Cyber as a new aspect of the global diplomacy in the sphere of nuclear nonproliferation and arms control

Dr. Elena Chernenko

Editor of the Foreign Desk of the Kommersant newspaper, member of the Board of the PIR Center

Where are we on cyber?

- Cyber security used to be a non issue for politicians and diplomats just a few years ago
- Turning points: Estonia, Stuxnet, Arabic Spring, Snowden
- Global discussions on cyber today comparable to the early 1960-s NPT efforts?

Links between cyber and nuclear

- Security of information networks of critical infrastructure incl. nuclear power stations
- Link between cyber threats and counter-attack options of countries incl. nuclear response
- Use of existing nuclear security infrastructure for cooperation on cyber (**Nuclear Risk Reduction Centers of Russia and US**)
- Initiatives to use cyber tools for non-proliferation purposes

Main differences between global players

Cyber security vs. International information story (protection of data and networks vs. control of content)

- Compromise: Security of the information and communication technologies and of their **USE** (first put on paper in the agreement between Russia and the US in 2013)

RF-US agreement on cyber 2013

- To create a mechanism for information sharing in order to better protect critical information systems, a communication channel and information sharing arrangements between Russia and US computer emergency response teams (CERT) was established

- To facilitate the exchange of urgent communications that can reduce the risk of misperception, escalation and conflict, the use of the direct communications link between the Russian-American **Nuclear Risk Reduction Centers** was authorized

- Officials in the Kremlin and the White House established a direct communication link between high-level officials to manage potentially dangerous situations arising from events that may carry security threats to or in the use of ICTs.

Other agreements

- OSCE confidence building measures (Dec 2013)
- NATO Wales summit decisions (Sept 2014)
- Russia – China (May 2015)
- United Nations Group of Government Experts (UN GGE) report (July 2015) – first steps to a code of conduct

United Nations Group of Government Experts (UN GGE) report

- Warns against inflicting damage on each others' critical infrastructure
- Prohibits knowingly allowing third party illegal cyber activity from a state's territory
- Assumes a duty to assist in the investigation of cyber attacks and cybercrimes launched from a country's territory
- Commitment to investigate thoroughly cyber attacks before pointing the finger at a culprit
- Warns against compromising ICT products with exploits and backdoors ("harmful hidden functions")

- Main weak points: voluntary non-binding norms, which are not enough specified

A cyber NPT or arms control treaty?

- Verification mechanism?
- Attribution?
- Not enough political will?

What then?

Thank you for your attention!

Dr. Elena Chernenko
chernenko@kommersant.ru
007 925 226 06 62