Resolution 71/28 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, ICT can also be exploited by criminal, intelligence, politico-military or terrorist actors. Disturbances, manipulation and specific attacks, through the use of cyber means are the risks that an information society entails. Moreover, cyberspace is increasingly being used for disinformation campaigns to influence public opinion across societies and to undermine trust in democratic institutions and political processes.

Against this backdrop, states have adopted national cybersecurity strategies and become increasingly engaged in a series of regional and international policy discussions and debates over cybersecurity. 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.

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 cybercrime, 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 implemented by the end of 2017. 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.).

Currently, Switzerland is in the final phase of developing a new cybersecurity strategy which will be published in the beginning of 2018.

In April 2016 the Federal Council adopted the Digital Switzerland Strategy, which indicated where and how authorities, academia, the private sector, civil society and politics must work together in order to shape the Digitalization process for the benefit of everyone in Switzerland.

**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 means of the Swiss national cybersecurity 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.

Against this background, Switzerland participates in different international processes aiming at developing global mechanisms.

Switzerland was a member of the Group of Governmental Experts on the Developments in the Field of Information and Telecommunication in the Context of International Security (UN GGE) 2016/2017. Switzerland is of the view that an open, free and stable cyberspace can be achieved through the application of international law, norms of responsible state behaviour, confidence-building measures and capacity-building activities. The OSCE has adopted confidence building measures (CBMs) in the realm of cyber security. Switzerland considers this process as paramount. Currently the focus lies on the implementation of the two sets of CBMs. Switzerland has developed concrete proposals on how to implement individual CBMs.

In addition, the London agenda constitutes a further important process within which Switzerland participates. Switzerland is a founding member of the Global Forum on Cyber Expertise (GFCE) and supports various cyber capacity-building projects.

Bilaterally, Switzerland holds regular political consultations with countries on cyber related issues.
Switzerland is a signatory country of the Council of Europe Convention on Cyber-crime, which entered into force on 1 January 2012 and considers its implementation as crucial in the fight against cybercrime.

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.

Switzerland is of the view that the UN should continue to play an important role in the debate on international cybersecurity. The topic has gained more attention at the political level and is of relevance to all member states of the UN. The normative cybersecurity debate at the global level needs to become more representative and include the broader UN membership. Moreover, international cooperation would benefit from the systematic involvement of the private sector, academia and civil society. The progress achieved by the 2010, 2013 and 2015 UN GGE reports is of great importance and should be consolidated. States need to build upon this strong basis by increasing and promoting the awareness and implementation of the UN GGE recommendations, including the application of international law to the ICT use, the voluntary non-binding norms, rules or principles of responsible state behaviour. These instruments contribute to an open, secure, stable and peaceful cyberspace. Regional organisations can play an important role in implementing the UN GGE recommendations. In addition, cyber capacity-building is needed to ensure that states are able to meet the requirements of the existing framework of rules.