Monika Pajurek
monikapajurek@o2.pl

Cybersecurity military entities of the United States of America

Wojskowe podmioty cyberbezpieczeństwa Stanów Zjednoczonych Ameryki

Streszczenie:

Siły zbrojne Stanów Zjednoczonych Ameryki prowadzą działania w cyberprzestrzeni od dziesięcioleci. Ze względu na swoją pozycję i wysoko rozwiniętą infrastrukturę cyfrową USA są narażone na ataki hakerów. Maja one wpływ na charakter planowanych i realizowanych operacji wojskowych oraz mogą prowadzić do szkód gospodarczych państwa. W artykule skupiono się na tym, jak zagadnienia cyberbezpieczeństwa postrzega Pentagon oraz inne wojskowe podmioty zapewniające cyberbezpieczeństwo. Obejmują one poszczególne dowództwa sił zbrojnych: USSTRATCOM, USCYBERCOM oraz Komponenty Służb Cyberprzestrzeni. W rozważaniach nacisk położono na ukazanie zakresu ich kompetencji, strukturę oraz ewolucję form działania, z uwzględnieniem wymiaru narodowego oraz globalnego.

Słowa kluczowe: cyberprzestrzeń, bezpieczeństwo cyberprzestrzeni, siły zbrojne USA, operacje cybernetyczne

Summary:

US armed forces have been operating in cyberspace for decades. Due to its position and highly developed digital infrastructure the United States are vulnerable to hackers. These attacks pose restrictions during military operations and can lead to the economic damage of the country. The article focuses on how the Pentagon perceives cybersecurity issues. Military cybersecurity entities include individual commands of the armed forces: USSTRATCOM, USCYBERCOM and Cyberspace Service Components. This article presents the military entities responsible for cybersecurity, pointing to their evolution and increasing importance in providing this kind of security for the country as well as on global scale.

Keywords: cyberspace, cybersecurity, The United States Armed Forces, cyberoperations

1. Introduction.

Along with the development of the new information and communication technologies and the development of the Internet a number of security threats apeared, including cyberterrorism, cyberspying, which include non-state actors as well as cyberwar as a dispute between states in cyberspace. Modern trends in the development of the cyber threats pose more and more influence to the level of security in cyberspace in the overall security of the country. Through the increased reliance on technology, cyber-attack can seriously jeopardize the functioning of societies and states. It is normal that the modern technologies used in the global information network are comprehensively used by the military sphere.

Today the cyberspace is an essential element of the global role of the US armed forces, as rightly pointed out by the Pentagon, which also defines the various terms related to this topic. The concept of the cyberspace has many definitions. The most recent definition of the cyberspace is contained in *the Department of Defense Dictionary of Military and Associated Terms* by which cyberspace "is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[1]. In turn, this dictionary defines cybersecurity as "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."[2] The area of cybersecurity is an area which permeates all sectors of the economy of the country and has also an impact on the functioning of almost all dimensions of the state and the society.

Previously there were some institutions which worked in the area of cybersecurity but their functions were not sufficient against new threats. Entities that are currently responsible for the cyber-security base their functioning on the strategies / doctrines that define terms related to the activities in cyberspace, define concepts how to operate in cyberspace. They also create and define the mission of the cyber -military structure. To those strategies and doctrines belong *The Department of De-*

[1] *Joint Publication (JP) 1-02*, *Department of Defense Dictionary of Military and Associated Terms,* p. 58, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, [accessed: 20.01.2017].

[2] Ibidem, p. 57.

fense Cyber Strategy[3], *Joint Publication 3-12 ® Cyberpsace Operations*[4] and *U.S. International Strategy for Cyberspace: Prosperity, Security and Openness in a Network World*[5]. These include a variety of military matters, including a description of the various entities responsible for cyber-security, as well as their specific characteristics. Very important are also documents and publications of the individual departments, which are coordinated by the Department of Defense: Department of the Army, Navy and Air Force. Military cyber entities include individual command of the armed forces: United States Strategic Command –USSTRATCOM, United States Cyber Command-USCYBERCOM and Service Cyberspace Components.

2. United States Strategic Command (USSTRATCOM).

United States Strategic Command-USSTRATCOM was created in 2002 as a merge of Air Force Strategic Command and the U.S. Space Command. It is headquartered at Offutt Air Force Base in Nebraska. USSTRATCOM is one of nine Unified Combatant Commands-UCC of the US armed forces. Command is used as a command and control center in the US strategic forces, as well as the military operations, including the operation of military satellites. As part of its functions it is responsible both for early warning of the missile attack, as well as for launching rockets in response to an attack[6]. About 4,000 personnel representing all four services, including civilians and employees of the Department of Defense, working in the command center[7].

Part of the Strategic Command of USSTRATCOM had its beginning in March 1964, with the establishment of the SAC - Air Force Strategic Air Command at Offutt. At the peak of the Cold War, Offutt was a command center for the "triad" of defense: strategic bomber and ICBM (Intercontinental Ballistic Missile) Air Force and SLBM (Submarine-launched ballistic missile) Navy. June 1, 1992 the year of the end of the Cold War, SAC and Navys's Joint Strategic Target Planning Staff merged in the U.S. Strategic Command. Since that time, the entire planning, management

---

[3] *The Department of Defense Cyber Strategy*, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, [accessed: 20.01.2017].

[4] *Joint Publication 3-12® Cyberspace Operations*, Washington 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf, [accessed 20.01.2017].

[5] *U.S. International Strategy for Cyberspace*, Washington 2011, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, [accessed: 20.01.2017].

[6] *About US Strategic Command*, www.stratcom.mil/About/History, [accessed: 20.01.2017].

[7] Command Snap Shot, http://www.stratcom.mil/About/Command-Snapshot/, [accessed: 20.01.2017].

in time of strategic forces war is under a single command, during normal operation remains under the different services.[8]

USSTRATCOM has worldwide functional responsibilities to other commands. The responsibilities of command include the following:

- "Deterring conflict by posturing forces to conduct operations in response to the threat of a major military attack on the United States.
- Employing forces as directed by the Department of Defense and the president.
- Coordinating directly with other combatant commanders and supporting other commanders with assigned forces as directed by the Department of Defense and the president.
- Conducting integrated strategic operational planning.
- Conducting worldwide strategic reconnaissance when appropriate.
- Coordinating with service component commanders and supporting combatant commanders on issues relating to the organizing, training, equipping and support of forces for USSTRATCOM missions."[9]

Previously, the U.S Strategic Command was subject of the Joint Task Force – Global Network Operations – JTF-GNO[10], but at the time of the activities, they were transferred under the operational control (OPCON - Operational Control) Joint Functional Component Command – Network Warfare – JFCC-NW[11], which is also subject to USSTRATCOM. The function of these two institutions were absorbed later by the USCYBERCOM – the U.S. Cyber Command. As stated by General Keith Alexander (the first Commander of USCYBERCOM) USSTRATCOM redefined the mission area in terms of cyber offensive- NW-Network warfare and defensive - NetOps- Network Operations and established JFCC-NW and JTF-GNO[12].

---

[8] *About US Strategic Command*, op. cit.

[9] *US Strategic Command*, http://www.globalsecurity.org/wmd/agency/stratcom.htm, [accessed: 20.01.2017].

[10] Joint Task Forces-Global -Network Operations it was one of the subordinate USSTRATCOM commands. Its duties included: directing operations and protecting US armed forces global information network at the strategic, operational and tactical level.

[11] Joint Functional Component Command – Network Warfare it was one of the subordinate USSTRATCOM commands. Mainly the command was responsible of the offensive actions in the cyberspace. See more: H. S. Kenyon, *Collaboration Key To Network Warfare*, http://www.afcea.org/content/?q=node/1641, [accessed: 20.01.2017].

[12] J. L. Caton, *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications*, 2015, p. 2 – 8, http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA615633, [accessed: 20.01.2017].

USSTRATCOM has a subordinate sub-components: service sub-components and functional sub-components (which include USCYBERCOM)[13]. The commander of the U.S. Strategic Command is currently General John E. Hyten. His responsibilities include: integration and coordination of command and control capabilities to ensure support of the most accurate and timely information for the President of the United States, Secretary of Defense and for regional combat commanders[14].

3. United States Cyber Command (USCYBERCOM)

The importance of computer networks and their use by the US military has grown rapidly in the late 80's and 90's of the XX century. It was that time when the threats posed by cyberspace were started to be perceived, but these problems has not been taken seriously by the most of the US experts. More serious approach was presented by the administration of George W. Bush, who began to develop offensive and defensive means of action in cyberspace. US military then began to discuss the need to create a centralized command, which would correspond to the operations in the cyberspace. Priority operations in the cyberspace had a NSA-National Security Agency, which since its inception, is responsible for electronic intelligence. Also in the air force and land, marine corps and navy, as well as the National Guard established separate units operating in cyberspace. Although the lack of a top-down structure that would coordinate their activities and problems related to the transmission of information caused that their actions did not give the expected results. The considerable problem was the use of these units mentioned above by the commanders. Their military education do not contained the directions and procedures in case of cyber operations. They learned how to behave in conventional armed forced situations. The technical obstacles were also highlighted, which hindered cooperation between Air Force and Navy. The naval preferred method of decentralized network management which was in opposition to the pilots, who were opting for centralized methods. The creation of a single command would be, on the one hand remedy for these problems, and on the other, to act as a deterrent to potential enemies before the attack on the American network. Then, another problem appeared, during the discussion on the appointment of United States Cyber Command (USCYBERCOM). It was noted that there may be duplication of competence USCYBERCOM with the

[13] A. Feickert, *The Unified Command Plan and Combatant Commands: Background and Issues for Congress*, s. 21 – 22, https://fas.org/sgp/crs/natsec/R42077.pdf, [accessed: 20.01.2017].

[14] *US Strategic Command - Commander General John. E. Hyten*, http://www.stratcom.mil/Leadership/Bio-Article-View/Article/958532/commander/, [accessed 20.01.2017].

National Security Agency (NSA)[15]. Despite everything, in 23 June 2009, the then Secretary of Defense Robert Gates ordered the creation of command. USCYBERCOM achieved initial operational capability in October 2009 and full operational capability in October 2010. USCYBERCOM took over the functions of JTF-GNO and JFCC-NW. The problem associated with the duplication of roles with the NSA was solved by appointing the head of the agency gen. Keith B. Alexander also the commander of USCYBERCOM. US Cyber Command has also, like the NSA, headquarters in Fort Meade, Maryland[16].

You might have noticed that during the Obama administration the cybersecurity have been made a main issue for US, then was launched decisive action to increase the security of the network. The mission of USCYBERCOM[17] includes „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."[18] Scheme 1 shows a standard procedure for issuing orders. As you can see the Cyber Command is responsible for coordinating and supervising the activities of all units of cyber forces.

Moreover, USCYBERCOM is designed to work with government and private partners and belongs to them, among others, FBI, Department of Justice, Department of Homeland Security, DISA-Defense Information Systems Agency. USCYBERCOM and the Department of Homeland Security are responsible for working together with private partners. Through the exchange of information with these partners on threats or probable vulnerabilities it is possible to achieve more effective defense[19].

---

[15] A. Kozłowski, *Dowodzenie w cyberprzestrzeni*, http://polska-zbrojna.pl/home/articleinmagazineshow/13813?t=DOWODZENIE-W-CYBERPRZESTRZENI, [accessed: 20.01.2017].

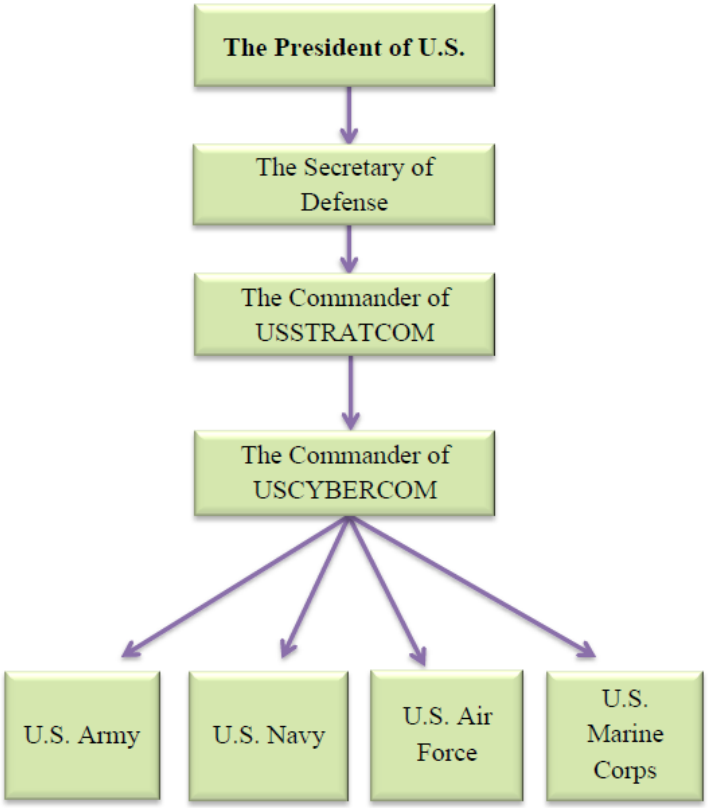
[16] J. L. Catton, *Army Support…..,* op. cit., p. 10 and 25.

[17] It is interesting that the logo Command is a string of 32 characters on the inner ring of gold, which after decryption means exactly the same as saved as the mission and objectives Command. It is used here MD5 hashing algorithm using which you can submit any message in the form of 128-bit shortcut.

[18] *Cyberspace Operations* (*DD 3-12*), http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-060.pdf, p. 22 – 23, [accessed: 20.01.2017].

[19] A. Kozłowski, *Rola dowództwa cybernetycznego Stanów Zjednoczonych w bezpieczeństwie kraju*, w: *Wyzwania i problemy współczesnych stosunków międzynarodowych – bezpieczeństwo, dyplomacja, gospodarka, historia i polityka*, red. R. Bani, K. Zdulski, Łódź 2015, p. 310.

Scheme no. 1. Issuing orders in the field of cybesecurity.



Source: W. J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, „Foreign Affairs", 2010 vol. 89 no. 5, p. 102.

The system today is based on three overlaying lines of defense. The first two phases of defense are based on standard measures such as antivirus programs and firewalls, which have the ability to detect malware. The third involves the use of government resources to active defense to defeat the attacks, which managed to break through the first and second line. That's what the National Security Agency (NSA) do, using all the latest technology to reduce the threat before gaining access to military networks. Despite these advanced procedures, you can still detect malicious software which penetrates military networks, and at that moment the role of USCYBERCOM begins. Consolidating the possibility of the Department of Defense is to track down and neutralize the programs, which are intended to infiltrate the military networks. In addition USCYBERCOM aims to organize training for particular types of armed forces in the field of cyber security

eg. Training missions[20]. USCYBERCOM must also monitor the development of the possibility of asymmetrical states and non-state actors. Command has also to work out measures that will deter or discourage potential attacks[21]. All activities and actions that Command carry out, must take into account the respect for privacy and freedom of all people who use the Internet in order to not violate the rights contained in the Constitution[22].

Under the leadership of K. Alexander USCYBERCOM presented five general commanding priorities:1) Concept for Operating in Cyberspace, 2) Cybersecurity Responsibilities, 3) Trained and Ready Force, 4) Defensible Architecture and 5) Global Visibility Enabling Action[23].

The First priority involves creation of doctrines focusing on operating in cyberspace. The armed forces take action on various battlefields that require appropriate strategies, different tactics and different ways to use technology. Of course there are hundreds of papers relating to operations on land, air and sea, but studies on the activities in cyberspace also appear. Then it will take a lot of time before the individual units learn to work together on the basis of the new strategy[24].

The second priority, presented as a responsibility of cyber security concerns extend cooperation with other government entities. General Alexander underlines that in order to ensure security in cyberspace, there is need for coordinated action between several key players from the government. He lists three key players who make up this team: Department of Homeland Security, the FBI and the Department of Defense. This is where important USCYBERCOM cooperation with private partners involving the exchange of information on new threats, is placed[25].

The third priority relates to the training and readiness of Cyber Army, which is to prepare the respective armed forces to conduct combat in cyberspace. General Keith Alexander underlines that one of the main problems USCYBERCOM is too small number of well-qualified employees. Therefore, there are proposed by the establishment programs to encourage young people to join the Cybernetic Command and trainings on cyber security for people who already work there.

---

[20] Ibidem, p. 311 – 312.

[21] *Statement of General Keith B. Alexander, Commander United States Cyber Command*, Senate Committee on Armed Services, 27.03.2012, p. 7, http://www.airforcemag.com/SiteCollectionDocuments/Reports/2012/March2012/Day28/032812alexander.pdf, [accessed: 21.01.2017].

[22] *Statement of General Keith B. Alexander..,* op. cit., p. 9.

[23] *Statement of General Keith B. Alexander, Commander..,* op. cit., p. 11 – 16.

[24] Ibidem, p. 11 – 12.

[25] Ibidem, p. 12 – 13.

Except for programs and training courses it also emphasized the importance of tactical exercises, which have already taken place the first edition under the name Cyber Flag[26].

The fourth priority relates to the creation of defensive architecture. This one which exists today was built as a channel of communication and a place to collect valuable information. General Alexander pointed out the need to build a strong operational platform, which will be sturdier to hacker attacks, but also suitable affordable to maintain. New defensive architecture is designed to provide efficient security model Use of databases and documents, and a system that will monitor users. This solution can help avoid a situation where one soldier is able to steal hundreds of secret data[27].

The fifth refers to the global awareness of cybersecurity trends. It is important to have knowledge about the existing threats, since without this, it is not possible to prevent them. Experts from the US Cyber Command must be able to access the knowledge of new malicious programs. That's why General Alexander in this priority presented a proposal to build a single information system, which use state institutions and private institutions, so it has to be ensured quick and strict reaction to the threat of network[28].

The present commander Admiral Michael S. Rogers continue and focused on the same five priorities. He also described the details of the planned structures for the training and preparation of cyber forces[29]. According to plans, the structure of the team is to include about 6,000 cyber professionals, divided into 133 teams in three areas of mission: National Cyber Misssion Force, responsible for the protection of critical infrastructure components, eg. power stations, dams, power grids and other facilities the main in the functioning of the state; Cyber Combat Mission, to help military commanders by carrying out offensive operations in cyberspace and Cyber Protection Forces, responsible for the protection and monitoring of the network of the Department of Defense.[30] As you can see on the Map 1, Cyber Support Elements-US Strategic Command CSEs are designed

---

[26] Ibidem, p. 14 – 15.

[27] USCYBERCOM is intended to operate which will not allow a repeat of leakage of secret data to the portal wikileaks.com that stole the soldier Bradley Manning, see more: F. Abrams, Y. Benkler, *Death to Whistle-Blowers?*, 13.03.2013, http://www.nytimes.com/2013/03/14/opinion/the-impact-of-the-bradley-manning-case.html, [accessed: 21.01.2017].

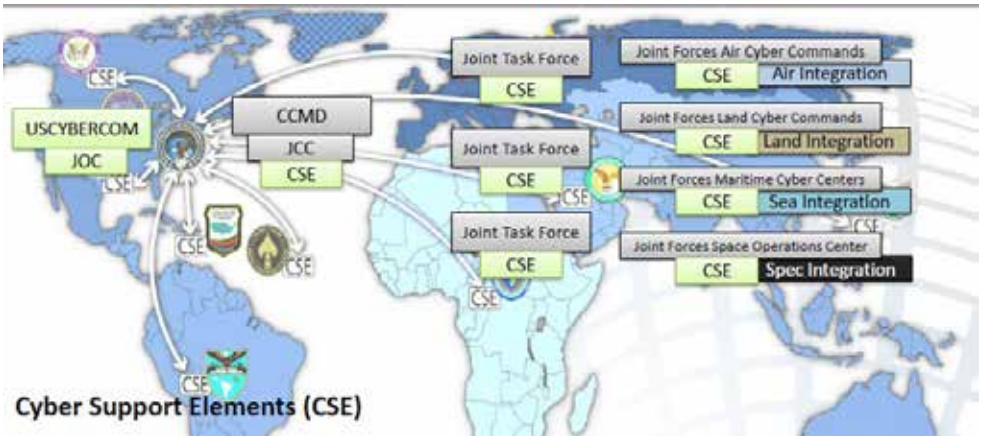
[28] *Statement of General Keith B. Alexander, Commander…,* op. cit., p. 16.

[29] J. L. Catton, *Army Support..,* op. cit., p. 13.

[30] C. Pellerin, *Rogers: Cybercom Defending Networks, Nation,"*DoD News", 14.08.2014, http://www.defense.gov/News-Article-View/Article/603083, [accessed: 21.01.2017].

to help coordinate cyber support by the commanders of the combined component, the commanders of the Joint Task Force (JTF) and combat commanders of the Joint Cyber Center(JCC). On the Map acronym JOC means Joint Operations Center, CCMD – Combatant Command.

Map no. 1. USSCYBERCOM support for Combatant Commands.



Source: G.J. Franz, III, *Effective Synchronization and Integration of Effect through Cyberspace for the Joint Warfighter*, presentation on AFCEA TechNetLand Forces-East Conference, Baltimore, 14.08.2012, slide 10, http://www.afcea.org/events/tnlf/east12/documents/4V3EffSynchIntEffthruCybrspcforJtWarfighter_forpublicrelease.pdf, [accessed: 21.01.2017].

Since formation of USCYBERCOM, the significant improvement of US cybersecurity may be noticed. In 2011 there was a break into tokens to RSA company, which is responsible for securing computers Department of Defense, by hackers from an unknown state. Quick response from USCYBERCOM, allowed to take a co-ordinated action[31]. Among the achievements of the US Cyber Command it must be pointed out the reduction of the damage which has been caused by hacker attacks by different groups e.g. Anonymous. Another success is constantly expanding cooperation with companies involving reinforcing the exchange of information, thanks to a warning from private companies they succeeded to prevent attacks on government networks. US Cyber Command has also developed a number of initiatives in cooperation with private partners, for example:

[31] Warnings were sent to employees who manage networks, in order to have launched a proper precautions. As a result, they succeeded to protect from theft the valuable information. In the same year, hackers used the Adobe software, in which they found loopholes that allowed for hacking into computers. Command then blocked every attempt to penetrate military networks.

Defense Industrial Base Cyber Pilot (DIB), it was a test program addressed to the Internet service providers, which aim was to increase the security of information transmission, government resources data. Another interesting initiative was the creation of the Enduring Security Framework namely working forum consisting of representatives of IT companies[32]. However, the new command failed to prevent the most serious cyberspying operation, which was against the US forces. It came in 2013, when Chinese hackers stole more than 20,000 documents related to the missile defense system[33].

The appearance of the US Cyber Command met with a firm criticism in the international arena, which was especially visible from Russia and China. They accused the US of cyberspace militarization. However, this process began much earlier and these countries had a significant impact on its deepening. In addition, before there was USCYBERCOM in many other countries armed forces there were already similar structures[34]. Undoubtedly, the creation of the new US command is a turning point for the international security. The decision to create such institutions can contribute to the reduction of hacker attacks and limit the effects caused by malicious software, but it can also lead to start the arms race. The militarization of cyberspace could lead to serious conflicts, which can modify the classic battlefield. Although General Alexander highlighted that the creation of US Cyber Command "is not a sign of the militarization of cyberspace, but a conscious response from the politicians and the military to current challenges and is a necessary step in improving the cyber defense"[35].

At the beginning, the USCYBERCOM employed about 1,000 people and had a budget of approximately 114 million dollars[36]. Currently, the budget is around 505 million dollars[37]. After retiring the gen. Keith Alexander in 2014, his successor, Admiral Michael Rogers also was simultaneously the commander of USCYBERCOM and the head of the NSA. Then, a part of the military thought, that it is a good time to separate the two institutions. It has clarified that this is too

---

[32] *Statement of General Keith B. Alexander, Commander..,* op. cit., p. 8 – 11.

[33] Documents containing the information on anti-missile defense systems: Aegsi, Patriot Pac-3 and also US military aircraft V-22, F-35, F/A-18; see: A. Kozłowski, *Dowodzenie…*, op. cit.

[34] A. Kozłowski, *Dowodzenie…,* op. cit.

[35] A. Kozłowski, *Rola dowództwa…*, p. 317.

[36] B. Fung, *Cyber Command's exploding budget, in 1 chart*, „The Washington Post", 15.01.2014, https://www.washingtonpost.com/news/the-switch/wp/2014/01/15/cyber-commands-exploding-budget-in-1-chart/, [accessed: 21.01.2017].

[37] A. Boyd, *CYBERCOM gets easiest budget hearing ever*, 16.03.2016, http://www.federaltimes.com/story/government/cybersecurity/2016/03/16/house-subcommittee-cybercom/81870980/, [accessed: 21.01.2017].

much accumulation of power in one person. In turn, the second part of the military pointed to the exemplary cooperation NSA and USCYBERCOM, as well as the benefits associated with the use by the same network, which gave the savings and reduced military spending. The appointment of Admiral Rogers also head of the NSA showed that the Obama administration agreed with arguments of supporters of the current model. For the coordination of the Armed Forces with the NSA is responsible Central Security Service - CSS[38]. Hence, the commander of USCYBERCOM is also head of the NSA, many people mistakenly believe that these two institutions are doing the same. As acknowledged by senior sergeant Commander (Maj) Major Rodney D. Harris reason why the same person is the commander in both institutions, is the core communication infrastructure, which operates USCYBERCOM because it is the same in which the NSA is working. USCYBERCOM and NSA have dynamically different missions. The task of the NSA is to gather intelligence to support the active defense of the nation. USCYBEROM task is primarily to defend all Army networks[39].

4. Service Cyberspace Components.

US Cyber Command in 2010 has absorbed liquidated elements: Joint Task Force-Global Network Opertions-JTF-GNO and JFCC-NW (Joint Functional Component Command - Network Warfare). USCYBERCOM consists of components belonging to all four of the armed forces of the United States, operating in various locations around the world:

- ❑ Army Cyber Command/Second Army
  - Army Network Enterprise Technology Command/9th Army Signal Command
  - United States Army Intelligence and Security Command
    - 1st Information Operations Command
    - 780th Military Intelligence Brigade
- ❑ Fleet Cyber Command/10th Fleet
  - Naval Network Warfare Command
  - Navy Cyber Defense Operations Command
  - Naval Information Operations Commands
  - Combined Task Forces
- ❑ 24th Air Force (Air Forces Cyber)

[38] A. Kozłowski, *Dowodzenie*..., op. cit.

[39] M. L. Lewis, *From weapons systems* to *squad leaders*, *cyber NCOs protect all that's connected, 04.03.2014,* http://ncojournal.dodlive.mil/tag/arcyber/, *[accessed: 21.01.2017].*

- 67th Network Warfare Wing
- 668th Information Operations Wing
- 68th Combat Communications Wing

❑ Marine Corps Cyberspace Command[40].

The components operate at different levels of operating, at the same time working to improve the efficiency of the common protect and defend state cyberspace.

Army Cyber Command (ARCYBER) was established on 1 October 2010 as a component subject to USCYBERCOM. In turn, the Second Army Cyber Command was activated March 6, 2014 year as the direct reporting unit of USCYBERCOM. ARCYBER / Second Army directs and leads the integrated operation of electronic warfare, information operations and cyber as authorized or directed to ensure freedom of action in cyberspace and receive the freedom of his opponents. ARCYBER has its headquarters in Fort Gordon, Georgia.[41] ARCYBER mission is to "plan, coordinate, integrate, synchronize, direct, and conduct network operations and defense of all Army networks"[42].

Fleet Cyber Command (FLTCYBERCOM) is the operational power of US Navy, responsible for programs related to cyber warfare. 10th Fleet (COMTENTHFLT or C10F) is the formation of a functional US Navy, it was reactivated 29 January 2010[43].

The task of the FLTCYBERCOM is to:

- "to serve as central operational authority for networks, cryptologic/signals intelligence, information operations, cyber, electronic warfare, and space capabilities in support of forces afloat and ashore;
- to direct Navy cyberspace operations globally to deter and defeat aggression in and through cyberspace;
- to ensure freedom of action to achieve military objectives in and through cyberspace"[44].

The task of 10th Fleet is also to serve as Numerical Unit for Fleet Cyber Command and exercising operational control assigned to naval forces. 10th Fleet is designed to cooperate and coordinate with other units of the Navy, the allies and Joint

---

[40] *U.S. Army Cyber Command*, http://www.arcyber.army.mil, [accessed: 21.01.2017].

[41] *U.S. Army Cyber Command and Second Army*, http://www.arcyber.army.mil/Pages/ArmyCyber.aspx, [accessed: 21.01.2017].

[42] *U.S. Army, Army establishes Army Cyber Command,* 01.10.10, http://www.army.mil/article/46012/army-establishes-army-cyber-command/, [accessed: 21.01.2017].

[43] *U.S. Fleet Cyber Command*, http://www.public.navy.mil/fcc-c10f/Pages/usfleetcybermission.aspx, [accessed: 21.01.2017].

[44] Ibidem.

Task Forces to implement the entire spectrum of information operations, electronic warfare and mission in cyberspace. Its headquarters is located in Fort Meade, Maryland[45].

24th Air Force is a component of the Air Force in USCYBERCOM and also a part of Air Force Space Command since 18 August 2009. The task of 24th Air Force is to provide commanders of combat training and readiness cyber forces which plans and carry out cyber operations, and its mission is to operate, expand and defense Air Force information network; defense mission critical systems and providing a full spectrum of capabilities which carries the cyberspace battlefield. His office is located at Joint Base San Antonio Lackland in Texas[46].

Marine Corps Forces CyberSpace Command (MAR4CY/MARFORCYBER) is a component of the Marine Corps of the United States in USCYBERCOM. It was created January 21, 2010 year[47]. Its task is to:

- „enables full spectrum cyberspace operations;
- the planning and direction of Marine Corps Enterprise Network Operations;
- direction of offensive cyberspace operations (OCO) in support of Joint and Coalition Forces, in order to enable freedom of action across all warfighting domains"[48].

Marine Corps Forces Cyberspace Command has its headquarters in Fort Made in Maryland.

5. Final Remarks.

This article presents the US military entities that provide cyber security. These entities conduct cyber operations, which are a very important part of military operations, necessary in order to achieve the operational tasks and ensuring the security of the country. The United States because of its potential, largely play and will play a key role in constructing the future of cyberspace. Considering the international position and the level of new technologies, The United States seek to create regulations for cyberspace, through cooperation with allies to ensure cyber security.

---

[45] *U.S. Tenth Fleet Mission*, http://www.public.navy.mil/fcc-c10f/Pages/ustenthfleetmission.aspx (accessed 21.01.17).

[46] *24th Air Force-AFCYBER*, http://www.24af.af.mil/About-Us/Fact-Sheets/Display/Article/458567/24th-air-force-fact-sheet, [accessed: 21.01.2017].

[47] A. J. McCombs, *Marines launch into cyberspace mission with new command,* 29.01.2010, http://www.army.mil/article/33744/Marines_launch_into_cyberspace_mission_with_new_command/, [accessed: 21.01.2017].

[48] *U.S. Marine Corps Forces Cyberspace (MARFORCYBER)*, https://marinecorpsconceptsandprograms.com/organizations/operating-forces/us-marine-corps-forces-cyberspace-marforcyber, [accessed: 21.01.2017].

The increase of cyber-attacks shows that cyber security is becoming a bigger problem for the country. Despite the fact that Pentagon has the ability to conduct cyber offensive, further focuses primarily on the defense of their own networks. The strategy released by the Pentagon in April 2015 emphasized the importance of preparing to defend against cyber-attacks. The following documents also stresses the importance of operations in cyberspace, conducted precisely by the relevant military entities.

The creation of US Cyber Command must be considered as a success, it was one of the most important decisions established by the Obama Administration in the field of national security. It noted how big a threat are the hackers, who are more often and more boldly undertake attacks on US infrastructure. US Cyber Command fulfills its main task, which is effective defending military networks and computer systems against attacks from hackers, but also against malicious software. A sufficiently probable presents a vision USCYBERCOM as one of the most important centers responsible for the field of safety, while the National Security Agency and the Department of Homeland Security will serve an accessory role. It's also necessary to remember about the international impact of the creation of USCYBERCOM, more and more US allies are considering setting up similar structures.

Currently, it is very important to take multidimensional action to improve the systems responsible for blocking the spread of threats in the network. It is about keeping, among others: training, simulation attacks, testing and recognition of the network. Such measures are already undertaken by US forces. The development of specialized institutions and individuals is supporting the functioning of the various types of US armed forces. As for the future operation of the armed forces for the security of cyberspace, it will be continuously developed and more and more functions will be transferred to Cyber Command. Now it can be see the development of its activities even by using it to fight the so-called "Islamic State".

US cybersecurity policy conducted with the aim of putting the defense in the case of strategic cyberwar is facing many difficulties that arise from the fact that the defense may restrict the rights of citizens. For this reason, Washington to strengthen capacities in cyberspace, must insist on a balanced response, containing the concretion of international standards for cyber conflict and enhancing the credibility of the US response to deter potential adversaries.

In summary military entities of the United States of America responsible for cyber security are evolving and increase the scope of its duties. The activities carried out by them effectively contributes the increasing of cybersecurity. In turn, the subject of cybersecurity will, as announced president Donald Trump be priority, which should allow for faster development and improvement of this safety.

Bibliography:

- Boyd A., *CYBERCOM gets easiest budget hearing ever*, http://www.federaltimes.com/story/government/cybersecurity/2016/03/16/house-subcommittee-cybercom/81870980/.
- Chen T. M., *An Assesment of The Department of Defence Strategy for Operating in Cyberspace*, Carlisle PA 2013.
- Dziwisz D., *Stany Zjednoczone a międzynarodowe bezpieczeństwo cybernetyczne*, Kraków 2015.
- Feickert A., *The Unified Command Plan and Combatant Commands: Background and Issues for Congress,* https://fas.org/sgp/crs/natsec/R42077.pdf.
- Franz G. J. III, *Effective Synchronization and Integration of Effect through Cyberspace for the Joint Warfighter*, http://www.afcea.org/events/tnlf/east12/documents/4V3EffSynchIntEffthruCybrspcforJtWarfighter_forpublicrelease.pdf.
- Fung B., *Cyber Command's exploding budget, in 1 chart*, „The Washington Post", 15.01.2014, https://www.washingtonpost.com/news/the-switch/wp/2014/01/15/cyber-commands-exploding-budget-in-1-chart/.
- *Joint Publication 3-12® Cyberspace Operations*, Washington 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.
- *Joint Publication 1-02. Department of Defense Dictionary of Military and Associated Terms,* Department of Defense, Washington 2015, URL http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
- Kozłowski A., *Dowodzenie w cyberprzestrzeni*, http://polska-zbrojna.pl/home/articleinmagazineshow/13813?t.
- Kozłowski A., *Rola dowództwa cybernetycznego Stanów Zjednoczonych w bezpieczeństwie kraju*, w: *Wyzwania i problemy współczesnych stosunków międzynarodowych – bezpieczeństwo, dyplomacja, gospodarka, historia i polityka*, red. R. Bani, K. Zdulski, Łódź 2015.
- Lewis M. L., *From weapons systems* to *squad leaders*, *cyber NCOs protect all that's connected,* http://ncojournal.dodlive.mil/tag/arcyber/.
- Lynn W. J. III, *Defending a New Domain: The Pentagon's Cyberstrategy*, „Foreign Affairs", 2010 vol. 89 no. 5.
- Pellerin C., *Rogers: Cybercom Defending Networks, Nation,* http://www.defense.gov/News-Article-View/Article/603083.
- *The Department of Defense Cyber Strategy*, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf .
- *U.S. International Strategy for Cyberspace*, Washington 2011, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.