As delivered

Statement by the Permanent Representative of Slovakia to the United Nations, Ambassador František Ružička in the Open Debate of the UN Security Council on Threats to international peace and security caused by terrorist acts: protection of critical infrastructure (13 February 2017)

Mr. President,

I wish to thank you for holding this debate on the protection of critical infrastructure against terrorist attacks and on promoting discussion on preventive measures against such attacks.

In this context I would like to recall the outcome of the Arria-formula meeting on cybersecurity and international peace and security organized by Spain and Senegal in November 2016.

As the threat landscape changes - becomes more complex - so must *change our approach to security problems* in the face of asymmetric and cross-border threats. As such they must be confronted at both - a national and international level.

No country is immune to cyber terrorism threats. Including mine. Slovakia adopted its national strategy to combat terrorism, set on four key pillars, in line with the objectives of the EU Action Plan on combating terrorism: *prevention, protection, prosecution and response.*

Mr. President,

The threats of major disruptions of critical infrastructure to economy and national security are real. These threats can be classified into 3 categories: (1) natural, (2) human-caused, and (3) accidental or technical threats.

Although reducing the vulnerabilities of critical infrastructure and increasing their resilience is the responsibility of individual state, *need for international cooperation appears to grow rapidly.*

Mr. President

As has been mentioned, cyber threats and attacks are becoming more common, sophisticated and harmful to states as we depend more and more on computer-communications systems.

At present cyberterrorist attacks are generally considered as a relatively low risk posed to States. But we are reminded, that despite the fact that *cyber-attacks occur with greater frequency and intensity around the world*, many either go unreported or are under-reported, leaving the public with a false sense of security about the threat.

While governments, businesses and individuals are all being targeted on an exponential basis, *infrastructure is becoming a target of choice among both individual and state-sponsored cyber-attackers*, who recognize the value of disrupting what were previously thought of as impenetrable security systems.

Many countries around this distinguished table have already dealt with this kind of attack in the recent past. According to Dell's 2015 Annual Security Report, *cyber-attacks against Supervisory Control and Data Acquisition Systems doubled in 2014*, to more than 160,000.

Today, according to Interpol *malicious code can potentially be used to manipulate the controls* of power grids, financial services, energy providers, defence, healthcare databases and other critical infrastructure, resulting in real-world catastrophic physical damage, such as blackouts or disruptions to an entire city's water supply.

Action is necessary. Some studies suggest following measures to be taken to improve Critical Infrastructure Protection:

- *Assess Critical Infrastructure vulnerabilities* to cyber or physical attacks.
- *Develop plans to eliminate* significant vulnerabilities.
- Propose systems for *identifying and preventing attempted major attacks*.
- Develop *plans for alerting,* containing and rebuffing attacks in progress.
- Rapidly reconstitute *minimum essential capabilities* in the aftermath of an attack.

It cannot be excluded in the future that the use of cyberspace by state or non-state actors may amount to a threat to international peace and security and *will require the Security Council to take more decisive steps to respond.*

As has been stated by the Secretary-General in the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security in 2015 (A/70/174): *"Making cyberspace stable and secure can only be achieved through international cooperation, and the foundation of this cooperation must be international law and the principles of the UN Charter"*.

But international treaties intended to address the problem have *so far limited impact* because of (1) the inability to hold signatories accountable and (2) the difficulty associated with accurately determining the identity of responsible actors.

(1) Enhanced information sharing combined with a (2) mandate to swiftly and accurately release information regarding attacks to impacted citizens, provide a sensible foundation for (3) designing a protocol to effectively address future attacks may help - *yet very few governments routinely engage in this practice.*

The United Nations Global Counter-Terrorism Strategy (A/RES/60/288) calls on Member States:

To step up all *efforts to improve the security and* protection of particularly vulnerable targets, while recognizing that States may require assistance to this effect.

To work with Member States and relevant international, regional and sub-regional organizations to identify and share best practices to prevent terrorist attacks on particularly vulnerable targets.

Recognizes the *importance of developing* public-private partnerships in this area.

In this respect I would like to underline the following (5) points:

- *To support States with practical assistance in the implementation* of the provisions of the UN Global Counter-Terrorism Strategy;
- *To establish appropriate mechanisms to facilitate enhanced sharing of best practices;*
- *To strengthen the capacity of both public and private sectors* and to increase the development of public and private partnerships, including by promoting awareness and understanding of the *necessary balance between economic and security issues,* in order to ensure an adequate level of protection and limit the detrimental effects of disruption on the society and citizens.
- *Anti-Money Laundering/Combating the Financing of Terrorism* should remain a key priority;
- Security Council should consider to make *better use of the CTITF* (Counter-terrorism Implementation Task Force) Working Group on the Protection of Critical Infrastructure including vulnerable targets, internet and tourism security.

Mr. President,

Terrorism poses threat not only to our security, but also to values, rights and freedoms of our societies and their citizens. My country is committed to play its part in the regional and global efforts to fight terrorism and violent extremism in all fronts – including protection of critical infrastructure.