Cyber defense capacity building Republic of Macedonia

Ljubica Pendaroska

Ohrid, August 2015

A few starting points

- Cyberspace presents new opportunities and challenges for states and the international community, while creating policies in different areas of social life.

- Public and private organizations openly acknowledge cyber attacks are one of the most prevalent and high impact risks they face with!

- The threats from cyber adversaries are continuing to grow in scale and sophistication.

- Staying protected against cyber-security threats requires all users, ranging from children and their parents to the most sophisticated users, to be aware of the risks and improve their security practices on an ongoing basis.

- Undeniable fact > cyberspace is not a “law-free” zone where anyone can conduct hostile activities without rules or restraint.

- International Law principles do apply in cyberspace (but, not a universal view in the world!)

✓ Everyone should be able to access the Internet and to an unhindered flow of information

✓ The importance of all stakeholders in the Internet governance model

✓ A shared responsibility between all relevant actors to ensure security (public authorities, the private sector, individuals)

As an illustration

- By completing the Digital Single Market, Europe could boost its GDP by almost 500 billion euros a year

- A 2013 Eurobarometer survey showed that almost a third of Europeans are not confident in their ability to use the internet for banking or purchases.

- Across the EU, more than one in ten Internet users has already become victim of online fraud.

In his Article, Jason Saul argued that

…"fifty-one of the world's one hundred largest "economies" are now corporations."

He also compared that:

"in 2007, Finland's budget was about 40 billion euros, 20 percent less than Nokia's annual sales.

Redefinition of power

Similarly, Al Gore argued that:

… "More money is allocated by markets around the world in one hour than by all the governments on the planet in a full year"

Al Gore

As a result:

MODERN THREATS ARE HYBRID:

some states, terrorists, criminals, insurgents, religious extremists

ONLY A FEW SECURITY CONCEPTS COULD PARTIALLY BE APPLIED TO COUNTER THEM

Process of Globalization

Fall of the Berlin Wall

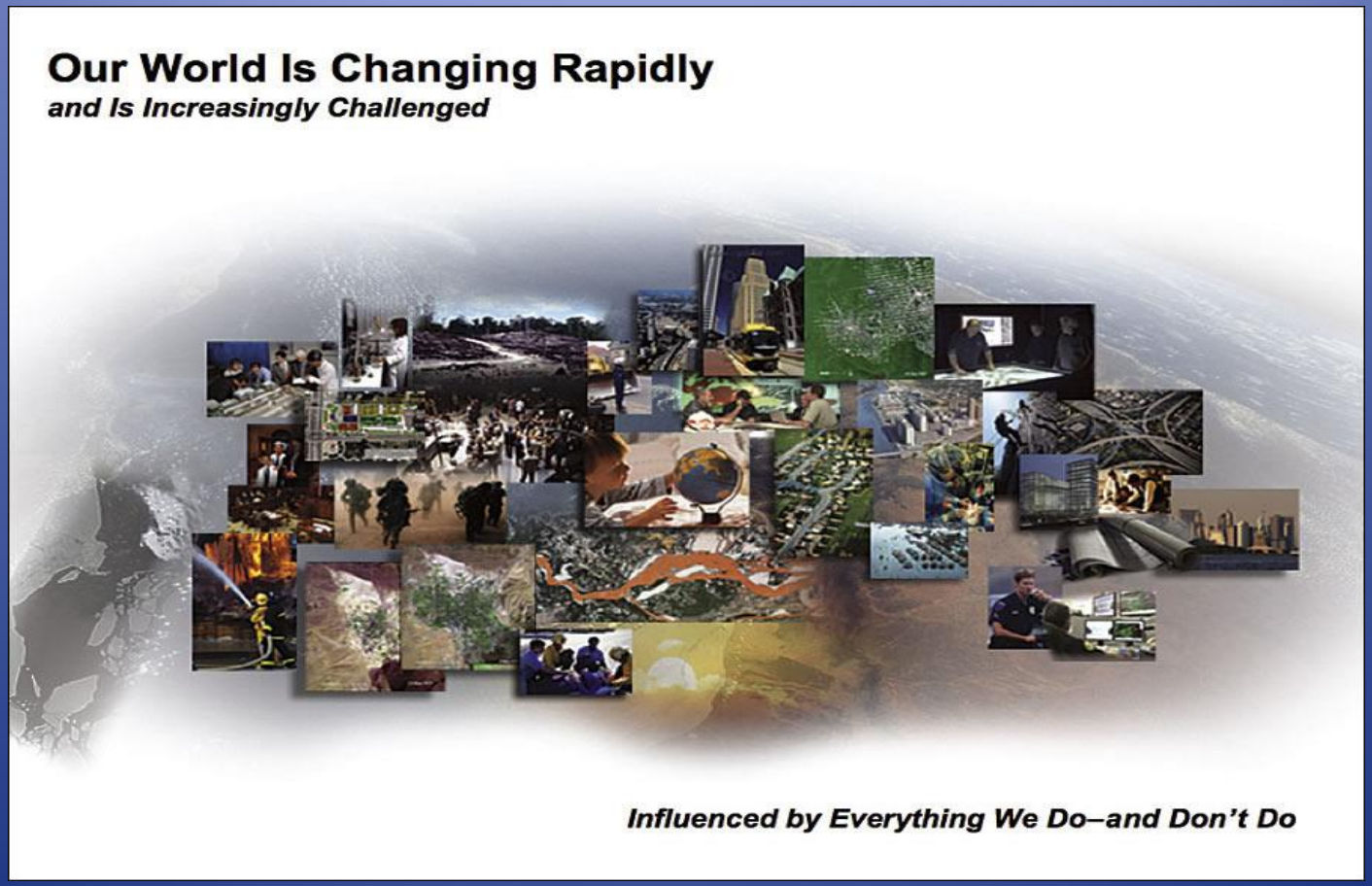
+

Technological development

Process of Globalization

+

Technologica development



Side effects…

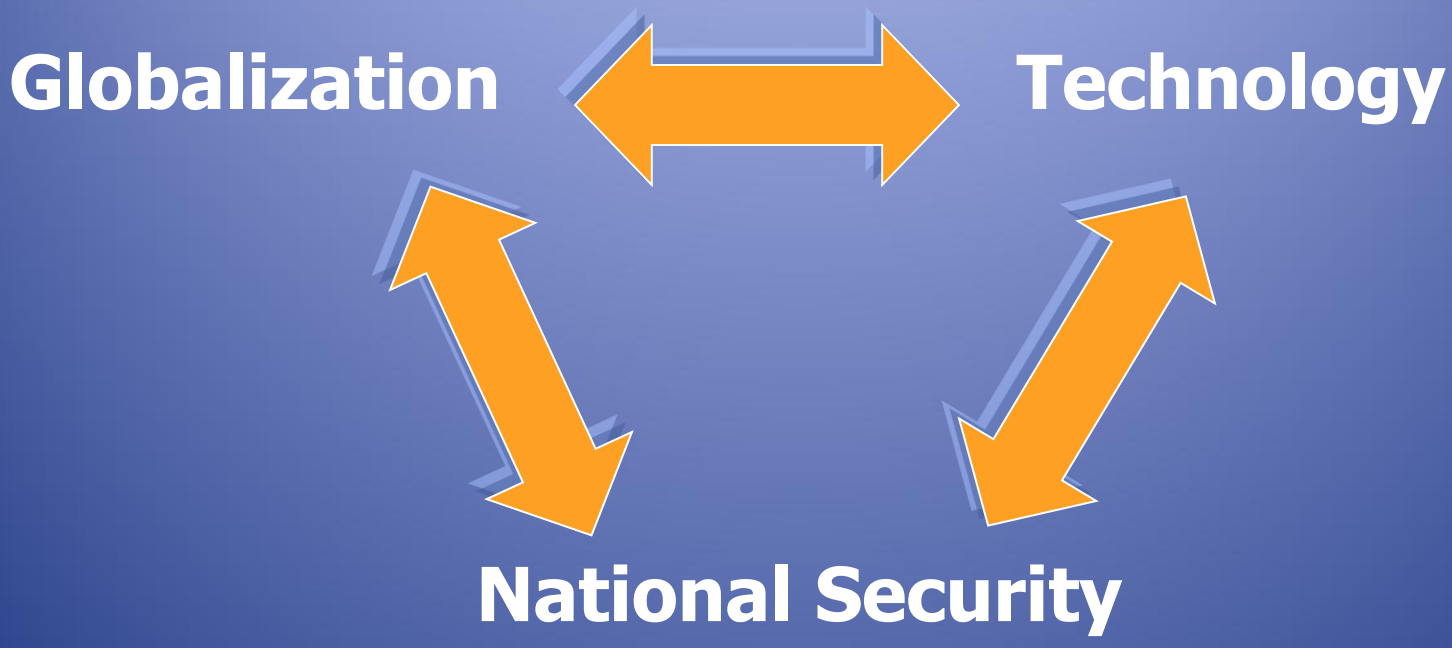
Governments lost the monopoly of power…

Rise of the private actors and corporate economy…

Networks of systems and services…

Improved communications: internet and digitalization

Global cyber security trends and Macedonia



Globalization and technology-double edge sword?

Global cyber security trends and Macedonia

Relevance for Macedonia

As the rest of the World, Macedonia is facing "paradox of modernity"

…The more we depend on internet and modern technology the more vulnerable we are…

Global cyber security trends and Macedonia

Influence for Macedonia

Geographical position

Euro-Atlantic aspirations

political and security dynamics

Cyber defense - Background

Macedonian society - phenomenal growth of the communications networks and information systems

In 2014:

- 68.3% of the households have internet access
- 93% of enterprises with 10 or more employees have internet access
- Internet connectivity via mobile broadband connection is growing too, at a pace of 4% as compared to 2013

- ICT have become the country's backbone of the finance, economy, energy, health, transport sectors

- National program "E-Macedonia", e-education, e-citizens, e-business, e-government and Information Security, developed by the Ministry of Information Society (since late 2009)

- Macedonian Cyber defense system must include:

Relevant National Legal Framework +

Adequate Institutional Infrastructure +

National Cybersecurity Strategy

Relevant Legal Framework

First steps >

In 2004 the Macedonian Parliament ratified the CoE Convention on Cybercrime;

In November 2005 Macedonia ratified an Additional Protocol to the Convention

Current Cyber area legal framework:

- Criminal Code
- Law on Criminal Procedure
- Law on defense
- Law on Electronic Communications
- Law on Communications Monitoring
- Law on E-Commerce
- Law on Electronic Management
- Code of Civil Procedure
- Law on Electronic Data Form and Electronic Signature
- Law on Personal Data Protection
- Law on Free Access to Public communications

Additional strategic security documents – defining the roles of various responsible actors

For example, as regards cybersecurity, crisis management system, include:

- The Ministry of interior
- The Ministry of defense
- The Protection and Rescue Directorate
- The Crisis Management Centre
- The Ministry of Transport and Communication
- The Directorate for Protection of Classified Information
- The Ministry of Environment and Spatial Planning

Institutional Infrastructure

- There have been discussions about the establishment of National bodies for dealing with cyber space issues:

Computer Incident Response Team (CIRT)

&

Computer Emergency Response Team (CERT) (since 2012)

Team of experts in information security, to act as:

- A point of Coordination: Monitoring, Identification, Warning and Determining answers to computer incidents
- To take proactive measures: to prevent or mitigate the consequences of possible damages (continuous monitoring and issuing security alerts; dissemination of relevant information; raising public awareness of the importance of information security)

- To undertake reactive measures for managing computer incidents (coordination of dealing with major computer incidents; collection, precession, preparation and distribution of security recommendations for information system vulnerabilities)
- Provider of support for building a national information security culture and raising awareness among citizens

- Idea to form the MKD-CIRT as part of the Agency for Electronic Communications

❖ No Team has been formed till today!

National Cybersecurity Strategy

- Macedonia does not have Cybersecurity Strategy!

- An assessment study for preparation of a National Cybersecurity Strategy is in progress – by a Working group consisted of members from the Ministry of Interior, Ministry of Information Society, Ministry of Health, Ministry of Defence and Ministry of Education (proposed and financed by the United Nations Development Programme)

The National Cybersecurity Strategy will cover 4 segments:

- ✓ Developing and promoting the cyber defense concept
- ✓ Measures and activities for cybercrime suppression
- ✓ Establishing and improving a system for preventing cyber attacks
- ✓ Managing incidents caused by cybercrime

Few concluding remarks

- The establishment of overall cyber defense system is progressing, but it has been slow, non-transparent and without significant results so far.
- Important reforms for aligning the national framework with the EU's and NATO's policy have been initiated, such as the adaptation of the legal and policy framework for cybersecurity, the establishment of a national corresponding body and the development of a National cybersecurity Strategy.

Recommendations

Macedonia's cybersecurity system needs measures for fostering research and development, investments and innovation

(establishment of Cybersecurity Innovation Centre)

- ✓ There is a need of capacity building measures for the defense sector (for instance, definitions on cyber resilience, cyber-enabled terrorism, hybrid war, cyber-warfare
- ✓ There is a need of introducing and developing a cybersecurity culture, followed by educational campaigns and raising public awareness
- ✓ We have to think towards securing and protecting cyber space more at a regional scale