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 working 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 emerging in and coming from the cyberspace, along with the related risks, as well as to reinforce Government coordination and the range of available tools.

2. This Strategy reflects the basic values enshrined in the Fundamental Law of Hungary, specifically freedom, security, justice, international and European cooperation, in a separate field of 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 vital systems and facilities. In accordance with the Hungarian National Security Strategy, accepted through Government Decision No. 1035/2012 (21 February), and using it as a basis, the Strategy elaborates on the endeavours and Government responsibilities mentioned in Section 31. Its roots go back to the Budapest Convention adopted in 2001 ("Convention on Cybercrime"); an international convention which defines internationally recognised principles and is still used as a reference. At the same time, the Strategy is aligned 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 Conception 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 combination of globally interconnected, decentralised and ever-growing electronic information systems, and social and economic processes represented in the form of data and information through these systems. The Hungarian cyberspace is a part of the electronic information systems of the global cyberspace located in Hungary, as well as social and economic processes represented in the form of data and information through the electronic systems of the global cyberspace which take place in, are directed to, or affect Hungary.

4. The increasing number of threats emerging in the cyberspace from several sources, whose consequences have also become considerably more severe, indicate that the number and efficiency of public and non-public users using the cyberspace for the illegal acquisition of critical data and information and for causing damage to communication and information systems has grown rapidly over the past few decades. This new form of warfare, called information warfare, which has rendered the cyberspace one of the most important theatres of operations in modern warfare, threatens the functioning of our vital electronic information systems and hence our vital systems and facilities. In addition to the external damage caused, a further risk is represented by the inadequate regulation of the operational security of the information and communication systems as constituents of the cyberspace. Dynamically developing new technologies, such as the cloud or mobile Internet, lead to the continuous emergence of new security risks. A key objective of this Strategy is to establish a political and professional decision-making focus and ability which will allow in the foreseeable future, by flexible adaptation, the proper management of new cyber security challenges arising from technological progress.

5. Cyber security is the ongoing and planned application of political, legal, economic, educational, awareness-raising and technical tools capable of managing cyberspace risks, transforming the cyberspace into a reliable environment by ensuring an acceptable level of such risks for the smooth functioning and operation of social and economic processes.

II. Hungary's cyber security values, vision and objectives

6. The protection of Hungary's sovereignty is a national interest in the Hungarian cyberspace too; a free and secure operation of the Hungarian cyberspace in line with the rules of democracy and law is regarded as a vital value and interest. In Hungary, the freedom and security of the cyberspace is ensured through the close cooperation and coordinated activities of the Government and the scientific, economic and civil communities, on the basis of joint responsibility.

7. Hungary strives to establish and maintain cooperation based on mutual trust with all public and non-public actors of the global cyberspace representing similar values, and endeavours to guarantee a 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. Hungary is aware that cyberspace threats and attacks may reach a level which would require the cooperation of allies, and regards it as crucial that the issue of cyber security has been included in the scope of collective protection under Article 5 of the foundation document of the NATO. Hungary is interested in this international alliance cooperation for the sake of its own security too. Hungary

pays special attention to the Central and Eastern European region, and sees room for improvement regarding cyber security in this region through regional cooperation.

8. To meet present and future challenges, Hungary stipulates 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 free and secure communication guaranteeing the protection of personal information,
b) for economic actors, to develop efficient and innovative business solutions,
c) for future generations, to ensure value-based education and the collection of experiences resulting in healthy, undisturbed mental development,
d) for electronic public administration, to promote the innovative and future-oriented development of public services.

9. To promote a free and secure use of the cyberspace, Hungary declares the following objectives, to be achieved by aligning the interests of national security, efficient crisis management and user protection:

a) to have efficient capabilities to prevent, detect, manage (respond to), address and correct any malicious cyber activity, threat, attack or emergency, as well as accidental information leakage,
b) to provide appropriate protection for its national data assets, to ensure the operational safety of the cyberspace functions of its vital systems and facilities, and to have a sufficiently fast, efficient loss-minimising correction system in situations where a compromise occurs, which can also be used at times of a special legal order,
c) to ensure that the quality of IT and communication products and services required for a secure operation of the Hungarian cyberspace reaches international standards, with special emphasis on compliance with international security certification standards,
d) to ensure that the standard of cyber security education, training and research & development is consistent with international best practices, promoting the establishment of a world-class Hungarian knowledge base,
e) to ensure that the establishment of a secure cyberspace for children and future generations is consistent with international best practices.

III. Tasks required for the above objectives

10. Hungary's cyber security situation is mostly stable. However, owing to the special structure of the cyberspace, it is necessary to consider a number of security risks and threats that pose a challenge to the nation. The tools available for maintaining and improving the level of cyber security and for achieving the objectives set in the affected areas include:

a) Government coordination. Basically, all Government bodies are individually responsible for a free and secure use of the cyberspace. However, due to the complexity of this area, these responsibilities can only lead to the achievement of the Government's objective regarding a free and secure use of the cyberspace through clear and efficient Government coordination. Therefore, there shall be special focus on the improvement of general Government coordination through the Prime Minister's Office, which is a prerequisite for the coordinated and concentrated use of government and

sectoral resources.

b) Cooperation. Our cyber security interests and goals call for improved cooperation and efficient information exchanges. To this end, it is necessary to create operational cooperation forums for representatives of the economic and scientific sectors in the Government's decision-making support processes, and to enable the members of these forums to put forward recommendations or opinions on the development and continuous improvement of cyber security activities.

c) Specialised institutions. Cyber security tasks should be assigned to organisations with specific skills and powers, which cooperate not only with one another but also with other organisations performing official functions in data and confidentiality protection. These tasks require contributions from organisations responsible for national defence, law enforcement, disaster prevention and vital institution and facility protection, as well as from institutions performing official functions in the field of electronic information security. Cyber security tasks are performed by the Government Incident Management Centre as a member organisation accredited by the European Governmental CERT Group, as well as the Sectoral Incident Management Centres in various sectors.

d) Regulation. In addition to a multi-stage legislative activity, it is necessary to conclude cooperation agreements with actors of the civil, economic and scientific sectors, to provide an adequate basis and set the terms and conditions for efficient cyber security operation on the basis of joint responsibility.

e) International cooperation projects. Hungary wishes to reinforce its role in cyber protection initiatives and cooperation projects within the EU and the NATO, as well as in the cyber security cooperation projects of the UN and the OSCE. It wants to carry on and expand cooperation regarding cyber protection practice and design within the EU and the NATO, and to maintain its leading role in developing and running operational government cooperation in these organisations, as well as in the Central and Eastern European region. Hungary lays special emphasis on implementing activities that are, on the one hand,

a) 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 attaches special importance to the North Atlantic cooperation 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 Management Centres, in the European Network and Information Security Agency, and in the Board of European Electronic Communications Authorities.

f) Awareness. Hungary maintains its leadership in organising Hungarian and international cyber security forums. Through its specialised institutions and via cooperation with actors of the civil, economic and scientific sectors, it supports activities for a secure use of the cyberspace and raising awareness, as well as initiatives promoting practical cyber security skills, with special focus on awareness-raising among individual users and small and medium-sized enterprises.

g) 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 retraining courses. Hungary strives for strategic cooperation with university and scientific research locations which have achieved outstanding and internationally recognised results in cyber security research and development and help establish cyber security centres of excellence.

h) Child protection. Hungary regards the creation and maintenance of an environment allowing the healthy development of children as a vital element of cyber security, which is treated 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

b) the establishment of a secure online environment. For this purpose, Hungarian non-governmental organisations which have been successful in online child protection are key partners.

i) Motivation of economic 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 cyber security, with special emphasis on compliance with international certification standards. Furthermore, Hungary wishes to cooperate with business actors to develop incentive measures for cyber security improvement.

IV. Government tools that are available and need reinforcement for implementing the National Cyber Security Strategy

11. Hungary already possesses most tools required for its strategic goals regarding both competences and the potential resources, including:

a) review and coordination of the Government organisations responsible for the security of the Hungarian cyberspace, establishment of efficient cooperation;
b) review of the civil, economic and scientific organisations responsible for the security of the Hungarian cyberspace, establishment of institutional cooperation;
c) review of vital information infrastructures and assets and national data assets, as well as 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 economic motivation systems;
i) enforcement of the aspects of cyber security 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.