Polish position on the issues outlined in the Resolution of the General Assembly of the United Nations entitled “Developments in the field of information and telecommunications in the context of international security”

1. General opinion on cybersecurity issues

Cybersecurity is vital for maintaining economic growth and functioning of civil society. Every year illegal activities in cyberspace cause huge financial losses, both globally and nationally. Economic rights of citizens are violated increasingly online, while personal information being stolen.

Cyberattacks can affect not only private sector and public administration, but also industrial automation systems (SCADA), including industrial automation in critical infrastructure facilities. Attacks in this sector can lead to physical damage to facilities that are important for the economy, the environment and the citizens.

Cyberattacks originate from the territory of Poland and from abroad, including the countries with which Poland does not have mutual agreements on legal assistance. It is often impossible to determine the location of the attacker, because of the wide use of anonymization methods used in cyberspace.

Potential attackers may be both criminal groups motivated by making profit and groups that are backed by foreign states intelligence agencies. These activities are aimed at acquiring information or undermining political, economic or social stability.

Ensuring a coherent system of information and telecommunication security is necessary in light of the nature of threats and growing dependence of businesses, administration and society on information technology. All stakeholders including the state, business and NGOs must be involved and contribute to national cyber security.

Effective protection of cyberspace is the cross-border, global challenge. It is necessary to develop and deepen international cooperation in the area of cyber security.

The respect for international law and norms, including sovereignty, territorial integrity of states and right to defend themselves is a necessary condition for maintaining peace and security between states in cyberspace. These norms contribute to the stability and predictability of international relations, including those in cyberspace.

Enhancing national capabilities to identify and prevent threats in cyberspace are the key elements in strengthening international security in cyberspace.

Expanding confidence in cyberspace will have a positive impact on relations between states in other areas. At the same time, the current violations of international law beyond cyberspace may undermine the determination of the international community in developing common norms and understanding in cyberspace.

Human rights and fundamental freedoms should be equally protected in cyberspace and in the real world. Respect for fundamental freedoms on the Internet is essential for democratic society, sustainable growth and prosperity.
2. National initiatives to strengthen cyber security and promotion of international cooperation

Polish system of cybersecurity is based on a network of institutions. It is based on cooperation of entities, both in the civil and military dimension and in the sphere related to cybercrime. The Ministry of Digital Affairs serves as a strategic and political coordinator of the system. The national powers related to the security of cyberspace are divided, among others, between the Ministry of Digital Affairs, the Ministry of National Defence, the Government Centre for Security, the Ministry of the Interior and Administration and the Council of Ministers, the Internal Security Agency, the General Police Headquarters, the Ministry of Justice, the Office of Electronic Communications, as well as CERT Polska operating within the structures of the Research and Academic Computer Network (NASK). There are also public and private Computer Emergency Response Teams (CERT). Their scope of activities include, among others, government and military administration and the Police, as well as teams established by telecommunications operators and scientific research communities.

The Polish government is advancing its efforts to develop a national cyber security strategy and national cybersecurity law (comprehensive legal act). The key elements of the Polish cybersecurity system will include: procedures, people and technology. Polish authorities are working to unify the procedures for cyber crisis management. The effectiveness of procedures will be ensured by clearly specifying the channels of communication and the flow of information between all stakeholders in cybersecurity management processes. People are always the weakest links in the system. Therefore, developing and improving personnel skills is an important as the education of users. It is necessary to plan and organise comprehensive exercises, training and tests that offer the possibilities to check all systems and procedures in response to cyber threats. Polish authorities are keen on promoting the best, highly qualified specialists, while providing incentives for them to remain part of the public administration. The government is working on a dedicated incentives programme which will allow reducing the outflow of specialists with the highest qualifications from government institutions. In the field of technology, we are currently working on the creation of the National Competence Centre and the national CERT. This institution will be in charge of direct management and implementation of different projects relating to national cybersecurity issues. At the same time, it will be responsible for the national early warning system.

It is important to improve the tools for monitoring and prevention of cybercrime and coercive cyber operations. Beyond that, the development of proper security environment, in terms of competences and procedures, will require the implementation of new tools for monitoring, preventing and responding in cyberspace. These tools should be the galvanising factor for the cybersecurity sector.

Last year, Poland hosted several major international events, such as SECURE 2015 Conference, European Cybersecurity Forum – CYBERSEC.EU and the International Conference on Cyber Security – Safety and Security beyond Borders. These fora contributed to the promotion of international cooperation.

3. Possible measures that could be taken by the international community to strengthen cybersecurity at the global level.

It is necessary to further develop confidence building measures in the field of cyberspace implemented globally, regionally and nationally. International exchange of information on cyber threats and good practices is critical. Development of strong mechanisms of cooperation within
regional organisations such as the EU is of a great importance. Additionally, it would be beneficial to develop common means of cooperation, for example, in the area of cyberdiplomacy.

The international community should encourage to build national capabilities in the area of cybersecurity. It should include the prevention of cybercrime, coercive cyber operations and the use of the Internet for terrorist activities.

It is also important to deepen bilateral and regional cooperation. A good example of regional efforts is the Central European Cyber Security Platform (CECSP), comprised of Poland, the Czech Republic, Slovakia, Hungary and Austria.

One should not underestimate the value of involvement in the international dialogue of stakeholders representing NGOs, business and academia.

Moreover, international exercises in the field of cybersecurity allow for better understanding of the nature of threats and means of responding to them. Exercises CYBEREUROPE or the NATO Locked Shields are a case in point.
Executive summary

1. General opinion

Cybersecurity is vital for maintaining economic growth and functioning of civil society. Cyberattacks can affect not only private sector and public administration, but also industrial automation systems in critical infrastructure facilities.

Ensuring a coherent system of information and telecommunication security is necessary in light of the nature of threats and growing dependence of businesses, administration and society on information technology. All stakeholders including the state, business and NGOs must be involved and contribute to cyber security.

The respect for international law and norms a necessary condition for maintaining peace and security between states in cyberspace.

Enhancing national capabilities is the key element in strengthening international security in cyberspace.

Expanding confidence in cyberspace will have a positive impact on relations between states in other areas.

Human rights and fundamental freedoms should be equally protected in cyberspace and in the real world. Respect for fundamental freedoms on the Internet is essential for democratic society, sustainable growth and prosperity.

2. National initiatives to strengthen cyber security and international cooperation

Polish system of cybersecurity is based on a network of institutions. It is based on cooperation of entities, both in the civil and military dimension and in the sphere related to cybercrime.

The Polish government is advancing its efforts to develop a national cyber security strategy and national cybersecurity law. The key elements of the Polish cybersecurity system will include procedures, people and technology.

Last year, Poland hosted several major international events that contributed to the promotion of international cooperation: SECURE 2015 Conference, European Cybersecurity Forum – CYBERSEC.EU and the International Conference on Cyber Security – Safety and Security beyond Borders.

3. Possible measures that could be taken to strengthen cybersecurity at the global level.

It is necessary to further develop confidence building measures in the field of cyberspace implemented globally, regionally and nationally.

The international community should encourage to build national capabilities in the area of cybersecurity.

It is important to deepen bilateral and regional cooperation. A good example of regional efforts is the Central European Cyber Security Platform, comprised of Poland, the Czech Republic, Slovakia, Hungary and Austria.

International exercises in the field of cybersecurity allow for better understanding of the nature of threats and means of responding to them. Exercises CYBEREUROPE or the NATO Locked Shields are a case in point.

One should not underestimate the value of involvement in the international dialogue of stakeholders representing NGOs, business and academia.