



AGENDA

Tenth International Forum «Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security»

and

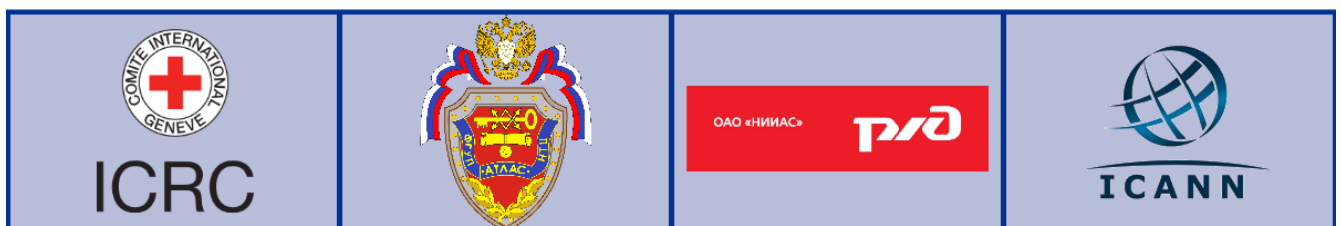
Thirteenth Scientific Conference of the International Information Security Research Consortium



April 25–28, 2016

Garmisch-Partenkirchen, Munich, Germany

Venue: Atlas Posthotel



April 25, Monday

09.00-10.00

Registration

10.00-13.00

Opening of the Conference
Plenary session

1. **Sherstyuk V.P.**, Co-Chairman of the Forum, Adviser of the Secretary of the Security Council of the Russian Federation, Director of Lomonosov Moscow State University Institute of Information Security Issues
2. **Krutskikh A.V.**, Special Representative of the President of the Russian Federation for International Cooperation in Information Security
3. **Dylevsky I.N.**, Ministry of Defense of the Russian Federation

11.30-12.00 – Coffee break

4. **A.Soldatov**, Council Chair, Foundation of Internet Development, Russia
5. **M.Yakushev**, Vice-President, Stakeholder Engagement, Eastern Europe, Russia and Central Asia, ICANN
6. **Gasumyanov V.I.**, Vice-President – Chief of Corporate Security Block, Norilsk Nickel, Russia

13.00-18.00

Workshop – Round table 1

Interpretation of basic concepts, principles and norms of Geneva Conventions with regard to cyberspace

Moderators:

- **A.Streltsov**, Lomonosov Moscow State University Institute of Information Security Issues
- **E.Tikk-Ringas**, International Institute for Strategic Studies, UK

Topics for Discussion

1. ICTs as means of warfare
2. Attribution of legal subjects of an armed conflict in ICT sphere
3. Identification of legal subjects and objects of ICT sphere protected by International Humanitarian Law
4. Combatants in an armed conflict in ICT sphere
5. Human rights in the context of an armed conflict in ICT sphere

Presentations:

1. **A.Streltsov**, Lomonosov Moscow State University Institute of Information Security Issues

2. **E.Tikk-Ringas**, International Institute for Strategic Studies, UK

14.00-15.30 Lunch

3. **William Boothby**, Geneva Centre for Security Policy, UK
Approaches to the application of law in cyberspace: a personal view

4. **P.Pilyugin**, Lomonosov Moscow State University Institute of Information Security Issues, Russia
Issues of object identification in cyberspace

5. **John Mallery** MIT, USA
Reflections on The Cyber Norms 4.0 Conference

April 26, Tuesday

9.00-11.30

Workshop – Round table 2
Challenges of nonproliferation and reduction of the risk of Cyberweapons use

Moderators:

- **V.Yashchenko**, Lomonosov Moscow State University Institute of Information Security Issues, Russia
- **Nigel Inkster**, International Institute for Strategic Studies, UK
- **Han Biao**, National University of Defense Technology, China

Topics for Discussion

1. The content of concepts «information weapon» and «cyber weapon»
2. Methodologies for achieving agreed definitions and concepts of military cyber capabilities and military cyber operations, that can also help define Confidence-Building Measures
3. The Wassenaar Arrangement as an element of information weapons non-proliferation regime
4. Possible principles of information weapons non-proliferation regime
5. International Information Security System as a means of preventing military conflicts that may arise in consequence of aggressive use of information weapons

Presentations:

1. **V.Yashchenko**, Lomonosov Moscow State University Institute of Information Security Issues, Russia
2. **Nigel Inkster**, International Institute for Strategic Studies, UK
3. **Han Biao**, National University of Defense Technology, China
4. **William Boothby**, Geneva Centre for Security Policy, UK
Possible approaches to defining military cyber weapons and their use
5. **Michael Sulmeyer**, Belfer Center for Science and International Affairs Harvard Kennedy School of Government
Thoughts on Controlling Escalation in a Cyber Crisis
6. **Tim Maurer**, Carnegie Endowment for International Peace
The private market of cyber capabilities
7. **Mika Kerttunen**, Cyber Policy Institute, Finland
IISS Military Balance – a framework for comparing military cyber capabilities
8. **Maurizio Martellini**, Insubria Center on International Security – ICIS, Italy, **Sandro Gaycken**, DSI, Berlin, Germany, **Clay Wilson**, CISSP, US

Recurring questions pertaining to the possible military dimensions of cyber warfare

11.30-12.00 – Coffee break

12.00-18.30

Round table
**Challenges of modern international relations in the
context of cyberspace**

Moderator:

A.Smirnov, the President of the National Institute for Research of Global Security (NIRGlobS), Extraordinary and Plenipotentiary Envoy of the Russian Federation

Topics for Discussion

1. State sovereignty in Cyberspace;
2. Rules of responsible behavior of States in ICT environment;
3. International authorization and responsibility for ensuring stability, reliability and security of the Internet.

Participants of the discussion:

Krutskikh A.V., Special Representative of the President of the Russian Federation for International Cooperation in Information Security

A.Streltsov, Lomonosov Moscow State University Institute of Information Security Issues

Sandro Gaycken, Digital Society Institute, ESMT – European School of Management and Technology, Germany

E.Tikk-Ringas, International Institute for Strategic Studies, UK

Han Biao, National University of Defense Technology, China

Nohyoung Park, Cyber Law Centre at Korea University, Republic of Korea

Daniel Stauffacher, ICT4Peace Foundation, Switzerland

Nigel Inkster, International Institute for Strategic Studies, UK

John Mallery MIT, USA

Rafal Rohosinski, SecDev, Canada

M.Yakushev, ICANN

14.00-15.30 Lunch

Presentations:

1. **A.Smirnov**, National Institute for Research of Global Security, Russia
Industry 4.0: information risks – a view from Russia

2. **Ben Hiller**, OSCE
Building confidence between States and Norms of responsible state behaviour in cyberspace: Two sides of the same coin
3. **William Boothby**, Geneva Centre for Security Policy, UK
Military to military dialogue on the use of cyber weapons as a distinct confidence building measure
4. **Sanjay Goel**, SUNY, USA
Internet Sovereignty
5. **Phil Gurski**, SecDev, Canada
What should we do about terrorists' use of social media?
6. **M.Polyakov**, Moscow State Institute of International Relations
New Media and Cyberspace: modern methods of production and distribution of information
7. **John Mallery** MIT, USA
Escalation Dynamics in Information Conflict

April 27, Wednesday

9.00-11.30

Workshop – Round table 3 Frameworks and tools of Public-Private Partnership for ensuring Information Security of Critical Infrastructure

Moderators:

- **A.Kulpin**, Norilsk Nickel, Russia
- **Sandro Gaycken**, Digital Society Institute, ESMT – European School of Management and Technology, Germany

Topics for discussion

1. **Information Sharing:** What constitutes a serious incident in CRITIS and how should it be reported? Should low-level intrusions be reported as well, given a potential to evolve into high-level incidents? Should incidents with a potential international impact be reported internationally?
2. **Technology Roadmaps and Investments:** What are interesting technologies to be developed, and how can industry and the state work together to create new IT-security companies to build them? Where do we get cybersecurity investments, and how can investors be sure to invest in the right product? How can the state help to sell products? What is the role of trust in IT-exports, and how does it impact the genesis and the fate of companies?
3. **Supply Chain Security:** How vulnerable is the supply chain, and what are the risks for CRITIS? How can it be controlled? Who should develop and implement the right technologies to secure the supply chain? Should it be regulated as strong as CRITIS?
4. **Regulatory leverage:** How much and where should infrastructures be regulated? What would be a smart regulation, and what would the regulator have to know to propose a good legislation? How can the industry be involved in regulation in a productive fashion?
5. **International Private Cooperation:** How should international private cooperation in cybersecurity be regulated? Which information, which technologies can be shared? How helpful is cooperation between multinational companies with different origins?

Presentations:

1. **A.Kulpin**, Norilsk Nickel, Russia
2. **Sandro Gaycken**, Digital Society Institute, ESMT – European School of Management and Technology, Germany
3. **A.Yarnykh**, Kaspersky Lab, Russia
Critical Infrastructure vulnerabilities, 2015 in review
4. **Rolf Reinema**, Siemens
(topic TBC)

5. **Charles L. Barry**, Institute for National Strategic Studies, NDU, USA
Strategic Considerations in Critical Information Infrastructure Protection
6. **A. Baranov**, National Research University Higher School of Economics, Russia
Information Security of wide-scale computer systems
7. **Tomas Lamanauskas**, Vimpelcom (Europe)
Telecom Operators: key partners in protecting critical infrastructure

11.30-12.00 – Coffee break

12.00-14.00

**Thirteenth scientific conference of the
International Information Security Research Consortium (IISRC)**

Moderator:

Sherstuyk V.P., Head organizer of the International Information Security Research Consortium, Co-Chairman of the Forum, Adviser of the Secretary of Security Council of the Russian Federation, Director of Lomonosov Moscow State University Institute of Information Security Issues

IISRC projects presentations:

1. **M. Medrish**, Internet Support Foundation, Russia
2. **A. Streltsov**, Lomonosov Moscow State University Institute of Information Security Issues
3. **Yerzhan Seitkulov**, Institute of Information Security & Cryptology at Gumilyov Eurasian National University
4. **Rafal Rohosinski**, SecDev, Canada, **Nigel Inkster**, International Institute for Strategic Studies, UK

Organizational questions:

5. Decision on Topic, Agenda, Time and Venue of the Fourteenth Scientific Conference of the IISRC.

14.00-15.30 Lunch

15.30-18.00

**Workshop – Round table № 4
Measures of countering the use of Internet for recruitment
and advocacy of extremism and terrorism**

Moderators:

- **R. Sharyapov**, Lomonosov Moscow State University Institute of Information Security Issues
- **Nohyoung Park**, Cyber Law Centre at Korea University, Republic of Korea
- **Rafal Rohosinski**, SecDev, Canada

Topics for discussion

1. Possible international-legal and political initiatives for countering the use of the Internet for recruitment and advocacy of extremism and terrorism. Development of liability arrangements in the framework of intergovernmental cooperation and public-private partnerships for web hosting companies who support extremist and terrorist websites.
2. Best national practices for countering the use of Internet for recruitment and advocacy of extremism and terrorism.
3. Problems of scientific and technological support of the works on identification of destructive content and its sources.

Presentations:

1. **R.Sharyapov**, Lomonosov Moscow State University Institute of Information Security Issues
2. **Nohyoung Park**, Cyber Law Centre at Korea University, Republic of Korea
3. **Rafal Rohosinski**, SecDev, Canada
4. **A.Masalovich**, DialogNauka, Russia (**topic TBC**)
Identification of signs of extremist propaganda on the Internet. Analysis of social portraits of extremists, recruiters and their potential victims
5. **N.Romashkina**, Primakov Institute of World Economy and International Relations, Russian Academy Of Sciences
Addressing threats in cyberspace: the role of scientific and educational institutions

April 28, Thursday

**Bilateral and Multilateral Negotiations and Consultations
(by appointment)**