Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary

1. The Government hereby approves the National Cyber Security Strategy of Hungary laid down in Annex No. 1.

2. The Government instructs the state secretary heading the Prime Minister's Office to take the necessary action to establish the National Cyber Security Coordination Council.

Person in charge: State secretary heading the Prime Minister's Office, supported by the ministers with the relevant responsibilities and powers
Deadline: 30 June 2013

3. The Government instructs the state secretary heading the Prime Minister's Office to prepare a work and action plan for implementing the tasks defined in the National Cyber Security Strategy of Hungary.

Person in charge: State secretary heading the Prime Minister's Office, supported by the ministers with the relevant responsibilities and powers
Deadline: 30 June 2013

4. This decision shall come into force on the day after its publication.

Viktor Orbán
Prime Minister
(signed)

Annex 1 to Government Decision No. 1139/2013 (21 March)

National Cyber Security Strategy of Hungary

1. In accordance with the principles of the Fundamental Law and based on the review of the relevant values and interests and on the analysis of the security environment of the cyberspace, the purpose of this Strategy is to determine national objectives and strategic directions, tasks and comprehensive government tools which enable Hungary to enforce its national interests in the Hungarian cyberspace, within the context of the global cyberspace. The strategy aims at developing a free and secure cyberspace and protecting national sovereignty in the national and international context, which has undergone a significant change due to the emergence of the cyberspace, a new medium which has become a key factor in the 21st century. Furthermore, it aims at protecting the activities and guaranteeing the security of national economy and society, securely adapting technological innovations to facilitate economic growth, and establishing international cooperation in this regard in line with Hungary's national interests. This Strategy indicates that Hungary is ready to perform and take responsibility for cyberspace protection tasks and intends to develop the Hungarian cyberspace as a key element of Hungarian economic and social life into a free, secure and innovative environment. By way of efficient protective measures based on prevention, the primary objective is to manage the threats and risks emerging in and coming from the cyberspace, as well as to reinforce government coordination and measures.

2. This Strategy reflects the basic values enshrined in the Fundamental Law of Hungary, specifically freedom, security, rule of law, international and European cooperation, in a separate field within security and economic policy; it is a document of cyber security for national data assets as part of national assets, derived from Section 38 of the Fundamental Law, as well as for the related critical infrastructures. In accordance with the Hungarian National Security Strategy, accepted by Government Decision No. 1035/2012 (21 February), and based thereupon, the Strategy elaborates the government efforts and responsibility laid down in Section 31 thereof. Its roots date back to the Budapest Convention adopted in 2001 ("Convention on Cybercrime"); an international agreement defining internationally recognised principles used as a reference. At the same time, the Strategy is in conformity with the recommendations of the European Parliament for the Member States included in Decision No. 2012/2096(INI) on cyber security and defence, adopted on 22 November 2012, and with the joint communication published by the European Commission and the High Representative of the Common Foreign and Security Policy of the European Union on 7 February 2013 under the title "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace". Furthermore, the Strategy is in line with the Strategic Concept of the NATO accepted in November 2010, the Cyber Security Policy of the Organisation adopted in June 2011 and its implementation plan, as well as with the cyber protection principles and objectives set forth in the documents of the NATO summits held on 19-20 November 2010 in Lisbon and on 20-21 May 2012 in Chicago.

I. The cyber security environment in Hungary

3. Cyberspace means the combined phenomenon of globally interconnected, decentralised and ever-growing electronic information systems as well as the societal and economic processes appearing in and through these systems in the form of data and information. The Hungarian cyberspace includes the parts of the electronic information systems of the global cyberspace which are located in Hungary, as well as the societal and economic processes appearing in and through the electronic systems of the global cyberspace in the form of data and information that take place in, are directed to, or affect Hungary.

4. The increasing number and various sources of threats emerging in cyberspace as well as the increasing order of magnitude of their consequences indicate that the number and efficiency of public and non-public users has grown rapidly for the past decade who use cyberspace to illegally acquire critical data or information and disrupt communication and information systems. Our vital electronic information systems and consequently, the functioning of our critical infrastructures are threatened by a new form of warfare, information warfare, making cyberspace one of the most important theatres in modern warfare. In addition to the damage caused by external factors, the inadequate regulation of the operational security of the information and communication systems constituting cyberspace poses a further risk. Dynamic emerging new technologies, such as cloud computing or mobile Internet, lead to the continuous evolution of new security risks. One of the key objectives of this Strategy is to create awareness and capacity at the political and professional decision making level which can manage the new cyber security challenges arising from technological progress by flexibly adapting to them in the foreseeable future.

5. Cyber security is the continuous and planned taking of political, legal, economic, educational, awareness-raising and technical measures to manage risks in cyberspace that transforms the cyberspace into a reliable environment for the smooth functioning and operation of societal and economic processes by ensuring an acceptable level of risks in cyberspace.

II. Hungary's set of values, vision and objectives relating to cybersecurity

6. The protection of Hungary's sovereignty in the Hungarian cyberspace is a national interest, too; a free, democratic and secure functioning of the Hungarian cyberspace based on the rule of law is regarded as a fundamental value and interest. In Hungary, the freedom and security of cyberspace is ensured through the close cooperation and coordinated activities between Government, academia, business sector and civil society based on their shared responsibility.

7. Hungary aims at establishing and maintaining trust-based cooperation with all public and private actors of the global cyberspace sharing the same set of values with Hungary, and endevours to guarantee free and secure use of the global cyberspace through its allies and international relations, particularly the EU and the NATO, the Organization on Security and Cooperation in Europe (OSCE), the United Nations, the Council of Europe and other international organisations in which the country is a member. Being aware of the fact that threats and attacks emerging in cyberspace may escalate to the level requiring allied cooperation, Hungary considers it highly important that cybersecurity has become an issue for

collective defence under Article 5 of the founding treaty of NATO. Hungary is interested in this allied international cooperation for the sake of its own security, too. Hungary regards the Central and Eastern European region with special attention, where cybersecurity can be further improved within the framework of regional cooperations.

8. To address present and future challenges, Hungary lays down the requirement that the Hungarian cyberspace shall provide a secure and reliable environment:

a) for individuals and communities to ensure social development and integration through communication based on liberty, freedom from fear, and guaranteeing the protection of personal data,

b) for the business sector to develop efficient and innovative business solutions,

c) for future generations to ensure value-based learning and unharmed collection of experiences resulting in a sound mental development,

d) for electronic public administration, to promote innovative and cutting-edge development of public services.

9. In the interest of a free and secure use of cyberspace, Hungary lays downs the following objectives to be met by aligning the interests of national security, efficient crisis management and user protection:

a) to have efficient capabilities to prevent, detect, manage (react), respond to and recover any malicious cyber activity, threat, attack or emergency, as well as accidental information leakage,

b) to provide adequate protection for its national data assets, to ensure the operational safety of the parts of its critical infrastructures linked to cyberspace, and to have a rapid, efficient mitigating and recovery capability in case of a compromise, deployable also during a state of emergency,

c) to ensure that the quality of IT and communication products and services necessary for the secure operation of the Hungarian cyberspace meet the requirements of international best practices, with special emphasis on compliance with international security certification standards,

d) to ensure that the quality of education, training as well as research and development meets the requirements of international best practices, thus contributing to the establishment of a world-class national knowledge pool,

e) to ensure that the establishment of a secure cyberspace for children and future generations meets the requirements of international best practices.

III. Tasks necessary to meet the objectives

10. The cybersecurity situation of Hungary is fundamentally solid. Arising from the special structure of cyberspace, however, a number of security risks and threats constituting a strategic challenge to the nation need to be considered. The tools available for maintaining and improving the level of cybersecurity and to meet the objectives, as well as the areas affected by fulfilling the tasks are the following:

a) Government coordination. Primarily, each government institution assumes its own responsibility for the free and secure use of cyberspace. However, due to the complexity of this area, these responsibilities can only meet the Government's objective regarding a free and secure use of cyberspace through a clear and efficient government coordination. Therefore, the central government coordination through the Prime Minister's Office shall be strengthened, a mandatory step for the

coordinated and concentrated use of government and sectoral resources.

b) Cooperation. Improved cooperation and efficient information sharing are needed to meet our objectives and cybersecurity interests. To this end, it is necessary to create operational cooperation fora ensuring the participation of representatives of business sector and academia in preparing governmental decision making, enabling the members of these fora to put forward recommendations or opinions on the development and continuous improvement of cybersecurity activities.

c) Specialised institutions. Cybersecurity tasks should be assigned to organisations with specific skills and powers, cooperating not only with each other but also with other authorities responsible for data protection and classified information protection. These tasks affect organisations responsible for national security, defence, law enforcement, disaster management and critical infrastructure protection, as well as authorities responsible for electronic information security. Cybersecurity incidents are handled by the Government Incident Response Centre as an accredited member of the European Governmental CERT Group, as well as the Sectoral Incident Response Centres in various sectors.

d) Regulation. In addition to a complex legislation, it is necessary to conclude cooperation agreements with actors of civil society, business sector and academia to provide an adequate basis and regulation for the efficient operation of cybersecurity based on shared responsibility.

a) International cooperation projects. Hungary wishes to enhance its role in cyberdefence initiatives and cooperation projects within the EU and the NATO, as well as in the cybersecurity cooperation projects of the UN and the OSCE. It strives to carry on and expand cooperation regarding cyberdefence exercise and planning within the EU and the NATO, and maintain its leading role in developing and running operational government cooperations, as well as in the Central and Eastern European region. Hungary lays special emphasis on implementing activities that are, on the one hand specified by the Digital Agenda of the European Union for the Member States and, on the other hand, prescribed by the NATO Cyber Security Policy and its implementation plan for allies. Hungary deems the North Atlantic cooperation very important in respect of cyber security. Hungary continues to play an active role in the European, Atlantic and global organisations of national/governmental and Sectoral Incident Handling Centres, in the European Network and Information Security Agency, and in the Board of European Electronic Communications Authorities.

e) Awareness. Hungary maintains its leadership in organising Hungarian and international cybersecurity forums. Through its specialised institutions and via cooperation with actors of civil society, business sector and academia, it supports activities for the secure use of cyberspace and raising awareness, as well as initiatives promoting practical cybersecurity skills, with special focus on awareness-raising among individual users and small and medium-sized enterprises.

f) Education, research & development. Hungary pays particular attention to integrating cyber security as a field in the information technology syllabus of primary, secondary and higher education, in training courses for government officials and in professional training courses. Hungary strives for strategic cooperation with university and scientific research centres which have achieved outstanding and internationally recognised results in cybersecurity research and development and help to establish cybersecurity centres of excellence.

b) Child protection. Hungary regards the creation and maintenance of an environment allowing the healthy development of children as a basic element of

cybersecurity, and treats it as a priority in all affected areas, achieving, at the same time, the objectives of the European Strategy for a Better Internet for Children. Particular emphasis is laid on encouraging the creation of quality online content for young people, supporting awareness-raising and preparatory measures, the prevention of the harassment and exploitation of children, and the establishment of a secure online environment. For this purpose, Hungarian non-governmental organisations with a proven record in online child protection are regarded as key partners.

g) Motivation of business actors. In determining cyber security requirements for public procurement tenders in information technology and communications, Hungary intends to encourage equipment manufacturers and service providers submitting bids to create the highest possible level of cybersecurity, with special emphasis on compliance with international certification standards. Furthermore, Hungary wishes to cooperate with business actors to develop incentive measures for cybersecurity improvement.

IV. Government tools that are available or in need of reinforcement for implementing the National CyberSecurity Strategy

11. Hungary is already in the possession of most tools required to meet its strategic objectives as regards capabilities and potential resources, including:

a) stocktaking and coordination of the government organisations responsible for the security of the Hungarian cyberspace, establishment of efficient cooperation;

b) review of the civil society, business and academic organisations responsible for the security of the Hungarian cyberspace, establishment of institutional cooperation;

c) stocktaking of critical information infrastructures and critical assets, as well as national data assets, in addition, ensuring their protection;

d) operation of specialised Government institutions;

e) provision of a regulatory environment;

f) participation in international and regional cooperation at political, operational and regulatory levels;

g) establishment of a support framework for research & development, education and awareness-raising;

h) establishment of business motivation systems;

i) integrating cybersecurity aspects in technical developments under state control and in tasks related to the development and operation of the Government's information systems.

12. The reinforcement and more efficient use of the available tools and their more effective practical application in terms of national security require the establishment and operation of a system for intra-governmental and non-governmental cooperation.