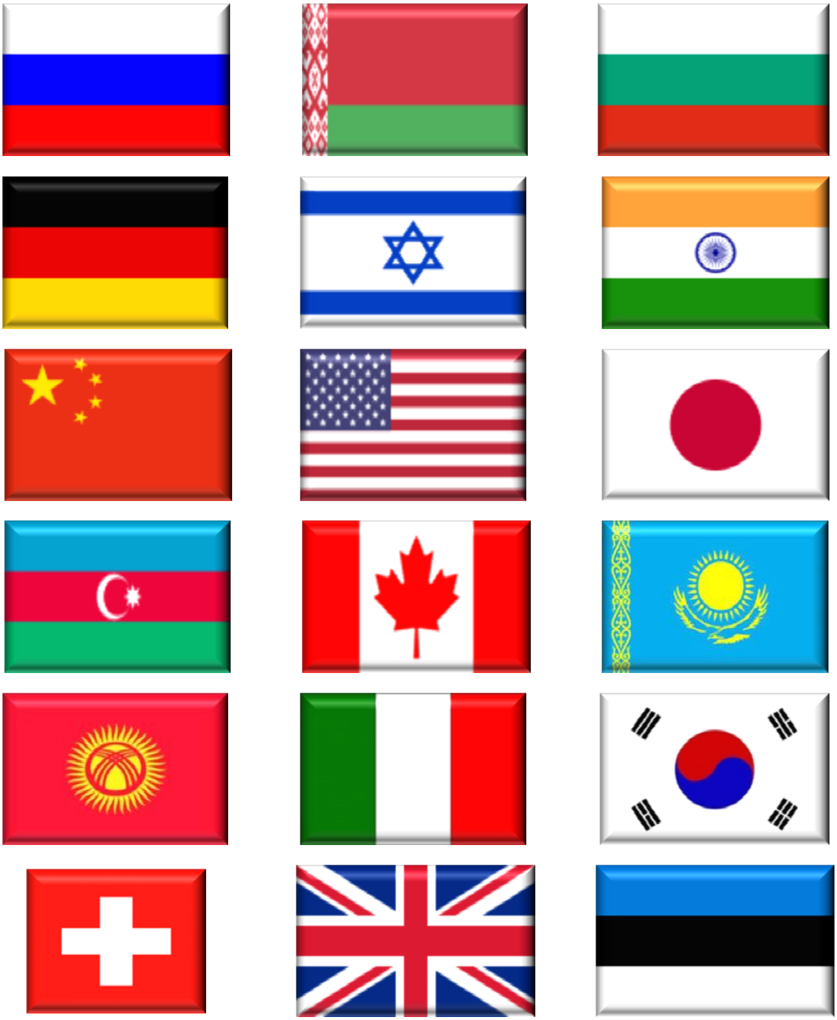
International Information Security Research Consortium was established at the initiative of the Institute of Information Security Issues of Moscow State University on April 25, 2010

IISRC Declaration signing ceremony
(Garmisch-Partenkirchen, Germany)

Initially **11** organizations of **9** countries became the members of IISRC

Presently there are **28** organizations from **18** countries in IISRC

As of April 2019 there are **28** organizations from **18** countries in IISRC



Organizations
Founding members of IISRC

1. Institute of Information Security Issues at Moscow State University (**Russia**)
2. United Institute of Informatics Problems of the National Academy of Sciences of **Belarus**
3. Internet Society of **Bulgaria**
4. Cybercrime Research Institute (**Germany**)
5. IT Security E-Government Division (**Israel)**
6. **Indian** Institute of Information Technology in Allahabad
7. **China** Association for International Friendly Contact (CAIFC)
8. “MFI SOFT” LLC (**Russia**)
9. The State University of New York (SUNY) (**USA**)
10. Global Cyber Risk LLC (**USA**)
11. Tokai University (**Japan**)

Organizations
Joined IISRC since 2010

1. EastWest Institute (**USA**)

2. Defence Research and Development Organization, Ministry of Defence, **India**

3. Khazar University (**Azerbaijan** - **USA**)

4. PayPal Inc. (**USA**)

5. Qafqaz University (**Azerbaijan** - **Turkey**)

6. SecDev Foundation (**Canada**)

7. Institute of Information Security & Cryptology at Gumilyov Eurasian National University (**Kazakhstan**)

8. Institute of Electronics and Telecommunications (IE&T) under **Kyrgyz** State Technical University named after I.Razzakov

9. Insubria Center on International Security (**Italy**)

10. **Korea** University Cyber Law Centre

11. ZTE Inc. (**China**)

12. ICT4Peace Foundation (**Switzerland**)

13. MMC "NORILSK NICKEL" (**Russia**)

14. The International Institute for Strategic Studies (**UK**)

15. Cyber Policy Institute (**Estonia**)

16. Kaspersky Lab (**Russia**)

17. Editorial team of the Journal “International Affairs” (**Russia**)

Priorities and research projects of IISRC:

1. Escalatory Models: Development of shared models of escalation in cyber conflict, including definitions of hostility levels;
2. Civilian Infrastructures: International legal status of civilian cyber infrastructures in the context of peace or war;
3. Cyber Definitions: Definitions of information warfare and cyber defense topics;
4. Cyber Law: International legal frameworks to increase stability of intergovernmental relations and promote orderly international economic processes;
5. Codes of Conduct: Development of shared norms for behavior in cyber space for individuals, countries and non-state actors;
6. Cyber Terrorism: International agreements to counter non-state actors seeking to launch cyber attacks on countries or provoke conflicts among countries using cyber means;
7. Cyber Crime: Legal and technical coordination against cyber crime;
8. Technical Cooperation: International mutual assistance across public and private spheres to improve cyber situational awareness, enhance

protection of critical infrastructures and respond to significant cyber failures or attacks;

9. Protection of the Commons: Framework to separate technical architectures and operation of cyber space from economic and political issues and provide separate mechanisms on the technical plane or the political economic level for resolving differences or marshalling international cooperation;

10. Industrial Espionage: International legal framework for industrial espionage whether sponsored by states or whether its fruits are purchased on criminal black markets by states;

11. Adaptation of International Law to Conflicts in the Information Space;

12. Information Security of Critical Infrastructure

13. Rules of responsible behaviour of the States in Information space;

14. Ensuring the security of critical information infrastructure;

15. Development of an international system for monitoring of threats to international information security;

16. Countering the use of ICTs for interference in the internal affairs of sovereign States;

17. Rules of responsible behaviour of Business entities in Cyberspace;
18. Issues of the use of ICTs for military and political purposes;
19. Elaboration of forecasts and analytical models of Internet development;
20. Security, stability and resiliency of Global Internet Infrastructure.

International Information Security Research
Consortium (IISRC)

Resolution of the XII International Forum «Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security» and the Sixteenth Scientific Conference of the International Information Security Research Consortium

April 16-19, 2018
Garmisch-Partenkirchen, Germany

1. The participants of the sessions have discussed the following topical issues of International Information Security:

- Current issues of Information Security in the context of Digital economy development (Workshop – Round table № 1);
- Frameworks for implementation of public-private partnership in the field of ensuring the security of Critical Information Infrastructure (Workshop – Round table № 2);

- Challenges of countering the use of ICTs for malicious military and political purposes (Workshop – Round table № 3);
- Frameworks for the implementation of norms, rules and principles for responsible behaviour of the States in the ICT environment (Workshop – Round table № 4);
- Challenges of ensuring the "Digital Sovereignty" of the States (Workshop – Round table № 5);
- Proposals on new IISRC projects in the sphere of international information security (Sixteenth scientific conference of the IISRC).

2. In the course of the Workshop – Round table № 1 the participants have discussed the following issues:

- Issues of international cooperation with regard to the development of the Digital Economy.
- Digitization of the economy and ensuring of Information Security.

Following the results of the discussions the experts concluded that there is no alternative to the development of the Digital Economy. It has a great investment potential, but the investors vaguely understand the threats to Information Security and are not ready to fund its maintenance.

3. In the course of the Workshop – Round table № 2 the participants have discussed the following issues:

- Recent initiatives of Private Business in the field of ensuring the security of Critical Information Infrastructure. How could we unite our efforts?
- The practice of regulatory and legal management of issues of ensuring Information Security, including the exchange of best practices in building frameworks for interaction between CERTs with different forms of ownership and in different jurisdictions.
- Monopolism of suppliers of IT-systems and solutions in the field of information security in

certain areas: issues, threats and challenges. Protection of domestic markets vs freedom of trade and entrepreneurship.

The experts have thoroughly discussed the state of development of the Public-Private Partnership in various countries on ensuring Security of the Critical Information Infrastructure. Despite marking some recent progress in this field, at the same time it has been noted that the measures taken are significantly lagging behind the qualitative and quantitative development of Cyberthreats. In particular, the participants have noted some issues of allocation of the roles between the State and Business in ensuring the Security of the Critical Information Infrastructure. In this regard, all experts have supported the initiatives of MMC Norilsk Nickel and Microsoft Corporation described in The Charter for Information security of critical industrial facilities and the Digital Geneva Convention.

4. In the course of the Workshop – Round table № 3 the participants have discussed the following issues:

- Quantitative and qualitative expansion of ICT threats in the politico-military sphere.
- Possible measures to counter or limit the dangerous activities in the information space.
- Defining measures for confidence building and deterrence to avoid the accidental escalation of conflict in cyberspace

The experts have agreed that it is necessary to continue the discussions in the framework of Garmisch-process on countering the use of ICTs for malicious military-political purposes – giving the priority to Cyberwar prevention measures. Following the results of the discussions the experts also concluded that:

- the issues of application of International Law for prevention of conflicts in cyberspace remain relevant; the most complex among them are:

the issue of attribution, the issue of recording of legal facts of malicious use of ICTs and the issue of determining of the causal link between a Cyberincident and the possible consequences of its implementation;

- malicious use of ICTs can become an influencing factor of Strategic Stability.

5. In the course of the Workshop – Round table № 4 the participants have discussed the following issues:

- What issues of ambiguous interpretation and applicability have been identified in the specific articles of the rules included in the 2015 GGE report?
- Is it possible to develop a Manual on application of the rules, mentioned in p.1?

Following the results of the discussions the experts have concluded that in the current situation of an accelerated mass development of Cyberspace by various actors – to leave it without rules would mean to create chaos with unpredictable consequences. The only feasible foundation for such rules can be the «Norms, rules and principles for the responsible behavior of States» included in the UN GGE Report of 2015. In this regard the efforts of the expert community should be directed towards the development of coordinated procedures and frameworks of implementation of the said Rules, without waiting for the consolidation of their final revision at the UN level.

6. In the course of the Workshop – Round table № 5 the participants have discussed the following issues:

- How to ensure the regime of the “digital border”? (what is a regime and what are its main functions; technological issues and possible technological solutions; economy of the border).
- How to come to an agreement on the “digital border”? (arrangement conditions; subject of a

border arrangement; subject of a border regime arrangement).

- Digital space and the borders in the future. (BGP, SDN, IPv6; geographical distribution of addresses and geographical routing; address as an attribute for the border regime (passport/visa); identification of the data flows and their management).

Following the results of the discussions the experts have concluded that from the technological standpoint it is possible to draw a «digital boundary». From the standpoint of ensuring «digital sovereignty» of the States there remain issues of political and legal nature: decision-making on the expediency of establishing a «digital boundary» regime and the issue of granting it an international-legal status in any form (unilateral act, bilateral or multilateral agreement).

7. At the Sixteenth scientific conference of IISRC, the participants, taking into consideration the outcome of the Workshop - Round table № 4, have discussed the questions pertaining the organization of work on the new IISRC Project on application of the rules of responsible behavior of the States in the ICT-environment. It has been decided to form a directorate of the Project comprising as follows:

- Anatoly Streltsov, Institute of Information Security Issues at Lomonosov Moscow State University, Russia;
- Andreas Kuehn, East-West Institute, US;
- Eneken Tikk, Cyber Policy Institute, Estonia;
- Nohyoung Park, Cyber Law Centre at Korea University, Republic of Korea;
- Daniel Stauffacher, ICT4Peace Foundation, Switzerland.

IISRC Conferences

Germany, Apr. 2010

Russia, Oct. 2010

Germany, Apr. 2011

China, Oct. 2011

Germany, Apr. 2012

Bulgaria, Oct. 2012

Germany, Apr. 2013

Azerbaijan, Oct. 2013

Germany, Apr. 2014

Kazakhstan, Oct. 2014

Germany, Apr. 2015

Republic of Korea, Nov. 2015

Germany, Apr. 2016

Germany, Apr. 2017

Russia, Dec. 2017

Germany, Apr. 2018

Russia, Dec. 2018