HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

ISTVÁN PARÁDA[1]

Cyberstrategy of United States – Chronology Process in the Light of the Goals

Az Egyesült Államok Kiberstratgiája – a kronológia folyamata a célok fényében

Abstract

Thanks to continuous technological progress and the emergence of new security challenges and threats, they become part of the daily activities of military activities. The capabilities and the ever-increasing tendencies have been recognized by NATO (North Atlantic Treaty Organization), the European Union, the United States of America and Hungary. Our country, the National University of Public Service and the Hungarian Defense Forces are facing major challenges in the development, creation and application of cyber-security and cybercrime capabilities. It is therefore important to examine the US strategy for the United States, to systematize the documents adopted at the meetings, which are related to the cyber defense efforts.

Key Words: Cyberstategy, Critical Infrastucture, Department of Defense

Absztrakt

A folyamatos technológiai fejlődésnek köszönhetően, valamint, az újabb biztonsági kihívások és fenyegetések megjelenésével a kiberműveletek a katonai tevékenységek mindennapi részévé váltak. Ezen képességek létjogosultságát és folyamatosan növekvő tendenciáit a NATO (North Atlantic Treaty Organization), az Európai Unió, az Amerikai Egyesült Államok és Magyarország is felismerte. Hazánk, a Nemzeti Közszolgálati Egyetem (mint felsőoktatási szereplő), valamint a Magyar Honvédség is jelentős kihívásokkal áll szemben a kiberhadviselésen és

[1] Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar – National University of Public Service, Faculty of Military Science and Officer Training, E-mail:parada.istvan@uni-nke.hu ORCID: 0000-0002-3083-6015 A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült. *The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance.*

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

a kiberműveleteken belüli képességek fejlesztése, létrehozatala és alkalmazása terén. Éppen ezért fontos megvizsgálni az Amerikai Egyesült Államok kiberstratégiáját, rendszerezni a találkozókon elfogadott dokumentumokat, melyek kapcsolódnak a kibervédelmi erőfeszítésekhez.

Kulcsszavak: Kiberstartégia, Kritikus Infrastruktúra, Védelmi Minisztérium

INTRODUCTION

In the information society, information infrastructures encompass our everyday lives. This results in the people connect to a network, to the cyberspace. We are online every hour of the day. Thanks to the continuous technological advances and the emergence of new security challenges and threats, cybercrime has become a daily part of private life, public service, and military activities. We live in the world of network connections. Companies and countries rely on cyberspace the movement of the military forces and internal security up to financial transactions. The computer technology blurs the line between the digital, cyber and the physical world. The justification and the ever-increasing tendencies of these capabilities have been recognized by NATO (North Atlantic Treaty Organization), the European Union, the United States of America and Hungary. The United States military service relies on secure networks and data to carry out its missions. The United States (in the following US) is committed to an open, secure, interoperable and reliable Internet enabling prosperity, public security and the free flow of trade and ideas. These are the properties the Internet reflects the fundamental American values. Worldwide, the US stands at the forefront of cybersecurity policy and strategy. Already in 2003, the government issued the first national computer security strategy.[2] *The National Cyber Security Strategy of 2003* established three strategic objectives: preventing cyber-attacks against critical infrastructures; minimize vulnerability to cyber-attacks; decrease the damage done to cyber-attacks and reduce the recovery time. To achieve these goals, five national priorities have been defined: provision of federal computer systems and networks; development of reaction power; creating a threat and vulnerability reduction program; awareness-raising and training program for cybersecurity; and the system of international cooperation. In the next sections, chronologically, you will review the most important strategic documents and federal legislation, including enforceable executive orders by US Presidents on cybersecurity. These documents include the protection of national critical infrastructure and the security of federal computer systems and networks; designating the role and responsibilities of federal, state, local, tribal, territorial and private partners; as well as cyber security aspects of international and national security, defense, and counterintelligence.

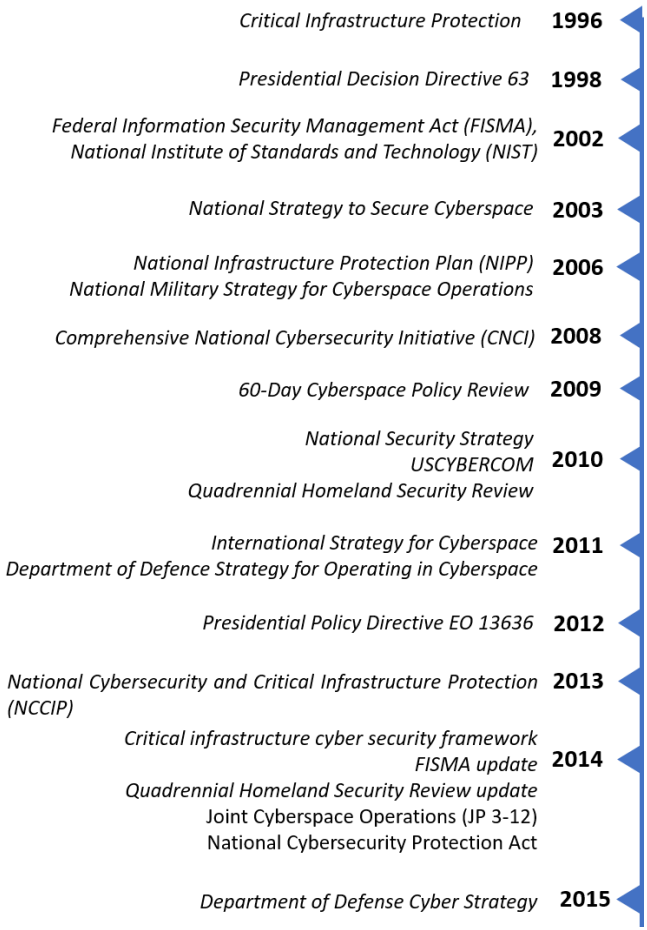
[2] The White House, 'The National Strategy to Secure Cyberspace', 2003 https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (Download 2018. 01. 21)

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

US CYBER STRATEGY CHRONOLOGICAL PROCESS

Cybersecurity in the early nineties became an uncomfortable problem with vital national security. The US cybersecurity directive is rooted in critical infrastructural defense efforts that he has even published under a Clinton administration. In 1996, President Bill Clinton issued the Executive Order 13010 on "*Critical Infrastructure Protection*"[3]. The decision set up the Critical Infrastructure Presidency Committee, which drew attention to cyber-attacks and national security threats. The United States Strategic approach to *Critical Infrastructure Protection* (CIP) focuses on public-private partnerships, while government agencies coordinate and define responsibilities. The 63rd Presidential DECISION DIRECTIVE (in the following PDD) of 1998[4] established a structure under the leadership of the White House to coordinate the activities of the federal government to protect critical infrastructures against cyber-attacks. PDD 63 established many cybersecurity-related organizations within the government including the National Coordinator for Security, Infrastructure Protection, and Counterterrorism with an Office of Critical Infrastructure to support the Coordinator and the



1. Figure the main documents regarding the development of cyberstrategy

[3] Executive Order 13025 - Amendment to Executive Order 13010, the President's Commission on Critical Infrastructure Protection November 13, 1996, https://www.gpo.gov/fdsys/pkg/WCPD-1996-11-18/pdf/WCPD-1996-11-18-Pg2390-3.pdf (Download 2018. 01. 11)

[4] PRESIDENTIAL DECISION DIRECTIVE/NSC-63 THE WHITE HOUSE WASH INGTON May 22, 1998 https://fas.org/irp/offdocs/pdd/pdd-63.pdf (Download 2018. 01. 11)

National Infrastructure Protection Center.[5]

The *Federal Information Security Management Act* (in the following FISMA), as part of *the 2002 E-Government Act*[6], applied a risk management framework developed by the *National Institute of Standards and Technology* (in the following NIST) to standardize cybersecurity processes among US governmental organizations. As a result of this event, Federal Chief Information Officer (OMB), this is responsible for overseeing the government's technological use, both in terms of spending and strategy. It clarified and strengthened NIST's responsibility to develop security standards for federal computer systems (with the exception of defense and intelligence systems), established a central federal incident headquarters and made OMB responsible for publishing federal cybersecurity standards.

In the beginning, the George W. Bush administration continued the Clinton approach, but because of the attacks of 11 September, their point of view was significantly redirected to the physical attacks of terrorist groups. The *National Strategy to Secure Cyberspace*[7] was published in 2003 but has been criticized as a comprehensive strategy paper that is bound to the ends, modes, and tools. *The Homeland Security Act*[8] established the *Department of Homeland Security* (in the following DHS) in 2002, inter alia, by coordinating the national infrastructure of critical infrastructure protection within the IT and communications sectors.45

The Homeland Security Presidental Directive 7 of 2003[9] established the identification and prioritization of critical infrastructures in the physical world and cyberspace in order to protect against terrorist attacks.47 The directive updated the role and responsibilities of different agencies outlined in the *Homeland Security Act in 2002* and in other documents. Confirmed DHS's responsibility to coordinate total critical infrastructure protection efforts and designated the class as the leading IT and communications industry agency to share threat information, evaluate vulnerability and take appropriate security action and emergency measures, plans Furthermore, he instructed DHS to produce a *National Infrastructure Protection Plan* (in the following NIPP), which is a federal government y and the Critical Infrastructure Owners and Operators. Therefore, they published The *National Infrastructure Protection Plan* in 2006[10]. During the Bush administration, a cybersecurity was complicated, with limited leadership and divided responsibility between the White House, Homeland Security and Department of Defense (in the following DoD). Homeland Security

[5] Who Should Lead U.S. Cybersecurity Efforts? By Kevin P. Newmeyer 2012, pp. 118-119 http://cco.ndu.edu/Portals/96/Documents/prism/prism_3-2/prism115-126_newmeyer.pdf
[6] The United States Congress, 'H.R.2458 – E-Government Act of 2002. 107th Congress (2001-2002)', 2002 https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf (Download 2018. 01. 15)
[7] The White House, 'The National Strategy to Secure Cyberspace', 2003 https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (Download 2018. 01. 21)
[8] PUBLIC LAW 107–296—NOV. 25, 2002 107th Congress an Act To establish the Department of Homeland Security, and for other purposes. https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf (Download 2018. 01. 21)
[9] U.S. Department of Homeland Security, 'Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection', 2003 http://www.dhs.gov/homeland-security-presidential-directive-7 (Download 2018. 01. 21)
[10] National Infrastructure Protection Plan 2006 https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf (Download 2018. 01. 21)

has been given a comprehensive coordination role, but responsibility remains with each agency.

In 2006, the *National Military Strategy for Cyberspace Operations*[11], issued by the Supreme Command, is the first comprehensive document describing the US military's approach to cyberspace operations. The document outlined the role of US armed forces in protecting American interests in the execution of military operations in cyberspace. According to the strategy, DoD "military, intelligence and business operations rely on cyberspace to reach national military targets."

The National Security Presidential Directive 54 and the *Homeland Security Presidential Directive 23* [12] The President of George W. Bush signed in January 2008, authorized DHS and OMB to set minimum operating standards for federal government civil networks. Both directives emphasized the whole governance approach followed by the *Comprehensive National Cybersecurity Initiative* (in the following CNCI)[13] guidelines. CNCI states that it provides protection against the most direct and complete spectrum of threats and strengthens the future security environment by providing a comprehensive approach that includes law enforcement, intelligence/countermeasure, counteraction and military capabilities.
Main activities of CNCI:

- relations between federal government and state government, as well as the private sector;
- Creating or enhancing rapid reaction capability;
- developing anti-counterfeiting capabilities;
- expanding a cyber course, coordinating and redirecting research and development efforts; and
- development of deterrence strategies.

To establish a strategic framework to ensure that CNCI is properly integrated, funded and coordinated with Congress and the private sector, President Obama has initiated a cyber-governance review named *60-Day Cyberspace Policy Review*[14] in 2009. The review advised a stronger White House as well as to strengthen federal leadership and accountability for cyber security. It also identified 10 short-term actions and 14 medium-term measures to support CNCI's overall objectives.

Wider national security and defense strategies also outline the objectives of cyber security. The 2010 *National Security Strategy*[15] was the first US national security strategy to pay attention to cyber threats, and the federal government has highlighted cyber threats, emphasizing non-state terrorism, up to the activities supported predominantly by the political

[11] National Military Strategy for Cyberspace Operations Chairman of the Joint Chiefs of Staff Washington December 2006 https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf (Download 2018. 01. 21)
[12]National Security Presidential Directive 54/ Homeland Security Presidential Directive 23 The White House Washington 2008 https://fas.org/irp/offdocs/nspd/nspd-54.pdf (Download 2018. 01. 21)
[13]Comprehensive National Cybersecurity Initiative (CNCI) https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf (Download 2018. 01. 21)
[14] Cyberspace Policy Review https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-028.pdf (Download 2018. 01. 21)
[15] National Security Strategy http://nssarchive.us/NSSR/2010.pdf (Download 2018. 01. 21)

and economic state. The *2010 Quadrennial Homeland Security Review*[16] has highlighted the "protection and security of cyberspace" as one of the five major national security missions.

Based on military defense considerations approaching cyber security processes USCYBERCOM was established in 2010 and started its operation in the same year. Its military components include Military Headquarters representing military service: Army Cyber Command (ARCYBER), US Flotta Cyber Command (FCC / C10F), US Marine Corps Forces Cyberspace (MARFORCYBER), 24. Air Force (AFCYBER) Cyber Command Command CGCYBER).[17]

To implement the *National Security Strategy* and to achieve the goals set out by the *Quadrennial Homeland Security Review*, the DHS developed an action plan which named *Blueprint for Secure Cyber Future*[18] in 2011 covering two areas: critical information infrastructure and the cyber environment.

In May 2011, the White House issued *International Strategy for Cyberspace*[19] reflecting the United States' approach to international relations and the communication of national priorities. The general objective of the strategy is as follows: *The United States will operate an international, open, interoperable, secure and reliable information and communication infrastructure that supports international trade and trade strengthens international security and promotes free expression and innovation. To achieve this goal, we build and maintain an environment in which norms of responsible behavior govern the activities of states, maintain partnerships, and support the rule of law in cyberspace.*

Because of the *International Strategy for Cyberspace, The United States National Military Strategy* (2011) recognized that cyberspace was transformed into a warship in its own right and that the United States "will increase the deterrence of air, space, and cyberspace and improve the United States' ability to defeat attacks on systems or infrastructures." The DoD published the first *Department of Defence Strategy for Operating in Cyberspace.*[20]

In 2012, the Obama administration backed the legislation that would provide DHS the permission to protect critical infrastructure networks; however, the bill failed twice to concede Congress.53 In response, Obama issued the – *Improving Critical Infrastructure Cyber Security* (EO 13636).[21] This binding document for the Presidency completes all previous documents and provides a better exchange of information between the federal government and the private sector. It also sets minimum criteria for improving the security of critical

[16] Quadrennial Homeland Security Review https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf (Download 2018. 01. 21)
[17] US Department of Defense U.S. Cyber Command Fact Sheet https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf (Download 2018. 01. 21)
[18] Blueprint for Secure Cyber Future https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf (Download 2018. 01. 21)
[19] International Strategy for Cyberspace https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Download 2018. 01. 21)
[20] Department of Defence Strategy for Operating in Cyberspace https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (Download 2018. 01. 21)
[21] Improving Critical Infrastructure CyberSecurity (EO 13636) https://www.dhs.gov/sites/default/files/publications/EO-13636-Improving-Critical-Infrastructure-Cybersecurity-508.pdf (Download 2018. 01. 21)

infrastructures. The *Presidential Policy Directive The Critical Infrastructure Security and Resilience* (PPD-21)[22], issued under *EO 13636*, did not make any major changes in politics, roles, responsibilities, and programs; but called for an assessment of the existing public-private partnership model, the baseline data and system requirements for effective information exchange, and the development of situational awareness.[23] He also called for the revision of the *National Infrastructure Protection Plan (NIPP)*, and finally the highlight of the third revision of the plan in 2013. *National Cybersecurity and Critical Infrastructure Protection (NCCIP)*[24] 2013 ensure the role of DHS in cyber security prevention and response and establishes an information exchange partnership between DHS and critical infrastructure owners and operators.

The Quadrennial Homeland Security Review[25] was revised in 2014. The investigation revealed the responsibility of DoD to develop new and expanded full-spectrum cyberspace capabilities to protect their country and to support military missions worldwide. The 2014 DoD *Quadrennial Defense Review* defines DoD's most important role in cyberspace: "Protect the integrity of DoD's networks, protect our key systems and networks, implement overseas operations at their command, and defend the nation against an impending, destructive cyber-attack."

Cyber Electromagnetic Activities (FM 3-38)[26], published by the US Army in 2014, provides instructional guidance for cyber-electromagnetic activities, and tactics and procedures for planning, integration and synchronization. The doctrine compares Army operations with electronic warfare. In addition, *the Joint Cyberspace Operations (JP 3-12)*[27], deals with the uniqueness of military operations in cyberspace, clarifies cyberspace operations. In 2014 the federal government created a voluntary cybersecurity framework, named *Framework for Improving Critical Infrastructure*[28], which includes guidelines, practices and voluntary standards for the private sector to ensure critical infrastructure protection.
In addition to the listed documents, the four bills on critical infrastructure protection were adopted in 2014:

[22] Presidential Policy Directive The Critical Infrastructure Security and Resilience 55 https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf (Download 2018. 01. 21)
[23] Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity Presidential Policy Directive
(PPD) 21 Critical Infrastructure Security and Resilience
https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf (Download 2018. 01. 21)
[24] National Cybersecurity and Critical Infrastructure Protection (NCCIP)
https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf (Download 2018. 01. 21)
[25] The Quadrennial Homeland Security Review
https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf (Download 2018. 01. 21)
[26] U. S. Department of Army, 'Cyber Electromagnetic Activities', No. 3-38, Washington, 2014
http://fas.org/irp/doddir/army/fm3-38.pdf (Download 2018. 01. 21)
[27] Joint Cyberspace Operations Cyberspace Operations
http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf (Download 2018. 01. 21)
[28] Framework for Improving Critical Infrastructure
https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (Download 2018. 01. 21)

- *National Cybersecurity and Critical Infrastructure Protection Act of 2013*
- *Federal Information Security Modernization Act of 2014*[29], which, clarifies the role of DHS in providing federal agencies' digital information, specifies that OMB is responsible for federal enforcement of FISMA requirements and creates cyber incidents reporting requirements.
- *The National Cybersecurity Protection Act of 2014*[30] was signed by President Obama in December 2014. This law allows DHS to share information with the private sector.
- *The Cybersecurity Enhancement Act of 2014*[31] allows the National Institute of Standards and Technology to authorize and support the development of voluntary standards for cyber-attacks to reduce the risk of critical infrastructure.

In military terms, the current national security strategy, adopted at the beginning of 2015, an updated version of the earlier 2011 release, recognizes the growing threat of destructive cyber-attacks and announces the United States' intention to strengthen the cyber security of critical infrastructures. The document focuses primarily on the US's intention to promote international standards in cyberspace. The new strategy offers greater transparency regarding DoD's own offensive and operational capabilities.

On the other hand, the federal interspecific cyber defense strategy provided by DHS. It was published in January 2018, commonly known as EO 13800.[32]

In the US, the Cyber Security Directive nowadays consists of partial measures; Likewise, legislation is less comprehensive and more local. More than 50 statutes deal with different aspects of cyber security. Since there is no comprehensive framework or national cyber security strategy that synthesizes these documents or comprehensively describes the current strategy, clear understanding and overall strategic goals and priorities are a complicated task. Most existing documents address the national priorities of the narrower cyber security domains, which at the same time promote deviation from the priorities and the structure, and do not determine whether or not they are related to or overwrite other policy documents. Most of these documents do not describe how they fit into the overall national cyber security strategy.[33]

STRUCTURAL QUESTIONS

[29] Federal Information Security Modernization Act of 2014 https://www.gpo.gov/fdsys/pkg/BILLS-113s2521es/pdf/BILLS-113s2521es.pdf (Download 2018. 01. 21)
[30] The National Cybersecurity Protection Act of 2014 https://www.congress.gov/113/plaws/publ282/PLAW-113publ282.pdf (Download 2018. 01. 21)
[31] PUBLIC LAW 113–274—DEC. 18, 2014 113th Congress An Act https://www.congress.gov/113/plaws/publ274/PLAW-113publ274.pdf (Download 2018. 01. 21)
[32] A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats 2018 https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf (Download 2018. 01. 21)
[33] National Cyber Security Organization: UNITED STATES 2016 https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf (Download 2018. 01. 21)

The US federal government's bureaucracy is huge and complicated; the exact number of agencies, offices is unknown. Each federal organizational unit and agency is responsible for the protection of its own ICT systems. The regulatory mandate of various organizational units and agencies varies; most departments have a general responsibility in the constituency, others have rules on cyber security, while some have no clear mandate to regulate cyber security. In some cases, computer security strategy papers provide high levels of responsibility and responsibilities to federal government agencies and their perception.

While the responsibility of the lead cyber-directive is widely distributed, the primary policy coordination role is brought to the White House by the *Information and Communication Infrastructure Commission (in the following ICI-IPC)* of *the National Security Council*. The ICI-IPC Co-Chair of the *Cyber Security Coordinator (in the following CSC*) at *National Security Council Cyber Security Office* and the *Home Security Council*. CSC leads the development of the national cyber security strategy and policies and oversees the implementation of these policies by agencies. As the main adviser to the chair of the *National Security Council*, CSC reports to the council, launches a consultation process at the White House and coordinates US cyber security policies and activities. National cyber security naturally involves DoD, DoJ, and DHS, but each has a different mandate to fulfill. Despite the established "supported vs. supporting" roles, the extent to which DHS or DoD attains primacy in practice remains unanswered. The existing cybersecurity connections between DHS, DoD, and DoJ provide an adequate starting point for analyzing the interagency dynamics regarding cyber organization and policy.[34]

DHS

The Department of Homeland Security is the main institution responsible for cyber security within the US borders. DHS five key tasks are to strengthen the security and resilience of critical infrastructure; provides assistance to federal civil agencies on cyber security procurement and supports the adoption of common risk-based policies and best practices; advance law enforcement, responding to events and reporting abilities; and provides a healthy cyber-ecosystem. DHS shows a direction and coordinates federal efforts to protect critical infrastructure. Among the DHS 22 agencies, the National Defense and Program Directorate (NPPD), which includes the National Cybersecurity & Communications Integration Center its mandate focuses on cyber security. [35]

DOJ

The Department of Justice (DoJ) is mainly responsible for implementing cyber security laws. The DoJ fights again cyber threat by investigating and persecuting incursions, pro-

[34] Michael Daniel, 'Assessing Cybersecurity Regulations', The White House Blog, 2014 http://www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations (Download 2018. 01. 21)
[35] The Quadrennial Homeland Security Review https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf (Download 2018. 01. 21)

moting the commitment of the nation-state, and delivering legal and political support to other departments. This institute investigates, attributes and disrupts cybercrime under its jurisdiction; conducts national security operations on cyber threats, including disruption of foreign intelligence, terrorism or other national security threats; and provides home collection, analysis, and dissemination of cyber threats.[36] In order to ensure a comprehensive governmental approach to the fight against national cyber threats, the DoJ National Security Department works in co-operation with the rest of the department. DoJ's Computer Crime and Intellectual Property Section prevents, investigates and punishes cybercrime with other government agencies, the private sector, university institutes and their foreign counterparts.[37]

DOD

Understood thing is DHS protects .gov infrastructure and civilian government networks, the Defense Ministry (DoD) is responsible for protecting the .mil domain and DoD global information infrastructure from cyber-attacks. DoD also has the responsibility to gather information on foreign cyber threats, to provide national security and military systems, and to detect cybercrime in military jurisdiction. DoD's cyber activities and missions are lead by the 2015 Department of Defense Cyber Strategy, which holds DoD's three main mission in computing: computer security and operational capabilities for DoD's networks, systems and information protection; the defense of cyber-attacks of "significant consequences" to the nation; and supports military operations and contingency plans. The role and responsibility of DoD's cybersecurity are provided by the USCYBERCOM Joint Operations Center (see 3.3.2), the National Security Agency / Central Security Service Center, the Defense Cyber Crime Center, and the Defense Information System Agency (DISA).[38] [39]

USCYBERCOM

Each military service is provided with a cyber component, which reported to the US Cyber Command (USCYBERCOM), which belongs to the US Strategic Command (USSTRATCOM). On June 23, 2009, the Secretary of Defense directed the Commander of U.S. Strategic Command to establish a sub-unified command, United States Cyber Command (USCYBERCOM). Full Operational Capability (FOC) was achieved Oct. 31, 2010. USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries. The Command has three primal areas: Defending

[36] U. S. Department of Justice, 'Cyber Security', 2014 http://www.justice.gov/jmd/2014factsheets/cyber-security.pdf (Download 2018. 01. 21)
[37] U. S. Department of Justice, 'Computer Crime & Intellectual Property Section', 2014 http://www.justice.gov/criminal/cybercrime/ (Download 2018. 01. 21)
[38] The Quadrennial Homeland Security Review https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf (Download 2018. 01. 21)
[39] National Cyber Security Organization: UNITED STATES 2016 https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf (Download 2018. 01. 21)

the DoDIN, providing support to combatant commanders for execution of their missions around the world, and strengthening our nation's ability to withstand and respond to cyber-attack. The Command unifies the direction of cyberspace operations, strengthens DoD cyberspace capabilities, and integrates and bolsters DoD's cyber expertise. USCYBERCOM improves DoD's capabilities to operate resilient, reliable information and communication networks, counter cyberspace threats and assure access to cyberspace. USCYBERCOM is a sub-unified combatant command subordinate to USSTRATCOM. Its service elements include Army Cyber Command (ARCYBER), Fleet Cyber Command (FLTCYBER), Air Force Cyber Command (AFCYBER) and Marine Forces Cyber Command (MARFORCYBER). Coast Guard Cyber Command (CGCYBER), although subordinate to the Department of Homeland Security, has a direct support relationship to USCYBERCOM. The Command is also standing up dedicated Cyber Mission Teams to accomplish the three elements of our mission.[40]

The above is described the best way with *March 2, 2017, Cyber Strategy and Policy the Committee on Armed Services, the United States Senate, the One Hundred Fifteenth Congress, the First Session.*

"At the end of that process, we assigned the responsibilities as follows: The Justice Department would, among other things, "investigate, attribute, disrupt, and prosecute cybercrimes; lead domestic national security operations; [and] conduct domestic collection, analysis, and dissemination of cyber threat intelligence;" Department of Homeland Security (DHS) would, among other things "coordinate the national protection, prevention, mitigation of, and recovery from cyber incidents; disseminate domestic cyber threat and vulnerability analysis; [and] protect critical infrastructure;" and DoD would "defend the nation from attack; gather foreign threat intelligence and determine attribution; [and] secure national security and military systems."Moreover, the "bubble chart," as this document was called, assigned the following lead roles: DoJ: investigation and enforcement; DHS: protection; and DoD: national defense."[41]

STRATEGIC GOALS OF DOD AND DHS VIEWPOINT

DOD STRATEGIC GOALS

1. Build and maintain ready forces and capabilities to conduct cyberspace operations;
2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions;
3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyber-attacks of significant consequence;

[40] U. S. Cyber Command (USCYBERCOM) Sept. 30, 2016, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/ (Download 2018. 01. 21)
[41] March 2, 2017, Cyber Strategy and Policy the Committee on Armed Services, the United States Senate, the One Hundred Fifteenth Congress, the First Session. https://www.hsdl.org/?view&did=800207 pp. -3 (Download 2018. 01. 21)

4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages;
5. Build and maintain robust international alliances and[42]

To work effectively in a cyberspace, DoD needs the strength and staff, which are trained highest quality, ready and have the highest technical capabilities. In 2013, a DoD the CMF initiative has initiated a significant investment in computer personnel and technology; Most- DoD needs to improve this investment by building people and building effective organizations and the full development of command and control systems and the capabilities required by DoD they work in a cyberspace. Although DoD cannot protect every network or system against any intrusion - DoDs entire network attack surface is too big to protect every threat and is too large to close every vulnerability - DoD needs to take steps to identify, prioritize and protect most networks and data to efficiently fulfill your mission. The DoD should also design it practice operating in a corrupt and disturbed cyber environment in the event that one attacks DoD networks and data, or if it is a critical infrastructure aspect in which it is DoD relies on its operational and emergency plans. Finally, DoD needs to raise technology and innovation to prevent the threat increases cyber-defense capabilities, including by building and employing a defendable network architecture and common information environment. DoD should work with a private sector to assist the defense industry's basic trading and be prepared to help other agencies against US networks. The Department of Defense must work with business partners, a private sector and an ally and partner nations to prevent and, if necessary, overcome it a cyber-attack with significant consequences in the US domestic and American interest. DoD should develop its intelligence, warning, and operational capabilities of a sophisticated, malicious cyber-attacks. In accordance with all applicable laws and DoD has a granular, detailed, predictive, and an intelligence capable of acting on global networks and systems, opponents' abilities and malware brokers and markets. In the event of increased tension or open-mindedness, DoD must be able to ensure the President with a wide variety of escalation management solutions. If instructed to do so, DoD must be able to do so use cyberoperations to disrupt the enemy's command control system and military networks. As part of the critical infrastructure and the full range of available tools, DoD has to develop and integrate usable cyber opportunities and integrate these opportunities Ministerial plans. In the interest of, DoD allows combat commands to design and synchronize cyberoperations with kinetics in all areas of military operations. DoD's cyber mission requires close cooperation with its foreign allies and partners. The international Internet engagement DoD aims to build partner capacity in cyber security and to deepen cyber-protection and, where appropriate, operational partnerships. Given the high demand and relative scarcity of cyber resources, the DoD make firm choices, and partner-capacity initiatives should focus on areas where basic U.S. national interests play a role. Over the next five years, with the ongoing partner capacity, DoD focuses on international commitment to the Middle East Asia and the most important NATO allies. DoD will follow this strategy continuously evaluates the international environ-

[42] FACT SHEET: THE DEPARTMENT OF DEFENSE (DOD) CYBER STRATEGY APRIL 2015 https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf (Download 2018. 01. 21)

ment and develops innovative partnerships respond to the challenges and opportunities that arise.[43]

DHS STRATEGIC GOALS

The chapters identified five complementary and mutually supportive goals that have been dramatically gone reduces the risk of automated, distributed attacks and improves the elasticity of ecosystems. A list the measures proposed by key stakeholders will reinforce each of the objectives. The goals are as follows:

1: To achieve clear adaptive, sustainable and secure technology marketplace

2: Encourage innovation in infrastructure to adapt to changing threats dynamically

3: Encourage innovation at the perimeter of the network to prevent, detect and mitigate the problem behavior

4: Creating coalitions between security, infrastructure and operational technology communities and around the world

5: Increasing awareness and education through the entire ecosystem

These goals and actions aim at presenting a comprehensive portfolio solution, that would improve the nausea of the ecosystem when implemented. Recommended actions and options include ongoing and upgraded activities as well as new initiatives. No investment or activity can harm, but organize discussions and stakeholders feedback allows us to re-evaluate and prioritize these activities based on their expected returns the ability to measurably influence investment and ecosystem flexibility. Since the draft report has been issued public comments, stakeholders are looking to help us refine value, utility and investment potential the proposed activities, support and leadership opportunities, and obstacles implementation. In order to increase the flexibility of the Internet and the communication ecosystem, it is essential that we do support and rewarding technology market support is continuous development, acceptance, and development innovative security technologies and processes. When market incentives encourage manufacturers functionality and performance complements security innovation the tools and processes that produce extremely safe products can be more easily verified. As these devices are sophisticated, they will be cheaper manufacturers and integrators to accept the components of a safe development lifecycle, encouraging it more manufacturers can compete with safety. Developing a more flexible Internet and communication ecosystem, standards and practices it is necessary to prevent, prevent and/or mitigate botnets and distributed threats and must be improved in all areas of the ecosystem in response to changing hazards and foresight. Creating a flexible web and communication ecosystem, the goal of infrastructure services protection against attacks should be complemented by increased detection and mitigation of weakened person devices the home or corporate networks, and these networks connect to the Internet. More context from local knowledge can improve your discovery and make it easier to select a segment firewall-specific devices or services behave abnormally. Improve the flexibility of the Internet and the communication infrastructure in order to implement coordinated actions geopolitical, public-private, industrial and technical boundaries should

[43] THE DEPARTMENT OF DEFENSE CYBER STRATEGY April 2015 https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (Download 2018. 01. 21)

be made easier to realize. Increasing the flexibility of the Internet and the communication ecosystem against distributed threats stakeholders need to recognize and be prepared to carry out their roles and responsibilities.[44]

CONCLUSION

This publication summarizes the process of evolving the cyberspace directive and summed up the most decisive documents. Summing up the continuous cyber-detection and the growing response of the US government and departments, the US has clearly recognized the new security challenges and wants to respond to the events and situations that have emerged. There are many examples of the need for a cyber defense directive through the Korean night up to the presidential election scandals.

In addition, you want to develop your skills and competencies that you have achieved so far and to support your educational, scientific, and research orientations. In addition, it intends to provide technical support to the Member States and to their own organization by providing adequate skills. It also recognizes the civil and private expertise and cooperates in both this and other international organizations. The interpretation and organization of the US process of building a cyberspace requires the development of a transfer test model, the establishment of a methodology and the creation of a professional framework.

BIBLIOGRAPHY

1. The White House, 'The National Strategy to Secure Cyberspace', 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (Download 2018. 01. 21)
2. Executive Order 13025 - Amendment to Executive Order 13010, the President's Commission on Critical Infrastructure Protection November 13, 1996, https://www.gpo.gov/fdsys/pkg/WCPD-1996-11-18/pdf/WCPD-1996-11-18-Pg2390-3.pdf (Download 2018. 01. 11)
3. PRESIDENTIAL DECISION DIRECTIVE/NSC-63 THE WHITE HOUSE WASH INGTON May 22, 1998, https://fas.org/irp/offdocs/pdd/pdd-63.pdf (Download 2018. 01. 11)
4. Who Should Lead U.S. Cybersecurity Efforts? By Kevin P. Newmeyer 2012, pp. 118–119 http://cco.ndu.edu/Portals/96/Documents/prism/prism_3-2/prism115-126_newmeyer.pdf
5. The United States Congress, 'H.R.2458 – E-Government Act of 2002. 107th Congress (2001-2002)', 2002, https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf (Download 2018. 01. 15)
6. The White House, 'The National Strategy to Secure Cyberspace', 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (Download 2018. 01. 21)

[44] A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats 2018 https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf (Download 2018. 01. 21)

7. PUBLIC LAW 107–296—NOV. 25, 2002, 107th Congress an Act To establish the Department of Homeland Security, and for other purposes. https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf (Download 2018. 01. 21)
8. U. S. Department of Homeland Security, 'Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection', 2003, http://www.dhs.gov/homeland-security-presidential-directive-7 (Download 2018. 01. 21)
9. National Infrastructure Protection Plan 2006, https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf (Download 2018. 01. 21)
10. National Military Strategy for Cyberspace Operations Chairman of the Joint Chiefs of Staff Washington December 2006, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf (Download 2018. 01. 21)
11. National Security Presidential Directive 54/ Homeland Security Presidential Directive 23 The White House Washington 2008, https://fas.org/irp/offdocs/nspd/nspd-54.pdf (Download 2018. 01. 21)
12. Comprehensive National Cybersecurity Initiative (CNCI) https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf (Download 2018. 01. 21)
13. Cyberspace Policy Review https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-028.pdf (Download 2018. 01. 21)
14. National Security Strategy http://nssarchive.us/NSSR/2010.pdf (Download 2018. 01. 21)
15. Quadrennial Homeland Security Review https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf (Download 2018. 01. 21)
16. US Department of Defense U.S. Cyber Command Fact Sheet https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf (Download 2018. 01. 21)
17. Blueprint for Secure Cyber Future https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf (Download 2018. 01. 21)
18. International Strategy for Cyberspace https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Download 2018. 01. 21)
19. Department of Defence Strategy for Operating in Cyberspace https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (Download 2018. 01. 21)
20. Improving Critical Infrastructure CyberSecurity (EO 13636) https://www.dhs.gov/sites/default/files/publications/EO-13636-Improving-Critical-Infrastructure-Cybersecurity-508.pdf (Download 2018. 01. 21)
21. Presidential Policy Directive The Critical Infrastructure Security and Resilience 55 https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf (Download 2018. 01. 21)

22. Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity Presidential Policy Directive (PPD) 21 Critical Infrastructure Security and Resilience- https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf (Download 2018. 01. 21)
23. National Cybersecurity and Critical Infrastructure Protection (NCCIP) https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf (Download 2018. 01. 21)
24. The Quadrennial Homeland Security Review https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf (Download 2018. 01. 21)
25. U.S. Department of Army, 'Cyber Electromagnetic Activities', No. 3-38, Washington, 2014 http://fas.org/irp/doddir/army/fm3-38.pdf (Download 2018. 01. 21)
26. Joint Cyberspace Operations Cyberspace Operations http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf (Download 2018. 01. 21)
27. Framework for Improving Critical Infrastructure https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (Download 2018. 01. 21)
28. Federal Information Security Modernization Act of 2014, https://www.gpo.gov/fdsys/pkg/BILLS-113s2521es/pdf/BILLS-113s2521es.pdf (Download 2018. 01. 21)
29. The National Cybersecurity Protection Act of 2014, https://www.congress.gov/113/plaws/publ282/PLAW-113publ282.pdf (Download 2018. 01. 21)
30. PUBLIC LAW 113–274—DEC. 18, 2014, 113th Congress an Act To provide for an ongoing, voluntary public private partnership to improve cybersecurity, and to strengthen cybersecurity research and development,
31. A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats 2018, https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf (Download 2018. 01. 21)
32. National Cyber Security Organization: UNITED STATES 2016, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf (Download 2018. 01. 21)
33. Michael Daniel, 'Assessing Cybersecurity Regulations', The White House Blog, 2014, http://www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations (Download 2018. 01. 21)
34. The Quadrennial Homeland Security Review https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf (Download 2018. 01. 21)
35. U. S. Department of Justice, 'Cyber Security', 2014, http://www.justice.gov/jmd/2014factsheets/cyber-security.pdf (Download 2018. 01. 21)
36. U. S. Department of Justice, 'Computer Crime & Intellectual Property Section', 2014, http://www.justice.gov/criminal/cybercrime/ (Download 2018. 01. 21)

37. The Quadrennial Homeland Security Review https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf (Download 2018. 01. 21)
38. National Cyber Security Organization: UNITED STATES 2016, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf (Download 2018. 01. 21)
39. U. S. Cyber Command (USCYBERCOM) Sept. 30, 2016, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/ (Download 2018. 01. 21)
40. March 2, 2017, Cyber Strategy and Policy the Committee on Armed Services, the United States Senate, the One Hundred Fifteenth Congress, the First Session. https://www.hsdl.org/?view&did=800207 pp. -3 (Download 2018. 01. 21)
41. FACT SHEET: THE DEPARTMENT OF DEFENSE (DOD) CYBER STRATEGY APRIL 2015, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf (Download 2018. 01. 21)
42. THE DEPARTMENT OF DEFENSE CYBER STRATEGY April 2015, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (Download 2018. 01. 21)
43. A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats 2018, https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf (Download 2018. 01. 21)