A/RES/70/237 Developments in the field of information and telecommunications in the context of international security

a) General Appreciation of the issues of information security

Information and Communication Technologies (ICT) have become an indispensable driver of social, economic, and political activities. Switzerland is committed to seize the opportunities that are generated by the use of ICT. Switzerland takes account of the new developments and challenges in relation to ICT.

However, the use of ICT has exposed information and communication infrastructure to criminal, intelligence, politico-military or terrorist abuse of functional impairment. Disturbances, manipulation and specific attacks carried out via electronic networks are the risks that an information society entails. Against this background, states have become increasingly engaged in a series of regional and international policy discussions and debates over “cyber security”. This engagement is generated from a growing sense of insecurity regarding vulnerabilities in computer systems and related technologies and how they can be exploited for malicious purposes.

Even though vulnerabilities and threats in this environment have been recorded since the 1980s, it was not until the past seven years that threats and vulnerabilities stemming from the use of ICT were put on the national security agenda. As a result, the Swiss Federal Government set up an expert group in 2010 in order to scrutinize the risks and to increase the national capacity to respond to these threats and vulnerabilities.

Switzerland’s functioning as a holistic system depends on a growing number of mutually networked information and communication facilities (computers and networks). This infrastructure is vulnerable. Country-wide or long-lasting disruptions and attacks could have severe adverse effects for Switzerland’s technical, economic and administrative performance. Such attacks can be launched by a variety of perpetrators and have various motives: individual perpetrators, political activists, criminal organisations intent on fraud or blackmail, terrorists or state spies who want to disrupt and destabilise the state and society. ICT are particularly attractive as targets not only because they offer many possibilities for abuse, manipulation and damage, but also because they can be used anonymously and with little effort. Protecting information and communication infrastructure from such disturbances and attacks is in Switzerland’s national interest.
b) Efforts taken at the national level to strengthen information security and to promote international cooperation in this field.

On 27 June 2012, the Swiss Federal Government adopted the national strategy for the protection of Switzerland against cyber risks (NCS), thereby laying the foundation for a comprehensive, integrated and holistic approach to tackling cyber risks. The strategy seeks to improve the early detection of cyber risks and emerging threats, make Swiss infrastructure more resilient to cyber attacks and generally reduce cyber risks. The main focus lies on cyber crime, espionage and sabotage. The underlying rational of the strategy is the need for a cyber security culture, shared responsibility and the need for a risk-based approach. It advocates a stronger coordination at the governmental level, fosters the private-public partnership and an enhanced cooperation at the international arena.

The strategy comprises a set of 16 measures, which should be put in place by 2017. In order to guarantee the effective and timely implementation of these measures, the Swiss Government has adopted a detailed plan for the implementation of the strategy on 15 May 2013. It has further called into life a Steering Committee, in which the leading agency for the implementation of a specific measure is represented. The Steering Committee is mandated to secure the coordinated, purposeful implementation of this strategy. Its roles and responsibilities range from ensuring coordination among the relevant Swiss Federal departments¹ and relevant agencies at the local level. At an operational level, the Swiss Government has set up a Coordination Unit which is supposed to support the work of the Steering Committee. The NCS is currently being reviewed. By the end of 2016 the Steering Committee will submit a report of recommendations to the Swiss government.

The set of measures ranges from risk and vulnerability analysis, analysis of the threat landscape, continuity and crisis management, as well as competence building measures to international cooperation and initiatives.

The 16 measures can be broken down into four main areas:

- **prevention** (i.e. risk and vulnerability analysis and threat landscape),
- **reaction** (i.e. incident handling, active measures and law enforcement),
- **continuity** (i.e. continuity and crisis management) and
- **supporting processes** (i.e. international cooperation, education and research, legal foundations, etc.).

**c) The content of the concepts mentioned in paragraph 2 of the resolution**

International cooperation is one of the action fields that need to be strengthened by

¹ Equivalent to a Ministry.
means of the Swiss national cyber strategy. Thus, Switzerland is determined to cooperate at the international security policy level so as to encounter the threat in cyberspace together with other countries and international organisations. Switzerland is committed to monitor and shape respective developments at diplomatic level and promote political exchanges within the framework of international conferences and other diplomatic initiatives.

The Swiss foreign policy in the field of cyber security focuses on the development of norms of responsible state behaviour, confidence building measures and capacity building. With this in mind, Switzerland participates in different international processes. The OSCE has adopted confidence building measures (CBMs) in the realm of cyber security. Switzerland considers this process as paramount. Thus, by pursuing a “dual track”, Switzerland will focus on the implementation of the adopted CBMs as well as on the development of further measures. In addition, the London agenda constitutes a further important process within which Switzerland participates. Switzerland supports a range of projects designed to develop capacity building.

Bilaterally, Switzerland holds regular political consultations with countries on cyber related issues.

Switzerland is a signatory country of the Council of Europe Convention on Cybercrime, which entered into force on 1 January 2012.

d) Possible Measures that could be taken by the international community to strengthen information security at the global level

Initiatives and measures designed to increase trust and build better understanding and confidence between states are to be focused on. At a bilateral level, track 1, 1.5 and 2 dialogues between states and other relevant stakeholders on cyber security issues have proven to be fruitful. Dialogues on cyber security need to be further developed and enhanced.

Information security could be strengthened at a global level by means of establishing joint mechanisms to avoid escalation to armed conflict. Thus, direct communication lines at both the technical and policy level could be established. By maintaining regular contacts at the highest level security in cyberspace can be improved.