a *UN Convention on International Information Security* presented by Russia in Yekaterinburg in September 2011. The key elements proposed include that each state is responsible for its own information space, including the state of its security and the data contained, that each state can manage cyberspace on its territory according to national laws and shall enforce fundamental freedoms and rights of individuals and citizens, that each state enjoys sovereign equality within the information realm, and that each state's security is inseparable from the security of the global community.

The first *Introductory Talk* on the second day of the conference gave an overview of **French security policy in cyberspace**. The talk began by pointing out that cyber threats have been addressed by both state and non-state actors in France for many years and that much work has been done, as cybersecurity is an area of priority for the French government. With the emergence of cyber-diplomacy, it was argued that the discussion – open to all stakeholders – has become global. Some elements of consensus for common action have started to emerge. International partnerships and bilateral relationships are thus engaged in ensuring security and helping to fight cybercrime. The European Union's concerted efforts to fight cybercrime, build solidarity and cyber-resilience, and establish policy co-operation with NATO were highlighted. The speaker argued that the OSCE focuses on confidence-building, while the UN Group of Governmental Experts (GGE) 2012 is committed to building an international consensus. A code of conduct is necessary to ensure freedom of expression and the reliability of the internet. The G8 *Deauville Declaration* of December 2011 agreed a number of principles on how to ensure the ongoing strength of the internet as a resource for global society: freedom, multi-stakeholder governance, respect for privacy and intellectual property, cybersecurity, and protection against cybercrime. A multi-stakeholder dialogue started at the London conference and shall continue in 2012 in Hungary after this conference in Berlin.

The **Chinese** government's perspective on information security was presented in the second *Introductory Talk*. The panelist pointed out that though cybersecurity is "fashionable", many countries are not prepared to defend themselves against cyberattacks. The speaker emphasized that the internet is a network of networks and it is thus arguably in no one's interest to use cyberspace as a battlefield, but rather to keep it as a peaceful, secure, equitable, and open space for information. In order to achieve this, concepts of common security and "favorable order" in cyberspace and information space have to be developed in an atmosphere of mutual trust and understanding. The speaker proposed that the leading role of state governments be assured as well as the establishment of "win-win cooperation" among the international community of states, so that each state can realize information and cyber prosperity. China does not see itself as one of the "cyber-powers" but rather as a major information and communication technology (ICT) user, who is facing severe challenges in cyberspace. It was pointed out that China is committed to strengthening information and cybersecurity from new angles, taking an active role in international co-operation with the aim of reaching international consensus, and to developing international norms and rules for the cyber domain. A letter with the outline of a proposal for an *International Code of Conduct for Information Security* was submitted at the United Nations General Assembly (UNGA) in September 2011. It was intended to provide a basis for the process of finding international answers to cybersecurity problems and is thus an invitation for international discussion.

The efforts of the **European Union** (EU) regarding cybersecurity were at the core of the final *Introductory Talk*. The panelist explained that an information-sharing platform for member states has been in existence since 2009. Pan-European cybersecurity exercises and functional Community Emergency Response Teams (CERTs) are to be established in all EU member states by 2012 to protect Europe from large scale cyberattacks. It was stressed that cybersecurity is an integral part of the Common Foreign Security Policy for the European Union (EU CFSP). The panelist argued that cybersecurity has a political dimension as well as relevance for defense and that the next steps of the European External Action Service (EEAS) will focus on the development of norms and standards for cyberspace, the promotion of the “Budapest Convention on Cybercrime”, capacity building in third states, development of a European strategy for cyberspace, and the organization of joint workshops with India, China and NATO.

SHORT PANEL SUMMARIES

Unless explicitly stated, the summaries are a collection of statements articulated by the panelists and do not represent an official agreement of the opinion of the whole group. The statements were intended as a basis for further discussion and the summaries are thus neither exhaustive nor complete.

TRACK 1.1

CYBERSECURITY AND SOCIETY

The first session focused on societal factors influencing the perception as well as the development of security in the cyber realm. The panelists gave an overview of the historical development of this sector, while discussing topics such as data protection, the security of IT infrastructures, the use of the web as a free commons, and the German cybersecurity strategy.

It was explained that data protection is highly advanced and sensitive in Germany and will have to be fully acknowledged in any German or European steps on cybersecurity. The importance of understanding the basic regulatory paradigms was stressed. An expert highlighted some of the most important approaches within German data protection and suggested some points for future collaboration. Equally important is an understanding of German digital culture and its views on the web as a free commons, as many international approaches will be influenced by the consequences of cybersecurity questions and as “Netzpolitik”, the politics of the internet, has grown to be an important item in Germany.

An expert argued that the security of critical infrastructures requires new defense measures. Agility, trust, cooperation and partnerships are necessary. Though it was emphasized that technology requires the freedom to develop, this should take place in an environment where business processes and security frameworks are adhered to. The value of general education in internet security and the adoption of safe practices were stressed.

Germany’s cybersecurity strategy, a panelist explained, distinguishes between two concepts – the internet as a public good and the internet as a public space – leading to different lines of action. The internet as a public good requires *cyberspace security*, meaning resilience of IT infrastructure, integrity, and availability of systems and data; whereas the internet as a public space requires *security in cyberspace*, which includes secure action in the cyber realm, authenticity, integrity, confidentiality of data and networks, legal security and legal obligation, security against crime and malicious activities. The expert outlined the goals and tasks of the

new-founded German Cyber Security Council – a cooperation between government bodies and industry – which include the coordination of cybersecurity policy stances, the identification and correction of structural trouble spots, discussion of cybersecurity issues, new technologies, transparency, collaboration, and recommendations to the Cyber Response Center. According to the speaker, concrete steps on the agenda entail enhancing and extending cooperation on critical infrastructure protection, creating more PC security by increasing provider responsibility, intensifying cooperation, both nationally and abroad, and establishing norms of state behavior in cyberspace in international forums (G8 and UN).

TRACK 1.2

CYBERSECURITY DILEMMAS

The second *Track* on the first day dealt with systemic challenges in the domain of cybersecurity and how best to meet them.

The first expert argued that the professionalization of attackers has made cybersecurity the key challenge of the 21st century. In order to control these risks and international threats, it was argued that governments, industry, and citizens will have to cooperate in a joint effort, while roles and responsibilities need to be divided. The existing European, international and national frameworks regarding cooperation could be linked, while international efforts, a speaker proposed, should be in line with national competencies, and further cybersecurity dilemmas, such as “individual privacy” versus “national security” should also be kept in mind. The need to understand the motives of attackers with strategic goals in order for cybersecurity to work was discussed. Other participants in this panel then pointed to some of the difficulties involved in this approach. The most pressing of all the regulatory questions in the cybersphere is the issue of attribution. One expert argued that attributing crimes to sophisticated attackers – the ones it is most important to combat – is not possible at present. There are systemic reasons for this, and no progress will be able to mitigate them. Another expert pointed out that systems are often said to fail because people who could protect them have no incentive to do so. This highlighted many of the economic problems associated with cybersecurity, which is a further true dilemma. There are no incentives for the industry to come up with robust cybersecurity, and what incentives there are often lead to poor cybersecurity solutions.

According to another panelist, information security could also be improved via policy means. Policy makers are argued that they should have a role in ensuring a consistent collection of relevant incident data. It was stressed that information disclosure could help to get a grip on the true extent of threats, while a “collaborative malware remediation program [...] deal with externalities of insecurity”. The same panelist also outlined the German approach to cybersecurity policy and stated that anything that can be done at national level should be done at national level.

TRACK 1.3

INTRODUCING TRANSPARENCY AND CONFIDENCE-BUILDING*

Session 1.3 dealt with the topic of identifying CBMs in cyberspace, outlining the current state of development, and how to move forward.

* A greater emphasis is being placed on the content of this session, as it was part of the UNIDIR-IFSH project.

The first speaker emphasized the potential for significant damage due to loss of control leading to escalation. The specific attributes of cyberspace already make it complicated to control, as states do not have monopolies and responsibility is hard to ascribe. This is expected to increase in the future, making traditional strategies ineffective. As a consequence, the measures taken by the US are based on thoughtful consideration and reflection on mutually reinforcing strategies instead of a single set of actions. The panelist stressed that further international dialogue is essential, while IHL and the sections of the United Nations Charter dealing with self-defense should also apply, as in some cases attacks could be seen as armed attack in the context of Article 51 of the UN Charter. According to the speaker, the UN Group of Governmental Experts (GGE) failed to confirm the IHL approach in 2009-10. It was also emphasized it is necessary to enhance transparency and predictability via the development of CBMs within the OSCE. The Code of Conduct (CoC) proposed by Russia and China is not considered by the United States to provide constructive guidance because it proposes justifying national control.

The second speaker talked about confidence- and security-building measures, *sui generis*, for the cyber domain. As potential “cyberweapons” are a feature of the post 9/11 international order, six categories for developing confidence- and security-building measures were identified: cybersecurity conferences; military CBMs such as exchanging information on cyberdoctrines, joint training, “hotlines”, law enforcement and economic measures, for example a Google anti-censorship function, network CBMs, and CERT protocols.

In the first discussion within Track 1.3, the Russian and Chinese draft CoC was criticized for focusing regulation of the internet in a national rather than an international context, promoting state control and emphasizing the predominance of state sovereignty over freedom of expression. It was also discussed whether a combination of CBMs and a restraint from offensive weapons is still possible. Furthermore, the participants debated whether more incentives for companies to protect their own critical infrastructures and networks are required. Certain standards of security were argued to be imposed in the US already.

The third talk focused on the importance of transparency and CBMs for international cybersecurity. The expert emphasized the need to engage states in developing legitimate state behavior, declaratory policy and in operationalizing cooperative cybersecurity. “Cybersecurity diplomacy” should be innovative as well as inclusive, seeking international cooperation to fight cyber threats by developing agreements on what constitutes responsible cyber activity by states. This process, the speaker stated, should start sooner rather than later, and must try to reconcile the differing existing concepts of what legitimate state behavior could be: some focus on the importance of the idea of the “global commons” remaining free from cyberattacks, whereas others view the cybersphere as another domain for warfare. The US *International Strategy for Cyberspace* calls, on the one hand, for building “collective security across the international community” (p. 13), while also emphasizing the right to use all means necessary to combat hostile acts, including unilateral measures. Talks have already begun: the expert recollected that cybersecurity was already prominent on the G8 agenda and should soon also appear on the agenda of the Group of Twenty (G20) – placing cyberspace challenges within accepted international structures. However, the speaker fears that this process is not being carried out fast enough as offensive state acts could compromise any efforts preventing or restricting global cyberattacks.

The expert noted that the employment of cyberattacks had been discussed by the Obama Administration during the crisis in Libya in 2011. Nonetheless, the US did not intend to set an “example” that other states might follow. Speeding up the process of developing accepted international legal regimes and norms describing responsible state action in the cyber domain is

therefore urgent if this gap in policy is to be addressed. The expert underlined this urgency by referring to the past: history has shown that once weapons are developed, preventing their use becomes difficult and, following this logic, the cyber threat will increase immeasurably in time if discussions are not undertaken now. However, the process of reaching consensus among states requires multilateral cooperation at the regional and global level, including civil society and the nongovernmental sector.

The UN Group of Governmental Experts (GGE) produced a report in 2009-10 encouraging states to develop CBMs. The speaker hopes that the new 2012-13 GGE report, which is to be presented to the General Assembly session starting in 2013, will provide a foundation for subsequent joint measures. Moreover, states are starting to articulate proposals for action in this area.

The proposed *International Code of Conduct for Information Security*, presented by Russia and China, focuses – according to the panelist – on confidence-building by offering a politically binding CoC rather than a treaty, which is based on verification provisions with challenging ratification processes. This CoC, which was submitted to the UN General Assembly in October 2011, constituted an invitation to engage in further discussions.

Transparency and CBMs were stressed as a means of response to the risks of misperception and escalation, which are increased by the characteristic attributes of cyberspace – such as its intrinsic dynamism and anonymity. They also contribute to the development of common norms of responsible state behavior. Measures could be drawn from conventional arms control, providing a basis for multilateral methods and potentially leading to the development of a “Code of Conduct”. Transparency and CBMs could therefore create the foundation of trust amongst the state community that is necessary if states are to enter into legally binding agreements.

The fourth speaker discussed state rights and responsibilities in cyberspace. It was argued that they can be realized in both the political and the legal domains, with states already starting to address state responsibility politically. These understandings of political and legal responsibilities of states could “help establish international law”. Just as a series of individual declarations by a sufficient number of states could over time – in addition to the broad principles articulated in the existing declaration of cooperative actions in the cybersphere – provide a more solid cooperation than any cybersecurity treaty could. The role of law, as pointed out by the panelist, could therefore focus on the weaknesses in these declarations instead. However, the speaker argued that the need for CBMs is greater than ever, and states have a legal obligation as well as a political responsibility to work faster towards creating them for cyberspace, as the process is currently very slow. The development of cybercrime cooperation mechanisms between the United States, China, and Russia was debated as a basis for building norms for responsible state behavior regarding the military aspects of the cyber domain. As developments in cyberspace have a harmful effect on “strategic nuclear stability”, it was concluded by the speaker that continuous dialogue at the international level should be opened immediately, while steps should also be taken to create CBMs relating to state accountability and responsibility in the cyber realm.

In the final presentation of this session, the speaker focused on state-sponsored cyberattacks and talked about multilateral approaches to cybersecurity requiring international rules and confidence-building. The current state of cyberspace security was described as defined by misperceptions and fears of escalation, and “preventive diplomacy”, which includes international transparency and CBMs, should be key to improving security. While the oft-feared “Digital Pearl Harbour” may be rather unlikely in the sense that a cyberattack could completely

shut down an entire army's ICT, it was pointed out that violations of individual property rights due to hacker attacks were taking place daily. The panelist noted that the fear of a first strike is comparatively high relative to the effect an attack could have on the adversary's military ICT. The biggest problem was argued to be the lack of attribution of cyberattacks. This could cause spiraling misperceptions, leading to conflict escalation in cyberspace or in general. Top priorities for Germany, the expert explained, are developing vigorous protective measures while also strengthening data and network safety and resilience. "Traditional security-policy instruments" were described as insufficient, as many cyber threats are asymmetrical compared to traditional threats, hence the current problem of attribution deems "deterrence through retaliation" to be infeasible. There is no "cyber-radar" that can pinpoint the exact computer from which an attack originated, or if that was possible, determine who actually sponsored the attack. As governments cannot easily be made liable for private "hackers" working individually, governments have so far been able to blame "patriotic" individuals for such attacks. As a result, it is necessary to hold a discussion on the obligation on states to take responsibility for cyberattacks launched from their territory and on the consequences that could follow if there was no attempt by a state to prevent an attack despite knowing of it in advance. It was argued that national and cooperative defense as well as international CBMs are required in approaching cybersecurity in a global manner. States should be responsible for establishing resilient defense and data-security measures to deter attackers by denying them access to the data they need to carry out attacks successfully – the speaker called this "prevention by denial". Another prevention method, described as "prevention by diplomacy", is a framework for "admissible state conduct", which should be defined by establishing international rules, norms, and principles while the risk of escalation should be diminished through transparency and CBMs. Giving due regard to the extent of worldwide online interdependency, the expert pointed out that measures need to be put in place at state level to reduce potential misperceptions that may lead to conflict. Complying with minimum security standards in cyberspace and adhering to an "all-threats attitude" could thus contribute to distinguishing genuine malicious attacks from events that are merely a result of negligence.

The speaker also proposed principles for norms of state action in the cybersphere that could lead to various concrete and complementary measures, including mechanisms for cooperation and CBMs. The problem with traditional arms-control instruments was identified as the lack of a definition of what "cyberweapons" are. Given how hard it is to uphold the traditional distinction between "civilian" and "military" in cyberspace, it was argued that basing the verification of the norms being applied and followed on this distinction would further complicate the implementation of conventional means of arms control. Current proposals for arms control in cyberspace are mostly elements of CBMs. For example: putting pressure on internet providers (IP) to disable botnets in the event of an attack, while states should – via an "obligation to assist" – ensure their compliance by threatening sanctions such as restricting online access in case of non-compliance.

The need to use the right forums in order to develop international norms of state behavior was discussed. At the regional level, it is hoped that the OSCE will develop CBMs and rules of behavior, while at the international level the United Nations should reach concrete, globally valid solutions addressing the issue of global cybersecurity to avoid the international destabilization of the cybersphere. According to the speaker, Germany has already advanced specific "CBM elements" based on work carried out by the GGE and the OSCE. They include transparency measures, risk reduction and stabilization measures, and support for cybersecurity capacity building in developing countries. Due to the nature and dynamics of the cybersphere, which involves multiple stakeholders – both private and public – it was argued that the attempt

to achieve international consensus in this process should initially focus on soft law. Seven general principles – put forward by the British Foreign Secretary William Hague in Munich in 2011 – to shape norms and responsible behavior in the cyber domain include: availability, confidentiality, competitiveness, integrity and authenticity of data and networks, privacy, and protection of intellectual property rights.

While cybersecurity requires a holistic and comprehensive approach that covers all the various dimensions of this complex issue – from economic and humanitarian aspects to cultural issues – it was deemed essential to start the process with the aspect where reaching consensus may be most likely in concrete CBMs. Regulating, restricting and, if necessary and appropriate, prohibiting hostile activities in cyberspace should consequently be the focus for CBMs. The other dimensions of cybersecurity also need to be included and addressed in the long term in order to retain and enhance the freedom-advancing effect of “cyber-media”. The expert concluded that states would have to press on to make real improvements in the OSCE and other forums such as the regional ARF if they want to lay a foundation that will enable genuine progress at the 2012 UN Cyber GGE.

In the *Comments* section of this session, it was argued that the UN is the only organization in a position to establish international legitimacy in cybersecurity.

The discussions in this session mostly dealt with the CoC proposed by Russia and China. One participant argued that the CoC was proposed to initiate discussions rather than as a real solution, adding that the internet should not be governed by the state but by the UN. There was also a strong demand for terminological clarifications, as the meanings of some of the terms used in the CoC are not defined, e.g. what constitutes “hostile activities”? The argument was put forward that an international CoC requires more dialogue, understanding, and support among the global community.

It was also argued that there is currently no forum that can unite security and civil society, and that existing approaches are top-down instead of bottom-up. Another proposal suggested including the private sector at UN level. How governments exchange best practices was another topic requiring further talks.

TRACK 2.1

UNDERSTANDING COMPUTER NETWORK ACTIVITIES

The first *Track* on the second day of the conference focused on responses and possible future strategies to deal with the security of computer network activities at national and regional levels.

One expert argued that while attribution is not the greatest challenge in the cybersphere, distinguishing between technical and political attribution is nonetheless required. It was explained that technical attribution is possible to some degree in terms of a potential to identify an attacking machine, but that being able to attribute this attack politically to an actor is another issue. However, given the potential gravity of cyberattacks, one speaker noted that some states would consider the possibility of retaliation without sufficient attribution.

Warfare in and around cyberspace can be linked to other types of warfare because of its transnational nature, according to one speaker. A key goal should therefore be to avoid escalation. The current discussion in the international community still focuses on the ambiguity of what constitutes an attack requiring the use of force as a response. It was argued that cyberattacks may be used to support conventional operations. The panelist stressed that the

focus should be shifted from reaction to resilience and prevention. The introduction of “cyberfingerprinting” could be an option.

The primary problem, according to one of the speakers, is not a possible military attack on critical infrastructure but political and economic espionage. The line between espionage and attack was argued to be very thin, and therefore determining whether one is already being attacked is difficult.

Another speaker explained that most US cyberweapons aim to prevent cyberwars. US Cybercommand is not supposed to work independently, but in support of other measures – it is firmly under civilian and political control.

The cooperation of government and the private sector was also stressed in this session by another speaker. The creation of trust achieves the free exchange of information and helps to share responsibility. The process of building trust must start small and sector-specific.

Methods discussed to achieve stability and predictability in cyberspace include transparency and CBMs, cooperation, norms, and sanctions for non-compliance. However, according to one expert, for security to improve internationally, every country has to improve its own security as well due to the interconnected nature of IT infrastructure. The more communication there is between states and stakeholders, the securer the world. Russia, for example, was said to be open for discussions with other states – bilaterally and multilaterally – especially in order to develop CBMs more rapidly.

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) in Estonia was deemed to be the “interface” between civilian and military entities by another panelist. For a greater degree of capability-testing and information-sharing, a higher level of trust would be needed, which has not been achieved so far. Items for information-sharing will have to be determined.

During the discussion in this session it was proposed that disruptive denial-of-service attacks might not pose a high risk after all, in contrast to their dramatic portrayal in the media.

It was also proposed that IHL should be proactive to keep up with technological developments, which are fast-paced, rather than stay reactive.

TRACK 2.2

HIGH-END HACKING

The second session of the second day focused on hacking activities undertaken by militaries and organized crime. It dealt with evolving trends in hacking, differentiating cyberwar and cybercrime, and requirements and options for successful cyber-defense.

One speaker argued that hacking is no longer focusing on malware, viruses, and bypassing firewalls, it is being carried out at all levels of computer systems, including hardware, and manufacturers are often unaware that their systems are compromised. Prevention should therefore start at the lowest level possible: the hardware. While even a massive cybercrime attack can be inexpensive, military cyberattacks are costly, according to the expert: while everyday criminal cyberattacks focus on open systems with identified problems, making use of already known tools on a mass-scale, i.e. attacking common platforms to reach a maximum of victims, military hacking and attacks are generally different. It was explained that military attacks focus on specific targets and systems, following concrete strategic goals – instead of simply seeking to break or shut down systems – while staying undetected for as long as

possible. Military “cyberweapons” are therefore single-use in nature and require various levels of effort and resources, which makes these attacks very costly compared to everyday cybercrime.

As also discussed in other sessions, the panelists argued that attributing cyberattacks is one of the biggest challenges of cybersecurity. Although this is complex, it is theoretically possible; however, it requires international cooperation.

It was emphasized that one of the key aspects of defending against, detecting, and countering military hacking is to know one’s own system better than any attacker and to keep developing and questioning its security constantly. The speaker added that a further defense mechanism is to enhance threat detection and diagnosis, which will reduce response time and thus minimize damage. The development of offensive defense mechanisms could also be an option, for example, having a team of experts gather intelligence on the attackers and analyze zero-day exploits. Many therefore argue that the ability to hack others is a requirement for successful defense. At the international level, one panelist also proposed that intelligence agencies and militaries should share vulnerabilities, knowledge of unknown attack mechanisms and zero-day exploits, while making use of trusted sources for attack and defense tools. Restricting the spread of malware, penalizing internet service providers (ISPs) for hosting malware, and making the software industry liable for their products were also proposed as options. In contrast to these new approaches to high-end cybersecurity, most products of the IT-security industry currently in place and marketed as advanced were considered to be of low or negligible value in the defense against sophisticated attackers. The IT-security industry was criticized for scaremongering about the wrong things and for selling a false sense of security instead of actual security.

TRACK 2.3 REGULATING CYBERSECURITY

The final *Track* examined the potential for international regulation in the cyber realm. While the need for international cooperation and public law regulating the response to challenges and attacks originating in cyberspace has not been questioned, it is, however, difficult to determine how existing law can be applied to the cyber realm. Among the key challenges – a panelist argued – is the lacuna in international law regarding cybersecurity or cyber activity, especially regarding the laws of armed conflict, since warfare is still pictured in conventional terms. So far few attacks have triggered state responses and the progress in defining what responses are legitimate is considered to be very slow, not least because of the attribution problem. A speaker argued that the present situation does not permit the exercise of Article 51 of the UN Charter, the right to self-defense, which requires several prerequisites to be met: the damage caused by an attack should be comparable to armed attacks, the identity of the attacker must be known, and a state needs to be attributed with the attack. The panelist also explained that the measures taken in response have to be proportional. As attribution – among other things – is not always currently possible, the expert concluded that Art. 51 is currently inapplicable. Regarding precautionary measures, international environmental law could be considered to be transferrable to the cybersphere, according to the next panelist, as “existing international law governs state activities wherever they are carried out, including in cyberspace.” Nonetheless, the expert pointed out, the unique and specific attributes of the cyber domain complicates the application of existing law, norms, and terminology. It was argued that some of the key challenges could be resolved by interpreting treaties using “common sense”, while others depend upon “unanimous

policy decisions” by the global state community. The panelist stressed, however, that neither the technological and military implications and potentials have yet been fully examined, nor has there been any broad dialogue internationally on how to interpret and apply existing international law to warfare in cyberspace. According to the expert, both cybercrime and cyberterrorism should be distinguished from cyberwarfare when IHL is concerned. The extent to which the principles and rules of *jus in bello* governing “traditional means and methods” apply to warfare in cyberspace therefore need to be determined. It has been proposed that *jus ad bellum* is difficult to apply unless attacks amount to a conventional armed attack, whereas *jus in bello* should be applied in the case of cyberattacks, as it is already used to deal with the attribution challenge in non-international armed conflict. The emergence of a treaty restricting cyber activities is still considered to be unlikely; however, an international code of conduct may become necessary, according to an expert. Customary international law may also lead to clarification of acceptable and non-acceptable behavior. Guidelines based on CBMs – for example, structured exchanges of national views on norms and national strategies, perceptions and best practices, developing technical recommendations for reliable and secure global IT infrastructures, accountability for combating terrorism using cyber mechanisms – will be required, according to one expert. Another issue raised was the current tendency for states to nationalize their internal network structures, and the modification of IT structures in the process of the emergence of a “Cyber Westphalia”, which it is argued will encompass the majority of nation states by 2020. It was observed that this move is a response to the current uncertainty in the cybersphere, with states attempting to give themselves time to respond when intrusions happen. Measures to compartmentalize networks are already beginning to be implemented, facilitating attribution and making the structure of the internet more resilient. This would be important, according to the speaker, when dealing with sophisticated actors, whose intrusions would require more disruptive responses.

For civil-system resilience – the panelist argued – a partnership between state and private actors is essential to enable collective defense. Coordinated reaction would reduce threats, while collaborative risk assessment could prove essential for public and private assurance efforts. Following the presentations by the chairs of the respective sessions, who gave a summary of the topics, ideas, and challenges discussed in each *Track*, the sessions on both conference days were closed by a plenary *Panel Discussion*.

The conference concluded with an additional panel discussion at which the representatives of the organizing institutions summarized the two days. The representatives thanked the participants for a fruitful conference with many lively discussions and expressed the hope that further dialogue will follow.

CONFERENCE RESULT: FOOD FOR THOUGHT

From the point of view of the IFSH, which co-organized the conference, the two days of intense presentations, discussions, and *Closing Panels* led to the following observations, which should guide the development of further research questions and policy responses:

1. The cybersphere is part of the daily life of many citizens, companies, and governments. Cyberspace entails not only ground-based assets and critical infrastructures, but also wireless communication and space-based platforms. Cyberspace is fast-growing and its technological, legal, industrial, political, and military implications have not been fully explored.
2. A larger framework, including international cooperation, is needed for the establishment of norms and rules for adequate, responsible state behavior to ensure and guarantee the peaceful use of the cybersphere.
3. There is a wide range of possible measures to prevent the large-scale build-up of offensive cyberattack capabilities and their military use, starting with confidence- and security-building measures in cyberspace and the development of a global code of conduct. However, definitions will need to be agreed in advance. One option for kickstarting this process would be for states to make unilateral declarations aimed at preventing large-scale harm to civilian critical infrastructures.
4. An international forum for discussion of cybersecurity issues has not yet been established, although the United Nations (and the OSCE) provides a good environment in which further consensus can be achieved. The upcoming GGE scheduled for 2012/13 can create a foundation for subsequent initiatives and measures at the UN.
5. The attribution of large-scale cyberattacks is not easy, but may be possible under some circumstances. If a catastrophic cyberattack were attributed, politically and military responses would likely follow. Threat detection and diagnostic forensics therefore can and must be improved.
6. More and more countries are establishing military and national security cybercommands. These states should make their cyberdoctrines public – explaining their offensive and defensive motives, measures, and resources. Organizations such as the OSCE could organize annual seminars to discuss capabilities and perceptions of national cyberstrategies as a further trust-building exercise.
7. Debates between governments in international forums should take into account new technological developments regarding the potential misuse of the cybersphere for conflict and war.
8. Individual states should be responsible for protecting cyberspace assets located on their territory. This requires them to cooperate to exchange technical and procedural information about the protection of ICT vulnerabilities, especially in times of crisis. Early warning, quick responses, and adequate stabilization measures are vital; less-developed countries should receive support.
9. IHL principles, such as proportionality and the distinction between combatants and civilians, can be applied to cyberattacks, but legal manuals and handbooks have to be adapted to new incident scenarios. Also, with regard to self-defense under Article 51 of the UN-Charter, it is necessary to clarify in legal terms precisely what might constitute an “armed attack” involving cybermeans.
10. Despite political and ideological differences, more multi-stakeholder conferences (such as the follow-up events to the London Cyber Conference) complemented by bilateral and multilateral consultations between governments and, most importantly, regional and international organizations are necessary in the years to come.

ABBREVIATIONS

ARF	ASEAN Regional Forum
ASEAN	Association of Southeast Asian Nations
CBM	confidence-building measure
CERT	Community Emergency Response Team
CoC	Code of Conduct
CSBM	confidence- and security-building measure
EEAS	European External Action Service
EU	European Union
EU CFSP	Common Foreign Security Policy of the European Union
FU Berlin	Freie Universität Berlin
GGE	Group of Governmental Experts
G8	Group of Eight
G20	Group of Twenty
IFSH	Institute for Peace Research and Security Policy at the University of Hamburg
IHL	international humanitarian law
ICT	information and communication technology
IP	internet provider
ISP	internet service provider
IT	information technology
NATO	North Atlantic Treaty Organization
NATO CCD COE	NATO Cooperative Cyber Defence Centre of Excellence
OECD	Organisation for Economic Co-operation and Development
OSCE	Organization for Security and Co-operation in Europe
TCBM	transparency- and confidence-building measure
UN	United Nations
UNGA	United Nations General Assembly
UNIDIR	United Nations Institute for Disarmament Research, Geneva

CONFERENCE DOCUMENTS

DOCUMENT 1

Opening Speech by Minister of State Dr. Werner Hoyer

Excellencies,
Ladies and gentlemen,
Distinguished guests,

I am delighted to have the privilege of welcoming you to the Federal Foreign Office. As the huge response this conference has attracted shows, the Internet is now a very important topic on the international agenda.

As a challenge for diplomacy, the Internet has many different aspects.

It has to do with human rights.

It has to do with international trade and economic policy.

It has to do with security policy, too – an aspect that's becoming increasingly important. On top of that, the Internet is an example of global governance as well. Obviously, global issues cannot be effectively addressed by any one country on its own.

Computer systems have become the nervous system of the modern world. They play an ever greater role in the business of government, in all our private lives and also in the functioning of our market economies – in logistics systems, power generation, the financial markets, you name it. And without Internet access it is hard to imagine how we could manage many aspects of daily life. In the world of the 21st century, protecting the Internet and its infrastructure is therefore a core task for governments, too.

We need to ask ourselves what governments, together with Internet providers, can and must do to guarantee security in cyberspace. This is important not only in the context of transnational cybercrime committed by individuals, but also in the context of dealings between governments.

However, we must not lose sight here of what it is that we want to protect. We need to protect the Internet as a new public space, a space of freedom, economic growth and personal development.

In an open and knowledge-based society, clearly, the Internet is just as essential for our freedom as it is for our prosperity. And it has become a synonym for the opportunities globalization offers. A connected world fosters education, innovation and a market place for new ideas. It boosts trade both inside countries and between countries. Last but not least, the Internet can galvanize economic progress in developing countries.

It can serve as a catalyst, moreover, for the development of free and open societies. It encourages a vibrant civil society. It can make government more transparent and government agencies more efficient. Broad access to the Internet spells greater equality of opportunity, also in contemporary industrial societies.

Democratic participation, access to education, personal contacts, business transactions, professional and above all personal development: the Internet is increasingly the platform where all these activities take place.

A free and global Internet helps foster international understanding and, by the same token, peace. Where free discussion is possible, contact with others around the world is easy, and everyone has access to the same content, people tend to understand other societies better. Everyone can find out for themselves what life in other countries is like. In the digital age governments cannot and must not any longer steer and control opinion.

A connected world accelerates not only the globalization of markets but also the globalization of values. People all over the world can use the Internet to help them exercise their right to freedom of expression.

Take North Africa, for example. The democratic revolution there did not happen because of some technology. It happened because the yearning for freedom triumphed. But the Internet – along with all the mobile phone services we have today – helped the democracy movement really take off. They made people no longer afraid to voice their views and demand their rights.

Cyberspace is a public space which must be preserved and managed. Since it has been a global space right from the start, this is a task requiring international cooperation: intergovernmental cooperation as well as cooperation with the private sector and civil society. That, as you all know, raises a host of issues, which are now under discussion in various international forums.

What rules and rights should there be in cyberspace: for users, for providers, in transnational communication, for access to the Internet? Where and by whom should such rules be laid down? What rules from the offline world must apply also in the online world? And how can they be implemented in a transnational context? What intergovernmental agreements relating to land, air, sea and outer space should we extend to the digital sphere?

Of course freedom in cyberspace would be seriously compromised without crime prevention or safeguards against unauthorized invasions of our privacy, be it by governments or by private individuals. Whether the issue is the individual's right to determine what happens to their personal data, the limits to privacy in a public space like the Internet or intellectual property rights, the principle of "delete rather than block" or crime prevention: of one thing there can be no doubt. Managing a global network requires international agreements.

We clearly can't allow the Internet to be outside the law, there have to be rules. So the rule of law must be upheld in cyberspace, too. But it must be done without unduly restricting the freedom of the Internet or the rapid pace of technological advance.

Where, then, is the need for rules and agreements most urgent?

What is important here, in Germany's view, is, firstly, respect for the right to access to information and for the right to freedom of expression. Secondly, we want to highlight the need for neutral access to the resource Internet, one that does not discriminate between states or Internet users. Thirdly, we view efforts to nationalize the Internet, as it were, by building a series of national networks as counterproductive.

In the 21st century world, free access to information as well as freedom of expression and of assembly are protected only if they exist also in cyberspace. US Secretary of State Hillary Clinton has called these Internet freedoms "the freedom to connect".

We therefore welcome all the work going forward at the Council of Europe, the UN Human Rights Council, the OSCE and other bodies with the aim of building consensus internationally on freedom of the media and freedom of expression.

In the context of bilateral discussions of human rights topics, too, we feel it is important to raise the issue of freedom of the media and the Internet.

Another priority is to prevent regimes which brutally oppress their own citizens, as we are seeing right now in Syria, from acquiring technology that could help them spy on, keep tabs on and harass people. This is why we have recently included such technologies in the EU's sanctions regime vis-à-vis Syria.

We also welcome the principles and agreements formulated by the G8 and OECD on Internet governance, the economic role of the Internet and its potential in promoting development as well as the discussions at the Internet Governance Forum, whose annual meetings bring together governments, business, users and civil society.

The many benefits generated by the Internet are due above all to the fact that it has been from the start a global, open, decentralized yet single network. That is why we should lobby internationally for the clock not to be put back. It cannot be in anyone's interest to develop a whole series of national walled-off networks.

In my remarks so far I have placed special emphasis on Internet freedom. This is because we in Germany feel the topic of our conference – "Challenges in Cybersecurity" – needs to be seen in

a wider context. Cybersecurity must be about protecting freedom in cyberspace, about protecting its openness, availability and integrity as a resource. In this sense freedom and security are inseparable twins. Freedom needs security to flourish; security needs freedom, otherwise it becomes an instrument of oppression.

Since cyberspace is by definition global, international action is needed to protect our international data networks. The rapid rise in cases of abuse of and attacks on data networks – particularly in the form of sophisticated computer worms such as Stuxnet – has driven home to us how dependent we are on international cooperation. Since we cannot protect ourselves completely from such attacks or discover who is behind them, we need something like cyber diplomacy. The primary aim of this kind of diplomacy is to negotiate internationally accepted safeguards, rules of conduct based on legal norms, and standards. Our national Cyber Security Strategy rightly speaks of the need to develop an “international cyber policy” – a whole new challenge for our foreign and security policy.

Four parameters will guide our efforts here:

1. Our approach is incremental and pragmatic. There is no point in looking for a silver bullet. What we want is to explore common ground with a group of like-minded stakeholders and make progress where we can.
2. Cyber diplomacy is already under way in a wide range of international forums and organizations. Given the complexity of the challenge, that is the right approach. We want to see a division of labor between the different forums; it is important to define as clearly as possible who does what.
3. We see maximum transparency and active confidence-building as the best way to guard against offensive – including military – uses of cyberspace.
4. We believe currently applicable international law provides by and large a sufficient basis for developing new norms in the area of cybersecurity. The important thing now is to bring different interpretations and standpoints more closely into line with a view to reaching a common consensus.

Let me now look at these four points in greater detail.

In recent years we have seen a major increase in international efforts to strengthen cybersecurity. The Council of Europe drew up its Convention on Cybercrime (2001) at a very early stage. It is regrettable that the Convention’s broad-based approach, which entails notably some necessary infringement of national sovereignty in connection with the collection of evidence and the tracking down of cybercrime suspects, has prevented many countries from signing up to it.

That is why it makes little sense – at least at the moment – to try to draw up comprehensive conventions and rule books. Here, too, grand strategies tend to be the enemies of progress. For this reason we argue for an incremental approach on the basis of soft law – in other words, politically binding rules of conduct that help to build trust.

That means we should focus on those areas where the desire for international cooperation is strongest. Apart from the fight against crime, I believe there is considerable international interest in agreeing measures to protect critical infrastructure, for example, give hospitals a special security status and enhance the security of submarine cables – which are amazingly few in number – and their network nodal points.

The more we strive in these and other fields to build trust and promote good governance, the more stakeholders will come to trust one another. That lays the groundwork for further advances in international cybersecurity.

Our incremental approach enables us, moreover, in ad hoc coalitions to reach agreements with other governments whose interests and positions we share. In line with our pragmatic approach, we believe some countries could also set an example by agreeing on standards and rules of conduct. Accordingly, the G8’s Deauville Declaration and the results of the London conference in this area could help promote consensus-building and intergovernmental agreements in the field of cybersecurity.

As we see it, regional organizations and forums concerned with security issues are going to play an increasingly important role here. Experience with transparency-building and confidence-building mechanisms in the area of conventional arms control is a good basis for attempts to develop similar measures for cyberspace. Germany has consistently supported the efforts of the OSCE to achieve tangible results in the area of confidence-building measures.

To this end we have put forward concrete proposals on, for example:

- early warning;
- transparency through information-sharing on cybersecurity policy and strategy;
- establishing national focal points;
- setting up dedicated communication channels for use in the event of a crisis;
- developing technical recommendations, and assistance with capacity-building.

We should not allow ourselves to be discouraged by the failure last week of the OSCE Ministerial Council to take any decision in this regard. It underlined once again how difficult it is for countries with different standpoints to agree on a common approach.

We commend what the OSCE is doing in this field and hope successful confidence-building under the auspices of regional organizations can be a model for similar endeavours at UN level.

Digitization has not only had a profound impact on the way military operations are conducted, how weapons are used and what military personnel actually experience on the ground. It also means that data networks used by the military are far more vulnerable now than they ever were in the past. In many of today's armed forces what began as efforts to protect their data networks from cyber attacks has now expanded into actual cyber commands with a remit to safeguard their country's capacity to conduct the full spectrum of military operations.

Nevertheless, I do not share the hysteria about a looming cyberwar fuelled by those such as journalists or security firms with a vested interest in boosting sales. In the foreseeable future we are unlikely to see anything of that kind.

However, we do need to confront the threats arising from the military use of cyberspace. That such use is, in the case of a number of countries, now an integral part of their national defence strategies reinforces the impression elsewhere that offensive capabilities are being developed in this area, from which other countries must protect themselves. This may set off a dangerous spiral, which along with martial rhetoric could fuel serious tensions and ultimately even lead to an outbreak of cyber hostilities.

The difficulty of identifying the source of any cyber attack obviously makes such scenarios even more dangerous. When there is no reliable way to identify the attacker or gauge the motives behind the attack, speculation, conjecture and suspicion have free rein. By means of subterfuge and deception, a really high-tech cyber attack can make an attack appear to come from a country that has nothing at all to do with it – which may then find itself the target of a reprisal attack.

Under such circumstances the doctrine of deterrence, which in the nuclear context has functioned well to date, is simply obsolete. We need to realize that here we have to do with a completely new type of asymmetry. Whether brilliant hackers, cyber mercenaries acting at others' behest or countries with weak data network infrastructure: all of them are capable of launching successful cyber attacks, without fear of reprisals, on countries with advanced data networks.

In the light of such risks as well as the danger of escalation I have outlined, there are three priorities the international community should focus on above all else.

- Firstly, we need to tone down the rhetoric.
- Secondly, we need transparency with regard to national defence strategies in the area of cyberspace.
- Thirdly, we need an internationally recognized rule book which lays down when and how the target country of a cyber attack may respond.

If we want to strengthen international cybersecurity, we cannot do this without bringing international law into play. In Germany's view the provisions of the UN Charter apply in principle also to cyber attacks. Humanitarian international law is by and large, we believe, all that is needed as a basis here. We are not looking for any new codifications in this area. As we see it, in the context of cyber attacks launched by private individuals, international law principles regarding state responsibility unfortunately do not currently entail any obligation on states to ensure cybersecurity. That is why Germany is in favor of creating a new obligation on states to ensure cybersecurity.

I am aware there are a number of contentious points regarding the interpretation, derivation and application of international law norms in the area of cyberwarfare and cybersecurity. Here, too, international efforts are needed to develop a common understanding of how such norms apply to the area of cybersecurity.

I am sure the conference that is starting today will make a valuable contribution, not only in the section devoted to international law, to clarifying the issues at stake and bringing positions on the points of contention more closely into line. Our conference has the advantage that – except for the opening session – it is being held under Chatham House Rules, so the high-calibre experts participating can discuss all these matters very candidly with representatives of industry and government. I hope this will help us make real headway in formulating what steps are needed to enhance international cybersecurity. What was just yesterday a niche topic is now one of the major new challenges which the international community needs to address.

On this note I wish all participants a stimulating and productive conference.

DOCUMENT 2

Opening Speech on “**International Cooperation in Developing Norms of State Behaviour for Cyberspace**” by *State Secretary Cornelia Rogall-Grothe*

Ladies and gentlemen,

Not all too long ago, cyber security and cyberspace still sounded like science fiction. At the CeBIT computer trade fair in 1995, Bill Gates himself described the Internet as "hype". Not long after, based on revised forecasts, Microsoft added its own Web navigation software to its Windows operating system.

The World Wide Web is only 20 years old, and today we live in a networked digital world, with an estimated 2 billion Internet users world-wide. This development has occurred at breathtaking pace compared to the spread of other media.

When I speak today of the digital world or cyberspace, I am referring to all IT systems networked at data level on a global scale, a space in which the Internet serves as a network of connection and transport. Infrastructures vital to our existence are connected with the Internet, which is where legitimate collective interests, not just individual interests, come into play across borders and legal systems.

Resilient infrastructures and a secure, available, intact and reliable Internet extending across national borders and legal systems make up the backbone of our globalized world. This is important in two respects:

1. for economic reasons
and
2. in the interest of public security
in almost every country!

Preventing threats, providing security and protecting public goods are among the traditional fundamental tasks of nation-states. Cyberspace and the Internet as a public space and public good, however, must be viewed in a global context. National efforts in cyberspace, for example to prevent threats, can only yield partial success.

By contrast, the international community can achieve a great deal when it is willing to work together.

Germany and many other states are becoming increasingly aware of the problem. We may use different terms, and the context may differ –

- information space vs. cyberspace
- information security vs. cyber security

– but we already appear to agree on a number of key points.

Despite major cultural, political and ideological differences in the different parts of the world, we can all certainly agree that major IT disruptions, especially as the result of cyber attacks, are a serious risk and a global threat. All countries and national economies are linked to each other via the Internet, and so all computer systems and IT-based infrastructures are in principle highly vulnerable, no matter where they are.

For example, imagine the following scenarios:

- disruptions to cross-border power grids,
- a botnet which uses millions of computers connected to the Internet to attack infrastructures of another state,
- or the publication of personal data taken from users of a popular social network.

These are all criminal and/or politically motivated hacker attacks for the purpose of world-wide sabotage, espionage, fraud, etc., where national borders are increasingly meaningless.

The facts are alarming: Last year, the number of cyber crime incidents in Germany rose by 19 per cent.

The Federal Police were also the victim of a known cyber attack this year.

Another problem is attribution: the source of crimes and attacks is often difficult and impossible to find, leading to the risk of misperception and improper responses, which may increase the risk of conflict.

This conference brings together decision-makers, experts in a variety of fields and industry representatives in a dialogue on current challenges and the possibilities offered by national and international rules, as well as technical and non-technical solutions.

The conference focuses on cyber security policy and international law, and on the question of who is responsible for cyber security in what form. Starting from my area of responsibility, I would like to take a closer look at the role of states and their cooperation in developing norms of state behavior in cyberspace.

I certainly see ways to improve the protection of cyberspace and make it less vulnerable, through national efforts and especially through international cooperation.

We can take advantage of the current interest in this topic. Based on very similar threat assessments, a number of states developed and published national cyber security strategies between 2009 and 2011. For example, Germany's strategy includes the following core items:

- greater protection for critical infrastructures and government IT systems against cyber attacks,
- protection of IT systems in Germany, including greater public awareness,
- the creation of a National Cyber Response Centre and a National Cyber Security Council, and –very important-
- international cooperation.

So Germany is just one of many states which have made international cooperation a strategic priority. Australia, Canada, the Czech Republic, France, Japan, the Netherlands, New Zealand, the UK and the US, for example, all assume a global threat to cyber security. Nine of these states explicitly describe international cooperation as a key measure.

In my view, the current situation impressively demonstrates the recognized need and demand for international attention to this issue, spanning continents and political ideologies. We must get past our differences over details and build on this shared understanding.

Ladies and gentlemen,

The year 2011 has a good chance of going down in history as a turning point towards consensual international attention to this issue.

The issue has been intensively discussed at conferences organized by individual countries and at many international forums.

- In this year's Deauville Declaration, the G-8 countries dedicated a separate paragraph to the issue of the Internet;
- the OSCE is working from the perspective of political/military disarmament to achieve agreement on a package of confidence- and security-building measures across three continents, from Vancouver to Vladivostok;
- the OECD and APEC are primarily interested in the economic aspects,
- while the Council of Europe is mainly interested in the law enforcement aspects of this issue;
- the network security aspects of this issue played a major role in NATO's Cyber Defence Policy adopted this summer;
- the European Commission wants to work on harmonization;
- and lastly, this issue has found broad support in the United Nations General Assembly committees, most recently this autumn in the First Committee.

This list could certainly go on.

With all the different debates, which are naturally influenced by different political interests, the question is whether a common denominator can be found for as many countries as possible.

Any understanding should include

- a package of material norms of state behavior in cyberspace and
- an acceptable form.

Even in our complicated world with widely varying interests, on closer examination at international forums one can find a surprising degree of consensus. The following points concerning the protection of global cyber space are addressed:

1. the ability of critical infrastructures to withstand failure,
2. economic aspects, protection of intellectual property and protection against crime,
3. human rights, and
4. development aid.

I would wager that most can agree on these points, because I am fairly certain that the defenders of economic interests, for example, would not seriously deny the importance of upholding human rights, and the defenders of human rights would not oppose having resilient critical infrastructures, and so on.

I think this is already a good material basis for developing principles or norms of responsible state behaviour in cyberspace.

I believe the best common denominator is economic growth: Both digitally dependent national economies, both established and expanding, must keep an eye on interoperability, network availability and the protection of critical infrastructures.

As far as an acceptable form for norms of state behavior, I believe the first option is "soft law", which is politically rather than legally binding although it encourages the formation of customary international law and can serve as an aid to interpretation in case of conflict. There are successful models for formulating common principles of international policy on the basis of soft law. As a prominent example, I would mention only the 1948 Universal Declaration of Human Rights, which is now considered part of customary international law.

I could imagine starting with a politically binding, soft law codex for norms of state behaviour in cyberspace which have broad international acceptance. I am hopeful that successful approaches will eventually become binding.

There is no need to re-invent norms of state behavior for cyberspace. If we could agree in a first step which internationally recognized principles can be applied to cyberspace, we would have already made significant progress.

My vision for a shared understanding of cyberspace oriented on the physical world is largely based on this idea:

- security and predictability of activities in cyberspace;
- transparency and trust- and security-building measures;
- international cooperation and fight against cyber crime.

States could agree on the following, in agreement with tried and tested general principles for cyberspace:

- peaceful use
- a culture of cyber security
- availability, confidentiality, integrity, authenticity
- an obligation to protect critical infrastructures
- an obligation to fight malicious software as well as criminal and terrorist misuse as generally understood
- cooperation among states in attributing cyber attacks.

Based on these principles, a series of concrete, confidence-building measures and cooperation mechanisms can be developed, such as

- building a network of points of contact for crisis communications
- creating early-warning mechanisms and improving cooperation between computer emergency response teams (CERTs)
- sharing national strategies, white papers and best practices
- capacity-building in less-developed countries
- improving resilience of critical infrastructures in view of cross-border dependencies, etc.

Along with these important preventive measures to ensure international cyber security, given the current risk of cyber attacks from outside — whether private or state-sponsored — we must consider and discuss the legal perspectives in connection with preventing such risks. International law can answer the question whether and how states may defend themselves against external attack. But the relevant literature is still discussing the issues of what is known as active network defence. The following problems result from the special nature of cyberspace:

- the lack of borders,
- the limited possibility of attributing an attack,
- the likelihood that non-state actors are the aggressor.

Possibly the greatest problem with the state prevention of external threats is that the relevant preventive measures take effect beyond one's own borders and may lead to retaliation — a vicious circle to be avoided.

Today customary international law provides a sufficient basis for preventing less serious attacks with similar means. Nonetheless, basic practical questions remain unresolved, of which I would like to mention just two:

- When is a state required to tolerate a preventive measure by another state on its territory, especially if the attack may have been carried out by non-state actors?
- How can the potential for conflict resulting from threat prevention which intrudes on the territorial sovereignty of a state following an attack launched from its territory be reduced?
- Summed up in a single question: How can violations of international law or conflicts under international law be avoided in case of measures taken under threat prevention law?

Consent to conduct a threat prevention measure of another state on one's own territory could help, but would probably be difficult to achieve due to time constraints and for political reasons.

Ladies and gentlemen,

I therefore propose discussing the possibility of implied consent!

My general suggestion would be to agree in the context of norms of state behaviour in cyberspace that states which tolerate or fail to prevent cyber attacks being launched from their territory should not be able to shirk their responsibility for such attacks and, in case of doubt, must tolerate reasonable countermeasures taken from outside.

In shaping cyberspace, in order not to hinder progress and opportunity, there are very good reasons to pursue the multi-stakeholder approach and avoid state interference in the form of regulations. Past experience has shown the potential benefits for humanity that can result.

However, when it is necessary to preserve, protect and strengthen global cyberspace and its advantages, then state action is unavoidable and desirable, just as in the physical world. This goal has been recognized world-wide. The relevant norms are currently being developed by consensus and in open discourse. This conference is an important contribution to the discussion.

The first important challenges have already been mastered. The international dialogue is under way.

I am optimistic that the urgent issue of political/diplomatic threat prevention can also be resolved in the near future. It is clear that the world is willing.

Thank you.

