Auswärtiges Amt

Freie Universität Berlin

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

United Nations
Institute for
Disarmament Research
UNIDIR

Challenges in Cybersecurity –
Risks, Strategies, and Confidence-Building
International Conference

(Preliminary Programme 10.10.2011)

Organising Institutions:

- Institute of Computer Science and Institute for International Law, European Law and Comparative Public Law, Freie Universität Berlin
- Institute for Peace Research and Security Policy at the University of Hamburg (IFSH)
- United Nations Institute for Disarmament Research, Geneva (UNIDIR)
- Federal Foreign Office, Berlin

Background:

The threat from cyberattacks is increasingly perceived as a problem of national and international security as cyberattacks grow in number and sophistication and as actors behind them are no longer only private hackers and organized criminals but also states. Yet, there appear to be widely different assessments of how real the threat is, where the risks are coming from, who is best placed to respond to this problem, and what kind of international measures and strategies are appropriate to secure information societies against malicious actors and to safeguard a peaceful use of the cybersphere. This conference brings together decision-makers and experts from several disciplines and industry in order to contribute to a detailed discussion of fundamental problems and evolving issues, of future national or international regulations, of technical and non-technical approaches with the goal of exploring options for confidence- and transparency-building measures in cyberspace.

States need to seriously address the daunting challenges to protect their information networks - especially those related to national security and critical infrastructure - from any attacker. But recent developments have shown that there is more to this debate than the solution of technical questions, in particular as many technical problems do not seem solvable at all. A larger framework that includes international norms of behaviour to ensure the peaceful use of cyberspace is needed. To enable such a framework, a variety of open questions have to be addressed.

- The potential of the newly emerging sophisticated cyberattackers, their motivations, tactics and procedures as well as the cost and benefits to national and international security of military doctrines incorporating offensive cyber operations have yet to be fully understood. Given the difficulty in attributing cyber attacks, offensive uses in the cyber domain could lead to geo-strategic instability and raise the risk of miscalculations in times of crisis which can lead to conflict. It is important to understand the current trends and developments regarding the potential misuses of cyberattacks for conflict and war, and the effects that may result to 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 why doing so is important for the future. For example, how should national militaries apply the laws of armed conflict and humanitarian law to cyber warfare? How does one judge a proportional response? What level of cyber disruption constitutes “unacceptable harm” to civilians? Even more fundamentally, what constitutes casus belli in the cyber domain?

- It should be investigated what constraints can, and should, be put upon offensive cyber operations given their technical conditions and the current legal regimes. Is it possible to control cyber operations at all? What are the strengths and weaknesses of major strategies to prevent the misuse of cyberspace? An effective response to the threat from cyberattack will have to involve a variety of stakeholders. But what is the respective role of substate 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 behaviour and confidence- and security-building measures? And what potential is there for international organizations such as the EU, OSCE, NATO and the UN? Can cyber operations be governed by them?

- Finally, the conference aims to discuss the relative value of elements of a possible international regulation aimed at preventing the hostile use of information technology. It aims to evaluate the lessons learned from efforts to regulate other dual-use technologies and apply them to the special case of cyberwarfare.

Procedures:

The conference language is English. Proceedings will take place under Chatham House Rule on a non-attribution basis.
The two-day conference starts with plenary presentations of different national cybersecurity policies with speakers from the United States, Russia, China and the European Union. This is followed by parallel tracks on specific issues related to the conference theme. Speakers are asked to contribute within the tracks, chairs will formulate a summary of most relevant insights.
Contributors are requested to give short introductions to their disciplinary perspective on the problem they deal with, followed by a presentation of their recommendations.
The chairs of these working group sessions will present the results in plenary meetings at the end of the day to the plenary. This serves also the purpose of creating input for future initiatives and activities on the national and the international level. Practitioners, experts and decision makers from the commercial, academic, military and governmental sector will be invited as participants.

Scientific Board:

- Dr. Sandro Gaycken, Freie Universität Berlin, Institute of Computer Science
- Prof. Dr. Heike Krieger, Freie Universität Berlin, Institute for International Law, European Law and Comparative Public Law
- Prof. Dr. Götz Neuneck, Institute for Peace Research and Security Policy at the University of Hamburg
- Theresa Hitchens, United Nations Institute for Disarmament Research, Geneva

Date:

13th and 14th December 2011

Location:

Conference Area, Federal Foreign Office, Berlin

Challenges in Cybersecurity –
Risks, Strategies, and Confidence-Building
International Conference

Programme

(All speakers to be confirmed, unless otherwise indicated)

Day 1, Tuesday December 13

8.30 a.m. — Welcome Address

Martin Fleischer, Head of International Cyber Policy Coordination Staff, Federal Foreign Office

Representatives of the organising institutes *(confirmed)*

9.00 a.m. — Opening Keynote

Dr. Werner Hoyer, Minister of State *(tbc)*

9.45 a.m. — Introductory Talk

Christopher Painter, Coordinator for Cyber Issues, State Department, USA: *How to deal with Cybersecurity: The US Approach (confirmed)*

10.15 a.m. – 10.45 a.m. — Introductory Talk

N.N., Ministry of Foreign Affairs, Russian Federation: *How to deal with Cybersecurity: The Russian Approach*

11.00 a.m. – 12.30 p.m. — Tracks

Talk 1: 11.00 to 11.45 (speech 20 min., discussion 25 min.)
Talk 2: 11.45 to 12.30

12.30 p.m. – 1.30 p.m. — Lunch break

1.30 a.m. – 3.45 p.m. — Tracks (continued)

Talk 3: 1.30 to 2.15
Talk 4: 2.15 to 3.00
Talk 5: 3.00 to 3.45

3.45 p.m. – 4.15 p.m. — Coffee break

4.15 p.m. – 5.45 p.m. — Plenary

Presentation of track results by chairs and final discussion

Programme

(All speakers to be confirmed, unless otherwise indicated)

Day 2: Wednesday, December 14

9.00 a.m. — Opening Keynote
N.N., Pentagon, US Cybercommand, USA: *Establishing Cyberdefenses in the US*

9.40 a.m. — Introductory Talk
N.N., Official Representative of China: *How to deal with Cybersecurity: The Chinese Approach*

10.20 a.m. — Introductory Talk
Mara Marinaki, Managing Director Global and Multilateral issues department; European External Action Service: *How to deal with Cybersecurity: The EU Approach (confirmed)*

11.00 a.m. – 12.30 p.m. — Tracks
Talk 1: 11.00 to 11.45 (speech 20 min., discussion 25 min.)
Talk 2: 11.45 to 12.30

12.30 p.m. – 1.30 p.m. — Lunch break

1.30 a.m. – 3.45 p.m. — Tracks (continued)
Talk 3: 1.30 to 2.15
Talk 4: 2.15 to 3.00
Talk 5: 3.00 to 3.45

3.45 p.m. – 4.15 p.m. — Coffee break

4.15 p.m. – 5.45 p.m. — Plenary
Presentation of summaries and final discussion

5.45 p.m. – 6.15 p.m. — Closing event
Representatives of the organising institutes

Day 1, Tuesday December 13

1.1 Track One: Cybersecurity and Society

Chair: Martin Fleischer, Federal Foreign Office *(confirmed)*

This section will look at different societal factors determining the perception and the development of cybersecurity.
It will answer to the following questions:

- Which societal factors are important to cybersecurity and how can they be ranked?
- How do we manage conflicting interests in cyberspace and its regulation? How will future conflicts develop?
- Are international approaches to cybersecurity feasible? How nation- specific are cyber-insecurities and their management?
- How do different states view cybersecurity?
- How do we deal with the militarization of the cyber domain and the potential for impacts on its commercial and societal uses?

Contributors (speech 20 min., discussion 25 min.):

- **Talk 1: 11.00 to 11.45**
  Prof. Dr. David S. Wall, Durham University: *The History of Cybersecurity and Society (confirmed)*

- **Talk 2: 11.45 to 12.30**
  Markus Beckedahl, Berlin: *The Web as a Free Commons (confirmed)*

- **Talk 3: 1.30 to 2.15**
  N.N., Federal Ministry of the Interior: *Germany's National Cybersecurity Strategy*

- **Talk 4: 2.15 to 3.00**
  Zoltan Wirth, Siemens: *The Cybersecurity of Infrastructures (confirmed)*

- **Talk 5: 3.00 to 3.45**
  Pascale Sourisse, Senior Vice President du Conseil Exécutif du Groupe Thalès: *Information Technology and Defense (confirmed)*

Day 1, Tuesday December 13

1.2 Track Two: Cybersecurity dilemmas

Chair: Dr. Sandro Gaycken, Freie Universität Berlin *(confirmed)*

This section aims to clarify a number of systemic problems inherent to the realm of cybersecurity. It will try to separate immutable characteristics of these problems from mutable ones and propose future avenues of action to mitigate effects.

The following questions will be investigated:

- What is the impact of technical, organizational and regulatory complexity and how much of our present practices would have to change to regain a sufficient level of control?
- What does the lack of attribution imply for defensive postures?
- Are trade-offs between privacy and security a necessary evil?

Contributors (speech 20 min., discussion 25 min.):

- **Talk 1: 11.00 to 11.45**
  Tim Dowse, Director Cyber Policy, FCO, UK *(confirmed)*

- **Talk 2: 11.45 to 12.30**
  Reinhard Clemens, Member of the Board of Management at Deutsche Telekom AG, CEO of T-Systems: *Complexity is the Enemy (confirmed)*

- **Talk 3: 1.30 to 2.15**
  Michael Hange, President of the BSI: *International or National Approaches? Technical and Regulatory Specifics of a German Approach to Cybersecurity (tbc)*

- **Talk 4: 2.15 to 3.00**
  Prof. Herb Lin, Director, National Research Council USA: *Attribution and Defensive Postures (confirmed)*

- **Talk 5: 3.00 to 3.45**
  Tyler Moore, PhD, Harvard University, USA: *The Economics of Cybersecurity – Past, Present and Future (confirmed)*

Day 1, Tuesday December 13

1.3 Track Three: Regulating Cybersecurity

Chair: Prof. Sylvia Kierkegaard, University of Southhampton, UK *(confirmed)*

This track will look at potential regulations in cyberspace, especially accounting for the threat of sophisticated attackers.

Questions will be:

- Is cross-border regulation credible without attribution? Is non-attribution tolerable?
- What could international law look like in a post-attribution environment? Can we apply lessons from other international efforts to prevent the misuse of dual-use technologies (Biological Weapons Convention, Chemical Weapon Convention, ENMOD-Convention, arms control in outer space)?
- How can internationally dispersed cybercrime be prevented? Which international agreements exist and how can they be extended to become more effective? How can the “de minimis” problem in cybercrime be countered?
- How to criminalize cyberattacks under international law?
- How can private actors with no inherent incentives for security be regulated? Will strong cybersecurity have to be enforced upon them?

Contributors (speech 20 min., discussion 25 min.):

- **Talk 1: 11.00 to 11.45**
  Prof. Heike Krieger, Freie Universität Berlin: *Post-Attribution International Law (confirmed)*

- **Talk 2: 11.45 to 12.30**
  Prof. Chris Demchak, Naval War College: *Westphalia in Cyberspace (confirmed)*

- **Talk 3: 1.30 to 2.15**
  Dr. Susanne Wasum-Rainer, Director-General Legal Affairs, Federal Foreign Office *(confirmed)*

- **Talk 4: 2.15 to 3.00**
  Dr. Nils Melzer, Centre for Business and Human Rights at the University of Zürich: *The Law of War in Cyberspace (confirmed)*

- **Talk 5: 3.00 to 3.45**
  Dr. John B. Sheldon, School of Advanced Air and Space Studies, Air University, Maxwell Air Force Base, Alabama: *National Security vs. International Security: constraints, risks and trade offs (confirmed)*

Day 2: Wednesday, December 14

2.1 Track One: Understanding Computer Network Activities

Chair: Prof. Paul Cornish, Chatham House, UK *(confirmed)*

This track will aim at a better understanding of military activities in cyberspace and try to provide detailed threat models to serve future regulatory or technical approaches to design cybersecurity.
The following questions will be investigated:

- What are military strategic interests and assets in cyberspace?
- Which kinds of operations do we have to account for?
- How could their likelihood and impact be measured and ranked? How could effects be mitigated?

Contributors (speech 20 min., discussion 25 min.):

- **Talk 1: 11.00 to 11.45**
  Dr. James Andrew Lewis, Director of Technology and Public Policy of CSIS, USA: *Cyberhype and Cyberreality (confirmed)*

- **Talk 2: 11.45 to 12.30**
  Ambassador Jean-François Blarel, Deputy Secretary General of the French MFA and Cyber Coordinator: *Cyber Defence in France (confirmed)*

- **Talk 3: 1.30 to 2.15**
  N.N., Russian Official Representative: *Cyber Defence in Russia*

- **Talk 4: 2.15 to 3.00**
  Dr. Jamie Shea, NATO-IS: *NATO's Approach to Cyber Defence (confirmed)*

- **Talk 5: 3.00 to 3.45**
  N.N, Federal Ministry of Defence (BMVg): *Cyber Defence in Germany*

Day 2: Wednesday, December 14

2.2 Track Two: High-End Hacking

Chair: ***Prof. Dr. Volker Roth, FU Berlin (confirmed)***

This track will investigate the new technical and organizational quality of hacking, emerging from new actors such as organized crime and militaries.

Questions will be:

- Which new technical and organizational means do we have to account for? How do we have to broaden our view? How will military and criminal approaches differ?
- How will the quality of hacking develop? Which classical threats are still relevant, which are not? Could there be a spiralling dynamic in hacking events?
- How much protection can we ever hope for?

Contributors (speech 20 min., discussion 25 min.):

- **Talk 1: 11.00 to 11.45**
  BMI/BSI, NN: Organized Crime as a New Actor – *The Professionalization of IT-Insecurity*

- **Talk 2: 11.45 to 12.30**
  Rich Cummings, HB Gary: *Military Hacking as a Service (confirmed)*

- **Talk 3: 1.30 to 2.15**
  Felix FX Lindner, Recurity Labs, Berlin: *Military-Grade Hacking (confirmed)*

- **Talk 4: 2.15 to 3.00**
  Ilias Chantzos, Director EMEA & APJ Government Relations for Symantec *(confirmed)*

- **Talk 5: 3.00 to 3.45**
  Dr. Richard Clayton, Cambridge University, UK: *Trends in Sophisticated Hacking (confirmed)*

Day 2: Wednesday, December 14

2.3 Track Three: Introducing Transparency and Confidence-building

Chair: Theresa Hitchens, UNIDIR, Geneva *(confirmed)*

This session will attempt to identify confidence-building in the international cyber-realm and strategies for implementation.

- How to implement international cooperation to protect civil infrastructures?
- Transparency: Does confidence-building work in cyberspace?
- How are the chances to establish “codes of conduct” for governments, companies or individuals and international norms of behaviour to ensure the peaceful use of cyberspace?
- Restricting offensive operations: Are declarations of no-(first)-use feasible?
- Is a convention to Limit Cyberwarfare in the UN framework possible?
- How can we hold states responsible for cyber attacks originating from their territories?
- How do we establish an international obligation to investigate cyber attacks?

Contributors (speech 20 min., discussion 25 min.):

- **Talk 1: 11.00 to 11.45**
  Michele Markoff, Senior Policy Advisor, Office of the Coordinator for Cyber Issues, US Department of State *(confirmed)*

- **Talk 2: 11.45 to 12.30**
  Dr. Gao Zugui, Assistant President of the Institute for Strategic Studies of the Party School of the Central Committee of the Communist Party of China: *Chinese views for Confidence-building Measures (tbc)*

- **Talk 3: 1.30 to 2.15**
  Amb. (Ret'd) Paul Meyer, Simon Fraser University and the Simons Foundation: *Transparency and Confidence-building Measures: Options for International Cyber Security (confirmed)*

- **Talk 4: 2.15 to 3.00**
  Dr. Greg Austin, EastWest Institute: *State Rights and Responsibilities in Cyber Space (confirmed)*

- **Talk 5: 3.00 to 3.45**
  Dr. Detlev Wolter, Federal Foreign Office, Germany: *Multilateral Approaches to Cybersecurity (confirmed)*