THE POSITION OF THE POLISH GOVERNMENT

I. DOCUMENT SPECIFICATION

Title
COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry.

Date of Sending an Application by the Parliament of the Republic of Poland	Date of Taking a Position by the Committee for European Affairs
22 July 2016.	

Signature of the European Commission	COM(2016)410

Leading Institution
Ministry of Digital Affairs

Cooperating Institutions
Ministry of National Defence
Ministry of Foreign Affairs
Ministry of Interior and Administration
Ministry of Development
Ministry of Finance
Ministry of Justice
Ministry of Health
Ministry of Infrastructure and Construction
Internal Security Agency
Government Centre for Security
Inspector General for Personal Data Protection
Office of the Prime Minister
Power Industry Regulation Office
Office of Electronic Communications
Civil Aviation Office
Centre for Shared Services
National Police Headquarters

II. PURPOSE OF THE DOCUMENT

The European Commission indicates that the purpose of the Communication is to find ways to address the evolving cybersecurity reality and assess additional measures that may be necessary to improve the EU's cybersecurity resilience and computer incident response.

The Commission also devotes attention to industrial capacities in the EU – supply of products and services that will provide for the highest level of cybersecurity is an opportunity for the cybersecurity industry in Europe and as a result could be a competitive advantage of the European industry.

As a result, in the opinion of the Commission, a strong political commitment is necessary, for example, through:

- stepping up cooperation to enhance preparedness and deal with cyber incidents;
- addressing challenges facing Europe's cybersecurity Single Market;
- nurturing industrial capabilities in the field of cybersecurity.

III. REFERENCE DOCUMENTS

- Cybersecurity Strategy of the European Union: an open, safe and secure cyberspace;
- Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems;
- Directive 2016/1148 of the European Parliament and of the Council (EU) of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union;
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A Digital Single Market Strategy for Europe", COM (2015) 192;
- Communication from the Commission to the European Parliament, the European Council and the Council delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union, COM (2016) 230.

IV. THE GOVERNMENT'S POSITION

The Government of the Republic of Poland supports the action aimed at strengthening Europe's cyber resilience system and fostering a competitive and innovative cybersecurity industry. The information revolution that started in the second half of the 20th century brought about streamlining of means of communication and internationalised information flows.

The Government of the Republic of Poland notices the essence of new cyberspace hazards that continue to evolve and are acquiring more considerable significance, in connection with transferring subsequent spheres of human life and activity into the virtual dimension. Currently, new technologies and the Internet play an essential role in social and economic life. These are critical resources for all sectors of the economy are based on them. For this reason, it is extremely important to strengthen our resilience to cyber incidents so that the economy and society may function smoothly, and develop.

Cyber threats are of transnational nature. They involve entire critical sectors, and not particular states. Therefore, international cooperation is becoming essential in respect of exchange of information about incidents, and also exchange of knowledge and technologies. At the same time, it should, however, be borne in mind that national security is one of the prerogatives of Member States. As a result, all actions taken by the EC in respect of cybersecurity, both in terms of EU cybersecurity potential development and the exchange of information about incidents, should be consulted with Member States in detail.

Directive of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ensures the legal basis for cooperation between Member States at a political and strategic as well as at an operational level. Establishment of the Cooperation Group and the CSIRT network are extremely important elements of the system and potential for increase in cyber resilience of EU. New activities are necessary to make it possible for political and operational cooperation to develop and function smoothly, provided that the activities are complementary in relation to already existing initiatives and activities.

The Government of the Republic of Poland notes with satisfaction intensified activities at the EU level to improve the EU's security in cyberspace and threat response in this respect. Cross-border nature, flexibility and innovative character of this type of crime cause that assumptions in this respect must be constantly updated. Given the above, the first line of defence against cybercrime should be the aspirations for constant security strengthening and capacity-building in cyberspace. In this context special attention should be paid to further nurturing the capabilities of the European Cyber Crime Centre (EC3) at Europol as well as the synergies between existing and developed initiatives, to increase the effectiveness of cooperation in this respect.

Decisions of the NATO Summit in Warsaw on taking cyberspace as another domain of military action and obligations of nurturing capabilities connected with it in the field of cyber defence that gave new weight to the issues of cybersecurity are not without significance. Reaching capacities in respect of cyber defence will be checked on a regular basis in practice during tests as well as national and international exercises in which it is desired that also EU relevant entities take part. The purpose of the optimisation and rationalisation of costs incurred by Poland related to membership in EU and NATO and establishment of uniform directions of action, initiatives undertaken in cybersecurity within the European Union should be considered in the context of activities already carried out or planned by North Atlantic Treaty Organisation.

Given the above and North Atlantic Treaty Organisation members' will to strengthen cybersecurity in the Euro-Atlantic region by supporting cooperation between NATO and the European Union, the Government of the Republic of Poland supports all EU initiatives for strengthening Europe's cyber resilience system. These initiatives should be coherent with the initiatives implemented by NATO and should not be duplicated at the same time. Such an approach should ensure synergy between state activities undertaken by the members of the North Atlantic Treaty Organization and the European Union, and also optimisation and rationalisation of costs incurred on this account.

The Government of the Republic of Poland supports the EC's position that a political commitment is necessary by stepping up cooperation to enhance preparedness and abilities to deal with cyber incidents and by addressing challenges facing Europe's cybersecurity Single Market. Nonetheless, it is important that these activities are well planned, potential of already existing and well-tried structures is used when these activities are carried out, and new entities are established only in the case that already existing structures/bodies are unable to implement entrusted tasks. The main advantage of use of existing structures is avoiding duplication of mandates and tasks causing the lack of clarity and ineffectiveness of activities carried out.

It is worth noting that some of the solutions presented in the Communication aiming to strengthen Europe's cyber resilience system are already functioning in Poland, for example, in the Ministry of National Defence (MND). Particularly, the Computer Incident Response System that cooperates with NATO Cyber Incident Response Capability and other Computer Incident Response Teams in respect of responding to cybersecurity incidents and exchanging information about potential cyber-threats has been operating within the MND's structures since 2008. According to the EU plans, corresponding cyber aspects are to be also integrated into existing crisis management mechanisms, which already occurred in the case of MND.

It is beyond question that strengthening Europe's cyber resilience system should go hand in hand with the protection of individual rights. Consequently, the Commission should consider what role a citizen plays in the process of creating framework of cybersecurity in Europe. Designing solutions at the EU level, it seems necessary to create legal framework conforming to the Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing of Directive 95/46/EC (General Data Protection Regulation) that will be used from 25 May 2018. and with Directive 2016/680 of the European Parliament and of the Council (EU) of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of preventing crime, carrying out preparatory proceedings, detecting and prosecuting prohibited acts and carrying penalties, on free movement of such data. Real assistance that can be offered by authorities of the European Union being a competence centre in this respect should be considered, which can involve the need to incur certain costs.

Any decisions related to the implementation of tasks provided for in the Communication should be, at every stage, consulted with Member States. We want to build Europe's a coherent cybersecurity system, based on cooperation and clear principles accepted by all States. The best Forum for this type of commitment and discussion is the so-called Friends of the Presidency Group on Cyber Issues operating at the Council. It is the forum of this group where discussions that include a wide spectrum of subjects in cybersecurity take place. This Group's mandate for the following years should be constructed so that Member States can in full use its potential. Particularly, communicated possible update of the EU cybersecurity strategy of 2013 should be discussed in detail. Poland would like to become particularly involved in this process.

I. The Government of the Republic of Poland supports the use of online network and information security cooperation mechanisms to the fullest extent possible.

Building the Joint Research Centre (further: the Centre) in cooperation with ENISA and CERT-EU so that knowledge of cybersecurity at the EU level is centralised is an extremely ambitious task. It is necessary to design such mechanisms/procedures for setting up the Centre so that specialists' potential from different Member States is fully used. From the point of view of resilience to attacks, the Centre should function more in the form of a cloud, rather than a geographically separated institution. All partners of such a Centre should receive detailed information about currently emerging threats. Poland would like to take an active part in the process of creating the Centre. As the development of the idea to create an "information hub", it is worth considering setting up *Cybersecurity Observatory* as a sub-page of the portal managed by the European Commission https://joinup.ec.europa.eu/or the ENISA agency. At the same time, from the point of view of individual rights and national security as well as transparency of data processing, the principles of the operation of the Centre should be detailed and it should be specified to what extent and for what purpose data will be collected as well as the mode of access to the collected information by all Member States.

Moreover, the Government of the Republic of Poland is of the opinion that in the course of creating a high-level advisory group on cybersecurity (further: advisory group) composed of experts and decision-makers, commitment of all entities that are members of the cybersecurity system, starting from representatives of industry, academia and civil society and other non-governmental organisations, is important. When setting up an advisory group, it must be ensured that the principles for transparent and secure processing of data are taken into account due to their scale and type.

In Poland, currently works are being carried out on comprehensive Cybersecurity Strategy for the Republic of Poland that, for example, will fulfil responsibilities arising from the NIS Directive. One of the elements will be the Forum for Cybersecurity (further: Forum) in whose operations we want to involve all entities willing to cooperate. We can see potential for cooperation between the planned advisory group and the Polish Forum.

The Government of the Republic of Poland supports also renewal of the European Network and Information Agency' (further: ENISA) mandate as quickly as possible. In view of increasing cyber-threats, it is extremely important that the Agency supports Member States with its expertise. It is essential to analyse ENISA tasks in the context of the NIS Directive, for example as the secretariat of networks of CSIRTs. Such activities can be taken, among others, on the forum of the aforementioned Friends of the Presidency Group on Cyber Issues.

We believe that it is worth involving other already existing regional organisations/entities occupied with cyber issues in cooperation. One of such entities is, for example, the Central European CyberSecurity Platform (CECSP), whose members are Poland, Austria, Czech Republic, Slovakia and Hungary. CECSP countries usually meet twice a year. A few days' meetings are devoted to strategic and purely technical issues. This year Poland holds the annual chairmanship in CECSP.

II. The Government of the Republic of Poland supports increasing efforts in cybersecurity education, training and exercises

The EU's initiative worth special supporting is the proposal to develop civil-military cooperation and synergies in training and exercises. Practical checking computer incident response capabilities and capabilities to exchange information in an international environment allows to obtain unique experience and objectively assess rightness of accepted assumptions in respect of organisational structures, procedures and training being specialists' development path. Confirmation of this is the Anakonda-16 exercise in the course of which in the international environment, parallel to operational activities, practical cyberactivities were implemented. Given the above, the integration of participation in exercises of subsequent military and civil entities as well as entities operating within the EU structures would make it possible to further enrich the formula of defence training and exercises carried out. Therefore, it seems correct for the EU to establish a cybersecurity education, exercise and training platform that would promote synergies between civilian training/exercises and defence training/exercises. Joint exercises will undoubtedly increase Europe's cybersecurity.

However, different specificity of training organised in case of cyber crisis in the civilian sphere (particularly concerning critical sectors) and another one, connected with a cyber component of military exercises, should be taken into account. It is worth noting that several extremely important exercises are already carried out at the EU level, for example, CyberEurope exercises organised by ENISA. However, it is still not enough.

A clear and precise European system for education, training, and tests is essential. The system should be developed so that it corresponds to needs and capabilities of Member States and should be

organised in cooperation with them. It is worth at the same time using forums, i.e. the recently set up European Cybersecurity Organisation (ECSO), under which the works of a working group devoted to these issues will commence soon. At the same time, to ensure coherent activities and to increase cybersecurity education and training capabilities, constant development of cooperation in this respect with the European Cyber Crime Centre at Europol (EC3) and the European Union Agency for Law Enforcement Training (CEPOL) is extremely important.

III. The Government of the Republic of Poland firmly supports cross-border and cross-sectorial cooperation to achieve increased preparedness and resilience to cyber incidents

A coordinated approach to cooperation in critical situations is necessary. For this reason, the aforementioned cyber exercises making it possible to test procedures and principles of cooperation between Member States are an extremely important element. They, however, cannot "pile off", and should correspond to specific needs and current real threats. Protection of critical infrastructure and crisis management mechanisms should take account of the specificity of cyber-threats. It is, therefore, important that also these elements are taken into account in the Action Plan on Cooperation presented to the EC.

It is also worth emphasising that although the Directive 2008/114/EC of the Council of 8 December 2008 on the identification and designation of European critical infrastructures (further: EIK) and the assessment of the need to improve their protection does not directly refer to data communication threats, the scope of solutions used to protect EIK depends on the assessment risk of disruption of its operation and does not exclude taking it into consideration in the Plan for Data Communication Security Protection (the scope of POI is specified in Appendix 2 to the Directive). In the content the Directive itself it is also emphasised that: "Where appropriate and in connection with the review of this Directive, as defined in Article 11, subsequent sectors that will be used for the purposes of enacting this Directive may be determined. ICT sector is given the priority".

For harmonisation and mutual supplementation of Directive 2008/114/EC and the NIS Directive, it is worth considering to take action in this matter. In the context of cross-sectional assessment, bear in mind the need to distinguish the risk of cyber incidents whose assessment the Commission will make, from the risk assessment at the national level or adequate lower level made by Member States, and resulting from the EU Civil Protection Mechanism. Based on this, Member Countries were under an obligation until 22 December 2015 to make available to the Commission summaries of significant elements of the risk assessment prepared at the national level or adequately lower level, which Poland did. Existence of national or regional risk assessment is also one of the *ex-ante* conditions contained in Section A5 Guidance on *Ex Ante* Conditions for European Structural and Investment Funds. Disruption of supply of key services as a result of an ICT attack can be taken into account in both cases. It would be, therefore, undesirable that these assessments overlap each other.

Complementing action specified in the Communication the European Commission could consider creating methodology for assessment of progress in approaching maturity in network and information cybersecurity in sectors included in the scope of the NIS Directive. Introduction of a measurement method could be aimed to understand existing gaps better, and therefore draw conclusions in a more appropriate manner as to further activities undertaken by the European Commission where the priority should be given to correct implementation of currently applicable legislation. As for suggesting and assessing implementation of its activities, the European Commission should follow the *EU Programme - Better Results as a Result of Better Lawmaking*

adopted in May 2015, in particular point 2.2. *More Understandable Explanation of What We do and Why.*[1]

IV. The Government of the Republic of Poland supports scaling up cybersecurity investment in Europe and supporting SMEs, and is in favour of stimulating and nurturing European cybersecurity industry through innovation and establishment of the cybersecurity cPPP (further: cPPP)

Poland is happy with the fact that a cooperation contract was signed on 5 July in Brussels between European Cybersecurity Organisation (ECSO), and the European Commission. Representative of Poland will have a seat in the first term of office of the Board of Directors. We support the cPPP idea, i.e. fostering the competitiveness of European industry, for example, by making use of funds by entrepreneurs available under HORIZON 2020. The Government of the Republic of Poland believes that entrepreneurs' joint activities and jointly implemented projects will help not only increase the sector innovation, but also will contribute to exchange of experience and knowledge between involved European partners. Construction of strong European IT industry companies should be sought that will be able to successfully compete in the global economy. If EU has no capabilities for technological development, it will be impossible to build cybersecurity. Special attention should be paid to the European SMEs - that have enormous potential for development on a global scale. Many years of underdevelopment in this respect should be addressed as soon as possible. It will be impossible without access to funds that should be ensured at the EU level through different sources, i.e. HORIZON 2020.

V. The Government of the Republic of Poland advocates that the EC should take into consideration the already existing and/or currently developed national certification capabilities, as far as certification and labelling is concerned.

Currently in Poland works are carried out on implementation of the national system for assessment and certification based on the international standard ISO/IEC 15408 (the so-called Common Criteria). As a target, it is planned to incorporate this system into the European SOG-IS system. It may prove to be necessary to establish protection profiles at the European level for specific categories of products of ICT industry so as to it is possible to fully implement mutual recognition of certificates. Nonetheless, the Government of the Republic of Poland as far as the national security is concerned is of the opinion that mutual recognition of certificates should be optional in nature.

V. REASONS FOR THE GOVERNMENT'S POSITION

In view of an evolving international situation and increase in the significance of new technologies, cybersecurity is now equally significant for security of individual countries, including Poland, as military and economic security. Cyberspace has no boundaries, analogous to these state ones. Therefore, to effectively counter cyber-threats and minimise their effects, ability to effectively act and cooperate beyond borders is extremely important.

The awareness of threats that exist in cyber world of how these threats can be avoided, despite almost 20 years of existence of the Internet and gradual migration of social life to virtual reality, is still relatively low.

[1] In any case we need to better explain why we undertake specific actions, which results we expect and what their effects may be. Every application of the Commission will be accompanied by a substantiation better than before 5 . Apart from explanation of the aim of the proposed measure, it will include information on how the principles of better law making have been applied: why a given initiative is necessary, why it is the best instrument that EU may use in a particular case, what is the opinion of the parties involved and what are the likely environmental social and economic effects, especially for the competitiveness and small and medium enterprises (SMEs). The substantiation will also containe more detailed clarification on the way in which a given initiative is consistent with two principles: subsidiarity (why the goal cannot be achieved by Member States on their own) and proportionality (why the proposed measure does not go beyond what is necessary to achieve the goal).

The Internet and digital technologies bring about a real revolution in our daily lives. From one day to the next, more and more devices are connected to the Internet. In Poland it is already estimated that the number of such devices is tens of millions. These devices used for different purposes, private, official or business ones can be infected with malicious software at any time.

That is why all initiatives, including those indicated in the Communication, which as a consequence will strengthen the cybersecurity system not only of individual Member States, but also of the entire European Union are so important.

Consequences of the Communication COM 11013/16

ECONOMIC: The Communication refers to increase in the competitiveness of European industry of cybersecurity segment, for example, through contractual Public-Private Partnership. Active participation of Polish entities in the ESCO project - will give our national entrepreneurs not only access to funds from the HORIZON 2020 programme, but also an opportunity to acquire additional knowledge and new business partners.

BUDGETARY: It is difficult to estimate, as EC did not give details concerning individual initiatives, what potential financial consequences this Communication can cause for Poland.

LEGISLATIVE: The Communication *per se* does not involve the need to change legal regulations applicable in Poland. On the contrary, in light of adopting the NIS Directive in July this year Poland, and also other Member States, is obligated to implement the provisions of the Directives to the legal order of Poland. Currently, advanced works on a draft of the Act on the national cybersecurity system are carried out in the Ministry of Digital Affairs.

VI. SOCIAL PARTNERS' OPINION

CYBERETYKA FOUNDATION

With reference to the Communication from EC on social consultations in relation to cybersecurity the CyberEtyka Foundation wishes to express our complete support for any activities of the Polish government concerning the strengthening of the Polish cyber resilience system in the first place, and for the development of common solutions under European systems.

Reviewing the document attached on the webpage of the Ministry, we are glad with activities described therein which are planned by the EC and we would like to announce our willingness to cooperate with Polish governmental institutions in this respect.

We, however, notice that while the direction of the activities is in our opinion certainly correct, special emphasis on the education of the youngest citizens is missing in these documents. In the document (chapter 2.2) cybersecurity education, training and exercises are, admittedly, mentioned, however, narrowing the scope only to preventing incidents in the sphere of security and to handling their effects may be insufficient.

Our opinion is that learning the so-called “cyber ethics” should start from the beginning, from an early age. We encourage to take advantage of our experience as Foundation in this matter, perhaps to together develop an educational programme for elementary schools, to together develop the computer science 2.0 programme under the partnership or even to introduce “cyber ethics” as an additional school subject – that in a comprehensive manner approaches the issues connected with data communication security and cybersecurity.

THE KOŚCIUSZKO INSTITUTE

The Kościuszko Institute completely supports all activities taken for strengthening of the European Union cybersecurity, and also contributing to propagating increase in supply of products and services on the part of the cybersecurity sector of the European Union. By implementing our projects (above all by organising the European Cybersecurity Forum - CYBERSEC, and the Polish Cybersecurity Forum - CYBERSEC PL), by becoming involved in national and international initiatives, we pursue to implement these objectives. By supporting ideas that lie behind the activities provided for in the COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: *Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry*, we would like to draw your attention to the several elements indicated below.

The communication is a strategic document with a high level of generality. Theses from item 3-4 (Confronting challenges facing Europe's cybersecurity single market) are a repetition of the postulates from the Communication on the establishment of a contractual Public Private Partnership in the field of cybersecurity (PPP) and the accompanying documents (above all: European Cybersecurity Industry Leaders Recommendations on Cybersecurity for Europe - A report to M. Günther H. Oettinger European Commissioner for Digital Economy and Society). For this reason, only stipulating the provisions in more detail will make it possible to better assess the action proposed in the Communication.

The communication assumes strengthening the existing and arrangement of new mechanisms of cooperation and quick exchange of information in the face of cybernetic crises. The objective of the European Commission is counteracting the dispersion and lack of expert knowledge organization, by establishing the EU centre of information that would gather and facilitate access to ordered information on the risk for the cybersecurity and potential remedies. Although tightening international cooperation as to cybersecurity is an undeniable asset, due to the recent experience of the EU legislative practice (e.g. modifications of item 10 of the Recitals of the Regulation on the European Border and Coast Guard) already at an early stage of legislative works, it is worth reserving that in connection with Article 4, paragraph 2 of TUE and Article 72 of TfUE, proposals of the European Commission cannot obligate Member States to share information, whose disclosure is in conflict with the basic interests of their national security. The communication indicates that delivery of products and services that ensure the highest level of cybersecurity, is an important opportunity of development for the cybersecurity industry in Europe and would become a strong competitive advantage. It should be emphasized that beside economic benefits, building the EU capacities is valid also from the point of view of providing cybersecurity of the whole EU and every Member State.

The Communication indicates that pursuit to make the EU the leader in this field must be accompanied by strong culture of personal data security, including personal data, and effective response to incidents. One of key elements from the point of view of ensuring the leader's position to EU is also providing safe operation of industrial control systems. It is important, both from the point of view of security and development of one digital market.

The communication stresses that the mechanisms provided in the content should operate as one consistent cybersecurity and cybercrime combating system, helping Member States to better cooperate in fight against terrorism, organized crime and cybercrime. The catalogue of possible sources of hazards is incomplete and should be supplemented, e.g. by hostile acts from state entities.

The communication emphasizes that a primary element of national capacities required by the Network and Information Security Directive are Computer Incident Response Teams (CSIRT), responsible for fast response to cybernetic hazards and incidents. From the point of view of national

cybersecurity systems, equally important links are operators and owners of the critical infrastructure, which is noticed also in the NIS Directive.

The communication indicates that the expert knowledge on cybersecurity is now available at the EU level, but in a dispersed and unorganized manner. In order to support mechanisms of cooperation with regard to safety network and information security, it is necessary to gather information in the information centre for them to be easily available upon request to all Member States. This centre would become the main source of information allowing EU institutions and Member States to exchange information in applicable cases. For full evaluation of this idea it will be necessary to provide more information on the methods of its operation.

From the point of view of ENISA assessment, which is to take place by the end of 2017 and discussion on the possible need for modification or extension of the ENISA mandate, attention should be paid to crucial role of the Agency in implementation of the NIS Directive. ENISA should, in this area, play an important role harmonizing the actions conducted at the level of Member States.

The communication indicates that currently, ENISA, the European Cybercrime Training and Education Group (ECTEG), in cooperation with the European Cybercrime Centre at Europol and the European Police College (CEPOL) all play an important role in providing capacity-building support – including on cyber forensics – by developing manuals, and organising training and cybersecurity exercises. An important area of the group functioning should be action focused on ensuring not only on strengthening skills of Police officers, but also activities focused on improving knowledge and skills of prosecutors and judges.

The communication stresses that cyberspace is a rapidly developing domain where dual-use capabilities play an essential role. It is therefore necessary to develop civil-military cooperation and synergies in training and exercises to increase the resilience and incident response capabilities of the EU. It is worth in this context refer to the need for strengthening cooperation with NATO.

The communication indicates that national initiatives are emerging to set high-level cybersecurity requirements for its components on traditional infrastructure, including certification requirements. The term "traditional infrastructure" should be clarified.

From the point of view of providing high standards of transparency important that the cooperation of the EU institutions with various entities supporting execution of the operations under construction of one European cybersecurity market (e.g. PPP) took place on transparent terms ensuring their equal rights. The Partner of EC in the implementation of PPP will be the European Cybersecurity Organisation (ECSO). This entity is assumed to represent interests of various internal market participants in contacts with of EC (Article 1 of the decision of 5 July 2016), participate in the costs of the investment and, above all, co-shape investment priorities in the field of cybersecurity (item 5-6 of the preamble the decision on creation of PPP, e.g. SRIA – Strategic Research and Innovation Agenda). Participation of the private sector representatives is necessary for programming public policies in the field of the cybersecurity market. Under PPP, ECSO will play the leading role. Considering countries of origin of entities included in its composition, there is visible domination of just a few Member States (Germany, France, Spain, Italy). Poland is represented only by 3 entities (including the Ministry of Digitalization and NASK) out of 134 members of ECSO. For comparison - as many as 22 entities come from Spain. Poland does has no representative from the private sector in ECSO (SMEs, large enterprises, business associations). For effective use of the PPP potential, it is important to encourage to increase the presence of the Polish business in ECSO. The Kościuszko Institute plans to join actions of ECSO as well as promote this initiative during the CYBERSEC Forum in which Secretary General of ECSO Luigi Rebuffi will participate.

EC also plans to establish high-level advisory group for cybersecurity - an expert team enabling acquisition of external specialist knowledge and input data concerning the EC strategy concerning cybersecurity, as well as possible regulatory measures and other documents. The advisory group is to consist of representatives of the industry sector, academic environment and civic society. Apart from comments indicated in the previous paragraph, it should be ensured that owing to the matters being the subject of advisory group work, its makeup includes a geographical and demographic variety of states (in a manner similar to the Declaration related to Article 15 paragraph 5 and 6, Article 17 paragraphs 6 and 7 and Article 18 of TUE) in a way enabling respect for justified interests of Member States in the domains sensitive from the point of view of requirements of national security protection. The Kościuszko Institute – organizer of CYBERSEC PL, can help in identification of experts and specialists involved in particular aspects of cybersecurity. It should also be ensured that selection of the makeup, as well as functioning of the advisory group take account of postulates of the European Ombudsman, the European Parliament and of civil society in terms of openness, transparency as well as relevant balanced proportions of representation of particular interests groups. Due to sensitive matters being the subject of the session of the advisory group, it is worth using, in relation to it, raised (in respect of new principles of 30 May 2016) standard of transparency, taking into account recommendations of the European Ombudsman. Additionally, as part of support for achieving goals faced by the Advisory Group it is worth using the already existing resources permitting building expert knowledge, exchange experiences and form recommendations.

Under item 3.2 EC undertakes to consider establishing smart specialization platform in the scope of cybersecurity to help states and regions interested in investing in the sector of cybersecurity. The aim of the platform would be coordination and planning implementation of the strategy with regard to cybersecurity and the organization of the strategic cooperation of entities within regional ecosystems. Support is also declared for the development of globally competitive cybersecurity clusters and excellence centres in regional ecosystems fostering digital growth, with the addition that such support must be related to the implementation of smart specialization strategies and other EU instruments, so that the cybersecurity sector in Europe could use them better.

Plans of EC are consistent with the governmental proposal related to investment in cybersecurity, such as e.g.: Enigma Cyberparks or actions taken in connection with recognition of cybersecurity as one of 10 of strategic sectors for development of the Polish economy (Resolution No. 14/2016 of the Council of Ministers of 16 February 2016 on acceptance of the "Plan for responsible development"). In the regional context it is worth paying attention to the initiatives already undertaken in Małopolska. Małopolska is the second province (voivodeship) in Poland in terms of employment rate in ICT sector. Furthermore, it is in the leading edge in Poland in terms of the number of graduates of majors related to the ICT sector (12%). Cracow is a place of dynamic development of both great national companies (such as Comarch), but also direct investments of global tycoons of the ICT industry (IBM, Motorola, Delphi, Cisco), as well as SMEs and start-ups. In the capital of the region there are also leading research centres – University of Mining and Technology, Cracow University of Technology, Jagiellonian University, Jagiellonian Innovation Centre or Cracow Technology Park. The discussed Plans of EC are also consistent with the initiative of the Kościuszko Institute – CYBERSEC HUB, receiving support from the Polish government for their development, also with regard to obtaining the EU funds for the development, may be the source of the first Enigma Cyberpark. CYBERSEC HUB at this stage of development, is a support program for companies from Małopolska from the ICT industry having or developing products and services for cybersecurity. The Programme is intended to accelerate and strengthen their competitive position through promotion of innovation and international expansion, building relations with investors and clients. The Kościuszko Institute coordinates building relations and cooperation of key stakeholders of the cybersecurity sector in Małopolska, as well as accumulation of knowledge capital and good practices as a result of the European Cybersecurity Forum - CYBERSEC - organized in Cracow.

Polish Chamber of Computer Science and Telecommunication [PIIT]

The communication contains reference to the report entitled "Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II". The author of this report is McAfee company and the report itself comes from 2014. We believe that in the message dated July 2016 it would be more beneficial to refer to more valid reports (e.g. the 2016 HPE report provided earlier to the Ministry, and publicly available) and present trends showing the economic losses due to cybersecurity breach, increasing every year. It would also be beneficial to present the position of Europe and EU countries, as compared to other regions of the world.

It is worth reflecting one the revision of the EU cybersecurity strategy of 2013. Over the last three years that have elapsed since adoption of the strategy, a number of events occurred, which significantly affected perception of the role of cybersecurity in the contemporary world. These events include: terrorist attacks, hybrid war, attacks or attempted attacks on systems of the critical infrastructure in Europe.

The content of communication contains many references to the importance of effective response to incidents in the sphere of cybersecurity. Unfortunately, the document does not specify the scope of this process. In our opinion, it would be advised to state directly and clearly that it means comprehensive incident management process. Response to an incident is just one of a number of tasks present in this process. It is worth proposing using the provisions of standard SO/IEC 27035: 2011 Information technology -- Security techniques -- Information security incident management.

In the approach proposed in the message there is no reference to the role and place of broadly understood security architecture, which will constitute the basis for construction of the Europe's Cyber Resilience System. Such an approach, namely no security architecture may in the future result in more frequent occurrence of security hazards and incidents and increasing investment expenditures for the elimination of gaps and vulnerabilities, and assuring the required safety level in EU cyberspace.

We believe that it is also important to specify the principles of certification of software/hardware from outside the EU as to fulfilment of cybersecurity requirements. This will enable providing competitiveness of European (and thus also Polish) entities against entities operating outside the EU.

The proposed cyberspace protection system does not provide for any role of ordinary citizens. It is them who often much faster experience or detect irregularities associated with attack on public institutions.

IBM Polska Sp. z o.o.

We are aware of the need for taking new, additional measures to strengthen the cybersecurity resilience, we believe that the NIS Directive provides good framework for it. Measures proposed in the Directive for operators of critical services, at their transposition into national law, will increase the readiness of operators. IBM helps the customer adapt to the new requirements, for example by security operations centres, providing centralized monitoring of hazards and responding to them.

We believe that the NIS Directive is an important first step to improve security against cyber attacks. There is more to do in areas to which the NIS Directive has not referred - for example enabling better terms for industry to share information on hazards with one another. IBM may constitute a perfect example of an open platform, which enables exchange of such information, namely global XForce platform to share information related to hazards, a platform that enables users to quickly verify the latest hazards to security, reach the aggregated information, co-operate with others http://www-03.ibm.com/security/uk/en/xforce/.

We fully support the assistance for European and global cooperation on cybernetic threats through national CERTs /CSIRTs specified in the NIS Directive - these organisations usually have already dealt with cyber issues at the national level, and are often recognized as domestic leading organizations of trust with regard to cybersecurity.

In our opinion, the introduction of particular framework of the European cybersecurity certification systems would be an unfavourable development as there are already recognized international certification and standard systems in which Europe participates and any European approach to certification should include international standards. Only European approach would exclude up to 80% of international ICT providers, which would have a reverse effect to the intended one, both from the economic and security point of view, and significantly harm the European community of start-ups looking for global partners for further development.

With regard to promotion of a more competitive European cybersecurity industry, we believe that open competitive approach is very important. Closing the EU market to international players, either by introducing special conditions of financing research or preference for the orders only for EU solutions may have a reverse effect - creation of only a silo European industry along with the development of only the European approach to cybersecurity, is in conflict with the fact that cybersecurity is a global problem and can be counteracted only by a number of activities at the international level, by international standards for operators or by cooperation and exchange of information about the environment of hazards and specific attacks. The best example of global cooperation for cybersecurity is a network of IBM operational security centres with one of 10 in Wrocław http://www.zdnet.com/article/ibm-opens-polish-sec-shop/.

We also support strengthening in Europe knowledge and research-development works in the area of cybersecurity through H2020 programmes for security projects, open for all qualified consortiums also with international partners, but we also firmly believe in the need to strengthen education on average and higher level of education in all Member States.

VII. CONCLUSIONS

The initiatives presented in the Communication deserve support, although in many points they should be particularized by the European Commission. On this note, Poland stresses the need for conducting deepened analysis as to whether the establishment of new structures is truly necessary and whether the tasks planned in the Communication could be rather implemented by the already existing structures/bodies. At the same time, Poland declares active participation in the actions undertaken at the EU level.

VIII. THE LEADING MINISTRY'S MANAGEMENT REPRESENTATIVE AUTHORISED TO PRESENT THE POSITION

Ms. Anna Streżyńska, Minister of Digital Affairs of the Republic of Poland