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

Conference Programme

Day 1: Tuesday, 13 December

7.30 a.m. — Admission/Security Check (Photo ID REQUIRED)
Registration of participants, location: Federal Foreign Office Conference Area, access via entrance at Unterwasserstr. 10, 10117 Berlin (Mitte district)

8.30 a.m. — Welcome (Location: *Europasaal*)
Herbert Salber, Deputy Political Director, Federal Foreign Office
Theresa Hitchens (UNIDIR)
Prof. Götz Neuneck (IFSH)
Dr Sandro Gaycken (FU Berlin)

9.00 a.m. — Opening Keynotes
Dr Werner Hoyer, Minister of State, Federal Foreign Office
Cornelia Rogall-Grothe, State Secretary, Federal Government Commissioner for Information Technology, Federal Ministry of the Interior

9.50 a.m. — “Family Photo”

10.05 a.m. — Introductory Talk
Christopher Painter, Coordinator for Cyber Issues, State Department, USA: *Building a Shared International Consensus on Norms of Conduct in Cyberspace*

10.30 a.m. to 10.55 a.m. — Introductory Talk
Wladislaw Petrowitsch Sherstyuk, Lomonossow State University, Adviser to the Security Council of the Russian Federation: *International Cybersecurity - the new Russian Initiatives*

11.00 a.m. — Tracks (detailed information in the “Track Programme”)
Locations:
Track 1: *Adenauer-Saal*
Track 2: *Stresemann-Saal*
Track 3: *Rathenau-Saal*

12.30 p.m. — Lunch Break

1.30 p.m. — Tracks (continued)

3.45 p.m. — Coffee Break

Conference Programme, continued

4.15 p.m. to 5.45 p.m. — Plenary

Presentation of track results by chairs and final discussion; Chair: Prof. Götz Neuneck (IFSH)

6.30 p.m. — Buffet Reception Hosted by Microsoft

Location: *Quadriga-Forum*, Werderscher Markt 15, 10117 Berlin (Mitte district) - within walking distance of conference location

Day 2: Wednesday, 14 December

8.00 a.m. — Admission/Security Check (Photo ID REQUIRED)

9.00 a.m. — Welcome (Location: *Europasaal*)

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

9.15 a.m. — Introductory Talk

Ambassador Jean-François Blarel, Deputy Secretary General of the French MFA and Cyber Coordinator: *The French Policy in the Field of Cybersecurity*

9.40 a.m. — Introductory Talk

Kang Yong, Deputy Director-General, Department of Arms Control and Disarmament, Ministry of Foreign Affairs, People's Republic of China: *China's Perspective on Information Security*

10.05 a.m. — Introductory Talk

Frank Asbeck, Principal Advisor Space and Security Policy, European External Action Service: *How to Deal with Cybersecurity: The EU Approach*

10.30 a.m. — Coffee Break

11.00 a.m. — Tracks (detailed information in the "Track Programme")

Locations:
Track 1: *Adenauer-Saal*
Track 2: *Stresemann-Saal*
Track 3: *Rathenau-Saal*

12.30 p.m. — Lunch Break

1.30 p.m. — Tracks (continued)

3.45 p.m. — Coffee Break

4.15 p.m. — Plenary

Presentation of summaries and final discussion; Chair: Theresa Hitchens (UNIDIR)

5.45 p.m. — Closing Remarks

Panel with the representatives of the organizing institutions; Chair: Herbert Salber (FFO)

6.15 p.m. — End of Conference

Track Programme

Day 1: Tuesday, 13 December

1.1 Track One: Cybersecurity and Society

Chair: Martin Fleischer, Federal Foreign Office

Location: Adenauer-Saal

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

- What societal factors are important to cybersecurity and how can they be ranked?
- How do we manage conflicting interests in cyberspace and in 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 its potential impact on the commercial and societal uses of cyberspace?

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

- **Talk 1: 11.00 a.m. to 11.45 a.m.**
  Prof. David S. Wall, Durham University: *The History of Cybersecurity and Society*

- **Talk 2: 11.45 a.m. to 12.30 p.m.**
  Peter Schaar, Federal Commissioner for Data Protection and Freedom of Information: *Data Protection - Limit or Benefit for Cybersecurity*

- **Talk 3: 1.30 p.m. to 2.15 p.m.**
  Markus Beckedahl, Berlin: *The Web as a Free Commons*

- **Talk 4: 2.15 p.m. to 3.00 p.m.**
  Dr Markus Dürig, Head of IT Security Division, Federal Ministry of the Interior: *Germany's National Cybersecurity Strategy*

- **Talk 5: 3.00 p.m. to 3.45 p.m.**
  Zoltan Wirth, Vice President, Head of Global Operations, Cassidian Security & Communication Solutions: *The Cybersecurity of Infrastructures*

Track Programme, continued

Day 1: Tuesday, 13 December

1.2 Track Two: Cybersecurity Dilemmas

Chair: Dr Sandro Gaycken, Freie Universität Berlin

Location: Stresemann-Saal

This section aims to clarify a number of systemic problems inherent to the realm of cybersecurity. It will seek 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 many 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 a.m. to 11.45 a.m.**
  Tim Dowse, Director Cyber Policy, Foreign and Commonwealth Office, UK: *The international policy debate after the London Conference on Cyberspace*

- **Talk 2: 11.45 a.m. to 12.30 p.m.**
  Wolfgang Kopf, Senior Vice President Public and Regulatory Affairs Deutsche Telekom AG: *Complexity is the Enemy*

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

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

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

Track Programme, continued

Day 1: Tuesday, 13 December

1.3 Track Three: Introducing Transparency and Confidence-building

Chair: Theresa Hitchens, UNIDIR, Geneva

Location: Rathenau-Saal

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

- How can international cooperation to protect civil infrastructures be implemented?
- Transparency: Does confidence-building work in cyberspace?
- What are the chances of establishing "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 cyberattacks originating from their territories?
- How do we establish an international obligation to investigate cyberattacks?

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

- **Talk 1: 11.00 a.m. to 11.45 a.m.**
  Michele Markoff, Senior Policy Advisor, Office of the Coordinator for Cyber Issues, US Department of State: *Building Confidence and Reducing Risk in Cyberspace*

- **Talk 2: 11.45 a.m. to 12.30 p.m.**
  Dr Rex Hughes, Cambridge University: *Suitable CSBMs / sui generis / for cyberspace*

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

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

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

- **Comments:**
  Tim Maurer, Harvard University

Track Programme, continued

Day 2: Wednesday, 14 December

2.1 Track One: Understanding Computer Network Activities

Chair: Prof. Paul Cornish, University of Bath, UK

Location: Adenauer-Saal

This track will aim at a better understanding of military activities in cyberspace and seek to provide detailed threat models to serve future regulatory or technical approaches to designing cybersecurity.

The following questions will be investigated:

- What are military strategic interests and assets in cyberspace?
- What 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 a.m. to 11.45 a.m.**
  Dr James Andrew Lewis, Director of Technology and Public Policy of CSIS, USA: *Cyberhype and Cyberreality*

- **Talk 2: 11.45 a.m. to 12.30 p.m.**
  Eric Rosenbach, US-Deputy Assistant Secretary of Defense: *U.S. Department of Defense Strategy for Operating in Cyberspace*

- **Talk 3: 1.30 p.m. to 2.15 p.m.**
  Igor Nikolajewitsch Dylevskij, Department Head, Ministry of Defence, Russian Federation:
  Questions regarding the use of global information space by Russian armed forces for defence and security

- **Talk 4: 2.15 p.m. to 3.00 p.m.**
  Dr Jamie Shea, NATO Deputy Assistant Secretary General: *NATO's Approach to Cyber Defence*

- **Talk 5: 3.00 p.m. to 3.45 p.m.**
  Brigadier General Hans-Werner Wiermann, Deputy Assistant Chief of Armed Forces Staff for Politico Military Affairs and Arms Control, Federal Ministry of Defence: *Cyber Defence in Germany*

- **Comments:**
  Dr John B. Sheldon, School of Advanced Air and Space Studies, Air University, Maxwell Air Force Base, USA

Track Programme, continued

Day 2: Wednesday, 14 December

2.2 Track Two: High-End Hacking

Chair: Prof. John Mallery, Massachusetts Institute of Technology *(*MIT*)*, USA
Location: Stresemann-Saal

This track will investigate the new technical and organizational quality of hacking, emerging from new actors such as organized crime and militaries.
The following questions will be addressed:

– What 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 classic threats are still relevant, and 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 a.m. to 11.45 a.m.**
cancelled

– **Talk 2: 11.45 a.m. to 12.30 p.m.**
Rich Cummings, HB Gary: *Military Hacking as a Service*

– **Talk 3: 1.30 p.m. to 2.15 p.m.**
Felix FX Lindner, Recurity Labs, Berlin: *Military-Grade Hacking*

– **Talk 4: 2.15 p.m. to 3.00 p.m.**
Ilias Chantzos, Director EMEA & APJ Government Relations for Symantec: *Understanding Information Security. Challenges and Opportunities in an Evolving Threat Environment*

– **Talk 5: 3.00 p.m. to 3.45 p.m.**
Dr Richard Clayton, University of Cambridge, UK: *Trends in Sophisticated Hacking*

Track Programme, continued

Day 2: Wednesday, 14 December

2.3 Track Three: Regulating Cybersecurity

Chair: Prof. Sylvia Kierkegaard, University of Southampton, UK
Location: Rathenau-Saal

This track will look at potential regulations in cyberspace, especially accounting for the threat of sophisticated attackers.
The following questions will be addressed:

- 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? What international agreements exist and how can they be expanded to become more effective? How can the “de minimis” problem in cybercrime be countered?
- How can cyberattacks be criminalized 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 a.m. to 11.45 a.m.**
  Jur.lic. Dirk Roland Haupt, International Law Division, Federal Foreign Office: *Why States Need International Law for Cyber Security*

- **Talk 2: 11.45 a.m. to 12.30 p.m.**
  Prof. Heike Krieger, Freie Universität Berlin: *Post-Attribution International Law*

- **Talk 3: 1.30 p.m. to 2.15 p.m.**
  Prof. Chris Demchak, Naval War College: *Westphalia in Cyberspace*

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

- **Talk 5: 3.00 p.m. to 3.45 p.m.**
  J. Paul Nicholas, Senior Director, Global Security Strategy & Diplomacy at Microsoft Corporation: *A Private Sector Contribution to the Global Cyber-Norms Discussion*