International Intergovernmental High Level Panel PROTECTING CRITICAL INFRASTRUCTURE FROM CYBER ATTACKS: A GLOBAL CHALLENGE February 14, 2017 Vienna, Austria

This International Intergovernmental High Level Panel is co-organized with the Federal Ministry for Europe,

Integration and Foreign Affairs of Austria, the Federal Ministry of Defence and Sports of Austria, the AIT Austrian Institute of Technology, the CSP Austrian Cybersecurity Platform and the EnergyPact Foundation and hosted by the Federal Ministry of Defence and Sports.

"The greatest cyber risk is a catastrophic attack on the energy infrastructure. We are not prepared for that".

These were the words of former chief of the US National Security Agency (NSA) General Keith Alexander. The energy infrastructure consists of all elements of energy production, transmission, distribution, and end use. This details a complex network of interdependent element owned by the government and commercial sector that are often not limited or bound by national borders. Such infrastructure if subject to a cyberattack could have cascading impact nationally, but also internationally.

Cyber exploitation and cyberattack have become a tool of crime, terrorism, and international conflict. Attack trends show an increase in attacker sophistication and an increased capacity of cyberattacks to do physical damage. Additionally the number of potential adversaries gaining cyber skills continues to grow.

Greater international dialogue is needed to address cyberspace and the growing risk that cyberattacks pose to national critical infrastructure. Natural disasters and grid failures have illustrated the socioeconomic effect of a large and sustained loss of electrical power. Imagine now the catastrophic impact of a malicious and strategic attack against the same energy infrastructure. States must engage in confidence building activities and open discussion to minimize the risk of occurrence and potential impact of cyberattacks against critical infrastructure.

Session 1

Austrian/EU Cyber Security Strategy for Critical Infrastructure Protection

Information and communications technology has become the backbone of our economic growth and is a critical resource which all critical infrastructure sectors rely on. National and international strategies must be developed to support the security and resilience of these sectors against cyberattack. An integrated cyber security strategy must place emphasis on tasksharing between multiple stakeholders including the State, industry, academia and the civil society. The strategy should address measures relating to: political strategic management, education and training, risk assessment, prevention and preparedness, recognition and response, limitation of effects and restoration as well as the development of governmental and nongovernmental capabilities and capacities.

This session provides discussion on the Austrian and EU Security Strategy for critical infrastructure protection. Key issues to be explored include:

- Context and goals of the Austrian Cybersecurity strategy
- Role of public private partnerships in implementation of cybersecurity strategy
- International alignment and dialogue

Session 2

Impact of cyberattacks and suitable strategies for enhancing cyber resilience

Critical infrastructure is composed of complex network of stakeholders that include government authorities, business investors, facility operators, technology providers, technical support organizations, and contracted parties. Stakeholders often additionally exist across international boundaries. System complexity and interdependent relationships can lead to cascading impact and far reaching consequence in a cyberattack against critical infrastructure. Greater understandability of the impact of cyberattack must be gained to support the development of mitigation and resilience strategies. This session provides discussion on:

- Possible effects of cyber attacks and their societal and economic impacts
- Strategies of critical infrastructure providers for cyber protection
- Contribution of science and technology for increasing cyber protection

Session 3

The role of cyber awareness and dialogue in safeguarding critical infrastructures

Ensuring cybersecurity is a common responsibility which encompasses multiple levels of stakeholders. A failure of any stakeholder could result in tremendous adverse impact across an entire industry and State. Unfortunately human error is a major contributor the cyber security incidents. Awareness of the threat, the risk and the roles and responsibilities of each stakeholder is a necessary element of cyber security. End users play a crucial role in ensuring the security of networks, information systems, and industrial control systems: they need to be made aware of the risks they face and be empowered to take simple steps to guard against them.

This session provides discussion on:

- The human factor in cyber preparedness
- The value of dialogue and information
- Building the necessary human resources and capabilities for increased cyber resilience

List of invited countries

Algeria, Brazil, China, the European Union, France, Germany, India, Indonesia, Iran, Italy, Japan, Nigeria, the Russian Federation, the Republic of Korea, the UAE, the UK and the USA