ПИР-ЦЕНТР
Центр политических
исследований России

The Challenge for Cyber-Security:
Prospects for Global Internet Governance?

Michael Yakushev
PIR Center, Moscow (Russia)

Scope

- Terminological conflict: *Cyber-Security*, *Internet Governance* etc.
- Legal conflict (gap): lack of globally recognized legal instruments
- Organizational conflict: ICANN vs ITU
- (potential) Political/Military conflict: cyber-warfare

- 2013: Snowden case: what's new

Terminology

- Global understanding: *Cyber-Security, security of the Internet, security of the cyberspace*
- Russian interpretation: “trinity” of
  - (Inter)National Security (e.g. preventing cyber-wars)
  - Public Security (e.g. combating cyber-terrorism and “*cyber-extremism*”)
  - Private Security (e.g. countering cyber-crime)
- Russian terminology: *International Information Security*
- Compromise (Obama-Putin Joint Statement, 2013): *issues of threats to or in the use of ICTs in the context of international security*
  - ICT stands for *Information and Communication Technologies*

Internet Governance & *Multistakeholder Approach*

- Working Group of Internet Governance (Final Report, 2005):

The development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.

- New Stakeholders: technical community, academia, international organizations

Legal Framework

- No globally recognized international treaty on global cyber-security or internet governance
- *Budapest Convention on Cybercrime* (2001), Council of Europe
  - Non-European countries participate (including U.S.A.)
  - Russian concerns on Art. 32 (B)
- Proposals of the Russian Federation on the *Concept of the U.N. Convention of the International Information Security* (2010-2012)
- Council of Europe Governing Principles (2011) as possible common platform for interaction

Who should govern cyber-security issues?

- Highly politicized issue (broader understanding of cyber-security, including freedom of speech, ‘cyber-extremism’ etc.)
- Dubai World Conference on Telecommunications (2012): only 89 of 152 countries signed the new version of the International Telecommunication Regulation
- Internet is a multi-layer network, substantially with different level of regulatory framework: physical lines, communications channels, core DNS servers, IP-addresses, DNS, applications etc.
  - No technological grounds for ITU vs ICANN conflict

Cyber-warfare

- Exists in reality
  - Sometimes the negative consequences may be caused not by software tools (Armenian case 2010)
- Known cases not confirmed (globally recognized): attribution issue (Estonian case 2007)
- Cyber Commands being created throughout the world
- Non-proliferation of cyber-warfare needed (if possible?)

Snowden case (2013)

- 1. Whether what Snowden revealed (=NSA surveillance), *is a 'bug' or the 'feature'* of the current Internet Governance System?
  - +how it affects the state of the global cyber-security?
- 2. If the 'bug' -> than it has nothing to see with the real regulatory system of the current Internet, and it should be solved on domestic (violation of privacy laws) and international (diplomatic level)
- 3. If the 'feature' -> new framework of Internet Governance should be developed to guarantee the stability and security of the cyberspace

New topics for consideration

- Identification of the Internet users and network resources owners
  - Attribution of the illegal acts in the cyberspace
  - US concepts on Trusted Identities (=> may be discussed globally)
- Electronic payments
  - Anti-money laundering, combating cybercrime and cyber terrorism
- Social networks regulation
  - Population of Facebook ‘citizens’ is the third ‘country’ of the world, after China and India
    - (>1 b users)

Conclusions

- 1. International Treaty on Cyber Security (and/or Internet Governance) may be our common objective by 2015-2016
  - Unified terminology
  - Governing principles
  - identity, e-Payments, social networks, privacy
- 2. Non-proliferation of Cyber-Warfare is now in the international political agenda
- 3. Multistakeholder approach should be a basis for any solution in the field of global cyber-security

Any questions?

- Thank you for your attention!

- *e-mail: m.yakushev@gmail.com*
- *http: www.pircenter.org/en/*