EU-US JOINT OPEN WORKSHOP ON CYBER SECURITY OF ICS AND SMART GRIDS

Importance of the EU-US cooperation and
the need of having a coordinated global response

Dr. Adrian SEVERIN (MEP)

Cyber world and culture

Characteristics of cyber civilization

Global contact

Rise of two different worlds

De-personalized users

The real world

Merger through consistent regulation

The cyber world

Undeniable universal right to access, use and communicate through the cyber network

Global Digital Infrastructure

GDI

Interconnectivity that has improved our daily lives, the way we work, play, interact and communicate

Innovation, economic development and worldwide social interaction

Tolerance and respect for diversity

Identity wars

Threat Environment

Global new threat environment

Borderless nature of the targeted systems

Capacity to use or to neutralize them available to anyone

National Governments

Mitigating attacks needs international cooperation

Strong Public Private construct

Field of their protection

Cooperation

Field of their development

Limitations vs. Openness

Regulations, laws ➡ **Exploited** in order to limit civil liberties

The Internet **has been able to flourish due to**

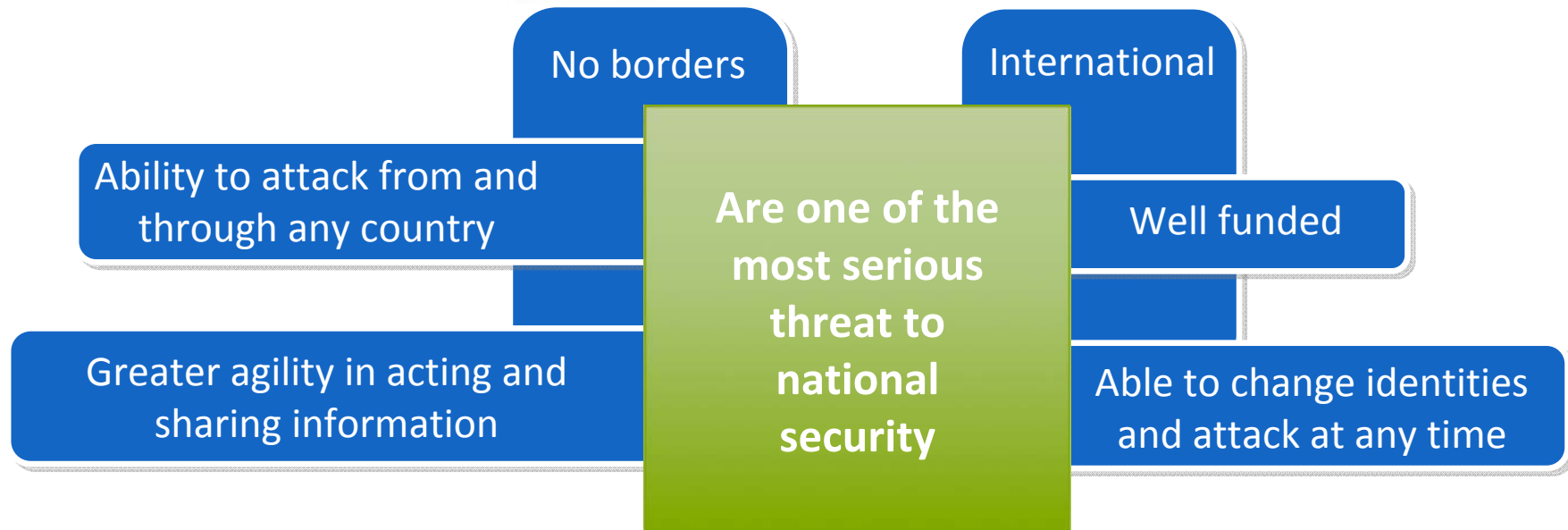1. **Openness** ⬅➡ **2. Lack of centralized control**

Equilibrium between security and liberty needed

Source and Nature of Cyber threats

private ← **Criminals** → public

Objectives

Steal considerable amounts of money

Unlawfully use intellectual property

Disrupt businesses

Spread fear

Challenge governments

Common characteristic: uncertainty of the identity of the attacker

Cyber criminals

No borders

International

Ability to attack from and through any country

Well funded

Are one of the most serious threat to national security

Greater agility in acting and sharing information

Able to change identities and attack at any time

Needed

1. Global strategic reaction

2. Transnational coordinated effort

3. Harmonized legal frames

4. Common anti cybercrime policies

Cyber terrorism

Absolute efficiency in stopping cyber terrorism = Dramatic limitation of the online individual freedoms based on national security concerns

Hacktivism not an alternative as a term

Fails to acknowledge the massive disruptive effects of such attacks

Keeping a balance between civil liberties

Labeling crucial

Fulfillment of security needs

Consistent in EU and US

Cyber war

Governments are walking into an **unknown territory regarding the following questions**

Could a cyber attack be seen as a *casus feoderis* in the meaning of article 5 of the Washington Treaty

Relevant to launch a conventional attack

Bilateral or multilateral obligations triggered

Technologic defensive is not enough

Transnational legal systems → Indispensable ← Deterring and retaliating joint capabilities

Global regulation needed to consolidating global security in an era of new weaponry

Transatlantic relation

The challenge → **<u>Uncertainty of shift from a bipolar to a multipolar world</u>**

EU and US have same strategic global:

concerns ↔ objectives

EU-US relationship will endure and must get stronger as new challenges arise

EU-US cooperation

| Imposed by necessity | ← | The EU-US cooperation in the field of cyber security | → | Test for the sustainability and effectiveness of the transatlantic relation |

Legislators need to

| 1. Support the development of industry initiatives | 2. Cultivate information sharing capabilities | 3. Improve communication between local, state and national public sector agencies | 4. Promote voluntary bilateral sharing between industry and government |

Legislative developments

EU

European Commission has launched a consultation on the issue of improving network and information security in the EU

EP AFET committee is working on a draft report on Cyber Security and Defense

US

Cyber security bill proposal, blocked in the US Senate, due to the failure of striking a balance between:

1. Regulating the private sector

2. Encouraging companies to increase security measures

Rumored draft executive order aimed at creating a voluntary program of protecting the critical infrastructure such as energy, water, finance and transport

Data protection and privacy

What is personal data?

Who owns it?

Need to address the issue of **security, data protection and privacy**

Who is allowed to process it?

What happens if personal details regarding one's usage of health services, driving patterns, electricity consumption etc, are just made public to the whole world to see due to an intrusion in the network?

Conclusions

Users need **re-assurances** that they will safely use the new services and applications

EU and US should put in place → Rules and agreements to keep the cyber world running → Developed at a global level

The biggest threats to the future of the Internet are related with

Privacy

Censorship

Cyber attacks

Thank you for your attention