László KOVÁCS

OBAMA'S NEW CYBERSPACE POLICY

OBAMA ÚJ CYBERTÉRI POLITIKÁJA

Jelen írás fő célja, hogy bemutassa Barack Obama amerikai elnök új, a cyberteret érintő politikáját. A 2009 májusában megjelent dokumentum felvázolja mindazokat a célokat és elképzeléseket, amelyekkel az Egyesült Államok információs és kommunikációs infrastruktúrájának biztonsága, valamint rugalmas működése megteremthető és fenntartható.

This paper main goal is to highlight the new cyberspace policy of President Barack Obama which was released in late of May 2009. The document includes measures and action plans in cyberspace and on the field of critical information infrastructures to assure a trusted and resilient information and communications infrastructure to the United States.

INTRODUCTION

The cyberspace is often defined as the interdependent network of information infrastructures. It includes the Internet, telecommunications networks, computer systems, and rooted processors and controllers in critical industries. Nowadays, the military information systems are also part of the cyberspace. Common usage of the term also refers to the virtual environment of information and interactions between people.

Today the cyberspace is real, many industrial, social, political, economic, security and cultural operations and actions take place in it.

In addition to the cyberspace includes many critical information infrastructures which are vital for our everyday life. Thus their protection is particularly important on the fields of economy, defense or social fields. The western countries, especially the United States heavily depend on these infrastructures.

President Barack Obama ordered shortly after taking his office to examine the government's current cyber security actions to inform him on how the government should guarantee this area. This examination was a 60-day review which conclusions and recommendations were published in a 76-page document titled *Cyberspace policy review.*[1]

CYBERSECURITY MEASURES AND ACTIONS BEFORE OBAMA

Before the Obama administration numerous cyber security measures and actions had been ordered by President Clinton and President Bush. For example[2]:

- *Presidential Decision Directive 63 (PDD-63):*
  It was signed in May 1998. This directive intended that the United States would take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on its critical infrastructures, including especially the cyber systems of the U.S.

[1] According to the policy review, the cyberspace policy "as used in this document includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. The scope does not include other information and communications policy unrelated to national security or securing the infrastructure." [1; p: 2]

[2] Although the USA PATRIOT Act of 2001 is also an important step toward on this field, it is not listed here.

- *The National Strategy to Secure Cyberspace:*
  This strategy was released in 2003. According to this strategy's main aim it is an implementing component of the National Strategy for Homeland Security and is complemented by a National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. Another purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. [2]
- *Homeland Security Presidential Directive 7 (HSPD-7):*
  President Bush signed this directive in 2003. It established a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. [3]
- *Comprehensive National Cyber security Initiative (CNCI):*
  In 2007, this initiative main aim was to give a "bridge" to historically separate cyber defensive missions with law enforcement, intelligence, counterintelligence, and military capabilities to address the full spectrum of cyber threats from remote network intrusions and insider operations to supply chain vulnerabilities. [1; p: 4] The CNCI strategy was codified in NSPD-54/HSPD-23 directives.

Nevertheless, many cyber attacks, cyber incidents, cyber crimes and malicious activities have executed in cyberspace during the last 10-12 years, which affected U.S. competitiveness, degraded privacy and civil liberties protections, undermined national security, or caused a general erosion of trust, or even crippled society. [1; p:2.]
The new cybersecurity policy review cites three examples to confirm the cyber threats:

- Failure of critical infrastructures. CIA reports malicious activities against information technology systems have caused the disruption of electric power capabilities in multiple regions overseas, including a case that resulted in a multi-city power outage.[3]
- Exploiting global financial services. In November 2008, the compromised payment processors of an international bank permitted fraudulent transactions at more than 130 automated teller machines in 49 cities within a 30-minute period, according to press reports.[4] In another case reported by the media, a U.S. retailer in 2007 experienced data breaches and loss of personally identifiable information that compromised 45 million credit and debit cards.[5]
- Systemic loss of U.S. economic value. Industry estimates of losses from intellectual property to data theft in 2008 range as high as $1 trillion.[6] [1; p:2.]

OBAMA'S CYBERSPACE POLICY REVIEW

The new cyberspace policy review summarizes the examination team[7] outlines and suggestions initial areas of action to help the United States achieve a more reliable, flexible, and trustworthy information infrastructure for the future. The document emphasizes that it does not provide an in-depth analysis of options or an extensive audit of programs. Instead, it presents the need for greater coordination and integrated development of policy. [1; p:4.]
The paper structure includes five key topics and three annexes which are the following:

1. leading from the top;
2. building capacity for a digital nation;
3. sharing responsibility for cyber security;
4. improving information sharing and incident response;

[3] http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5

[4] http://www.bankinfosecurity.com/articles.php?art_id=1197

[5] http://www.infoworld.com/d/security-central/retailer-tjx/reports-massive-data-breach-952

[6] http://www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html

[7] The team was led by Melissa Hathaway, the interim White House cybersecurity advisor and former intelligence official. [4] Today she is the top cyberofficial at the National Security Council.

5. building the architecture of the future.

Annexes:

a. bibliography;
b. methodology of the study;
c. brief history of modern communications technology.

The new cyber security policy is „strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.*"* [1; p:2]

NEW CYBERSECURITY CZAR IS NEEDED

At the same time with the policy review was published President Barack Obama confirmed that the White House would be creating a new office to be led by a cyber security czar. (The governmental officials are not using the term czar, but it is commonly use in the newspapers and the media. The White House uses the term of coordinator instead of czar). The new office was suggested by the cyber security policy review team.

The main reason is to establish new cyber security office that "currently, no single individual or entity has the responsibility to coordinate Federal government cyber security-related activities. Independent efforts will not be sufficient to address this challenge without a central coordination mechanism, an updated national strategy, an action plan developed and coordinated across the Executive Branch, and the support of Congress." [1; p:7.]

According to the originally plan the coordinator will be responsible for organizing and integrating all cyber security policies for the government. The official will work with the Office of Management and Budget (OMB) to ensure that agencies have money allocated for cyber security priorities, and coordinating the government's answers to the major cyber incidents.

The main tasks of the new office and its leader are the following:

- The cyber security policy official should harmonize cyber security-related policy and technology efforts across the Federal government, ensure that the President's budget reflects federal priorities for cyber security, and develop a legislative agenda, all in consultation with the Federal government's Chief Technology Officer and Chief Information Officer—along with the appropriate entities within the Office of Management and Budget, the Office of Science and Technology Policy (OSTP), and the NEC;
- The czar also would make crisis management as the White House action officer for cyber incident response. It is a similar role to the action officers who help the White House monitor terrorist attacks or natural disasters;
- The cybersecurity policy official should prepare for the President's consideration an updated national strategy to secure the information and communications infrastructure;
- The official should help coordinate intelligence and military policies and strategies for cyberspace—including for countering terrorist use of the Internet—to ensure integration of all mission equities. The cybersecurity policy official should engage external advisory bodies;
- The new official should work with departments and agencies to recommend coherent unified policy guidance where necessary in order to clarify authorities, roles, and responsibilities for cybersecurity-related activities across the Federal government. [1; p:7-8.]

However, there is a huge fear on the side of civil liberties advocates that the office and the czar has got too much rights and they will violate privacy and civil liberties of U.S. citizens.

Regarding to this fears the President immediately declared: "Our pursuit of cyber security will not include — I repeat, will not include — monitoring private sector networks or internet traffic. We will preserve and protect the per-

sonal privacy and civil liberties that we cherish as Americans. Indeed, I remain firmly committed to net neutrality so we can keep the internet as it should be, open and free." [5]

It is necessary to mention that before this policy review a new Cyber Command was established by Department of Defense in April 2009. The new command main task is to execute military cyber security operations and provide support to civil authorities. Defense Secretary Robert Gates nominated the director of the National Security Agency to head the new Pentagon Cyber Command. [6] In addition to, in May 2009, U.S. Air Force announced it would establish a 400-person cyber headquarters and opcenter. The new HQ will deploy in Lackland Air Force Base (San Antonio, Texas), with main mission to coordinate cyber defense with other services. This mission includes possibilities of launch offensive cyber attacks when it is necessary. [7]

However, it is not clear yet which relations and coordination will be established between the Cyber Command and the new White House official.

NEW CYBERSECURITY STRATEGY OF THE GOVERNMENT: NEAR- AND MID-TERM ACTION PLANS

The review recommends a near-term and a mid-term action plan. These plans include major and essential steps toward securing the cyberspace and protect the critical information infrastructures.

The near-term actions include the following steps:

- Appoint a cyber security policy official responsible for coordinating the Nation's cyber security policies and activities; establish a strong NSC directorate, under the direction of the cyber security policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cyber security-related strategy and policy.
- Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.
- Designate cyber security as one of the President's key management priorities and establish performance metrics.
- Designate a privacy and civil liberties official to the NSC cyber security directorate.
- Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cyber security-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cyber security-related activities across the Federal government.
- Initiate a national public awareness and education campaign to promote cyber security.
- Develop U.S. Government positions for an international cyber security policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cyber security.
- Prepare a cyber security incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement
- In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.
- Build a cyber security-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation. [1; p:37.]

The suggested mid-term actions are the following:

- Improve the process for resolution of interagency disagreements regarding interpretations of law and application of policy and authorities for cyber operations.

- Use the OMB program assessment framework to ensure departments and agencies use performance-based budgeting in pursuing cybersecurity goals.
- Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy.
- Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the Federal government.
- Determine the most efficient and effective mechanism to obtain strategic warning, maintains situational awareness, and informs incident response capabilities.
- Develop a set of threat scenarios and metrics that can be used for risk management decisions, recovery planning, and prioritization of R&D.
- Develop a process between the government and the private sector to assist in preventing, detecting, and responding to cyber incidents.
- Develop mechanisms for cyber security-related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial.
- Develop solutions for emergency communications capabilities during a time of natural disaster, crisis, or conflict while ensuring network neutrality.
- Expand sharing of information about network incidents and vulnerabilities with key allies and seek bilateral and multilateral arrangements that will improve economic and security interests while protecting civil liberties and privacy rights.
- Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations.
- Use the infrastructure objectives and the research and development framework to define goals for national and international standards bodies.
- Implement, for high-value activities (e.g., the Smart Grid), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy.
- Refine government procurement strategies and improve the market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services. [1; p:38.]

SUMMARY

President Barack Obama ordered an examination of the government's cyber security actions shortly after he took president's office.

The examination team revised the cyber security directives and actions before Obama administration. The team executed a 60-day review and summarized its suggestions and plans for the future in a cyber security policy review. This document suggests a series of improvements. The recommended near- and mid-term plans includes actions to protect the cyberspace in the U.S. which are major steps toward better securing the nation's information systems, computer networks and critical information infrastructures.

Keywords: cyber space, cyber strategy, critical information infrastructure

Kulcsszavak: cyber tér, cyber stratégia, kritikus információs infrastruktúra

REFERENCES

[1] Cyberpolicy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure, Washington D.C. 2009
http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (Downloaded: 19 August, 2009)

[2] The National Strategy to Secure Cyberspace, Washington D.C. February, 2009.
http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (Downloaded: 19 August, 2009)

[3] Homeland Security Presidential Directive-7, Washington D.C. December 17, 2003
http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1 (Downloaded: 19 August, 2009)

[4] NAKASHIMA, Ellen: Obama Set to Create A Cybersecurity Czar With Broad Mandate. in: Washington Post, May 26, 2009
http://www.washingtonpost.com/wp-dyn/content/article/2009/05/25/AR2009052502104.html (Downloaded: 19 August, 2009)

[5] ZETTER, Kim: Obama Says New Cyberczar Won't Spy on the Net.
http://www.wired.com/threatlevel/2009/05/netprivacy/ (Downloaded: 19 August, 2009)

[6] GORMAN, Siobhan: Gates to Nominate NSA Chief to Head New Cyber Command. in: The Wall Street Journal, April 24, 2009
http://online.wsj.com/article/SB124060266381953839.html

[7] IANNOTTA, Ben: Coordinator in Chief. in: C4ISR Journal. 2009. July. Vol. 8, No 6. p.: 20-21.