Side Event

Protection of critical infrastructure against terrorist attacks
in the context of implementation of UN SC Resolution 2341 (2017)

Tuesday, 26 June 2018, 13:15, Conference Room 9, UNHQ

Background note


1) In recent decade, the terrorist threat has grown at an exponential rate. Terrorists endanger public security, threaten state organs and undermine public confidence in security institutions. Their attacks result in civilian casualties, large-scale damage and loss of property, disrupt proper work of public infrastructure, and bring chaos in the social order (society), and may cause highly diverse environmental consequences as well as significantly undermine national defence capabilities.

2) Objects of critical infrastructure have long been attractive targets for terrorist groups. They have to be protected against a growing number of diverse threats, both physical and cyber.

3) Working Paper encourages exploring ways to assess vulnerabilities, interdependencies, capabilities, and cascading effects of impact of terrorist attacks on critical infrastructure, as well as to consider Ukraine’s experience on possible preventive measures as an example to follow while developing national strategies and policies in this field.

- Protection of Critical Infrastructure against Subversions and Terrorist Attacks

1) In light of violations of international law as well as changing of geopolitical and geo-economic relations the protection of national security and critical infrastructure becomes a top priority. The emerging threats are becoming increasingly multifaceted and complex, with a major objective to create the so-called “cascading effect” on the areas of finances, energy and transportation, that can entail partial or complete termination of life-support systems’ operations. The ongoing foreign military aggression has turned Ukraine into a testing ground for the advanced hybrid warfare technologies that encompass subversive, economic, social, diplomatic, political and informational tools. Moreover, the modern intervention tactics in various combinations affect other countries across the world.

2) Critical infrastructure is highly vulnerable to subversions and terrorist attacks. Increasing threats to life-support systems stemming from hybrid aggression require effective countermeasures and deepened international cooperation.

3) It is important to implement consolidated approach on protection of critical infrastructure from subversions and terrorist attacks; to improve resistance of Member States’ security systems against hybrid challenges and threats; to develop preventive measures and enhanced response mechanisms to the attacks against important life-support facilities; to promote interoperability and cooperation in order to maintain international security.
Cyber-attacks against Critical Infrastructure Facilities as an Element of Russia's Hybrid War against Ukraine

(1) Influence operations and cyber influence efforts targeting the Ukrainian statehood that are orchestrated by Russian intelligence agencies are the key elements of the Russian hybrid warfare against Ukraine.

(2) The Security Service of Ukraine is among the primary state actors responsible for fighting Russian aggression in information and cyberspace. Coordinated international efforts contributed to mitigation of the Russian destructive acts as well as prevented a series of cyber attacks against Government critical infrastructure.

(3) Cyber attacks (BlackEnergy, Petya, WannaCry, etc.) along with international terrorism are currently among the key global challenges as they affect both regional and international security, thus requiring a consolidated response.