Yadigar N. Imamverdiyev
Institute of Information Technology, ANAS, Baku, Azerbaijan
yadigar@lan.ab.az
DOI: 10.25045/jpis.v06.i2.02

CYBER-TROOPS: FUNCTIONS, WEAPONS AND HUMAN RESOURCES

Conflicts between countries are transferred into cyberspace, and operations in the virtual space in peacetime and wartime require a special type of troops: cyber-troops. To provide information security, in some countries there are cyber-troops or plans to develop cyber-troops in the coming years. This paper studies the problem of forming cyber-troops. The main aspects of forming cyber-troops, the tasks and functions of cyber-troops, the structural and organizational models of a cyber command, the arsenal of weapons and human resources of cyber-troops are considered, and the experiences of developed countries in this field are analyzed. Problems with coordinating the activities of cyber-troops and other public organizations involved in cyber security and issues of international cooperation are also discussed.

Keywords: *information warfare; cyber war; cyber defense; cyber-troops; cyber weapons; cyber-command.*

Introduction

In the current phase of globalization, interstate conflicts have moved into the information space, and large-scale information wars have occurred. Cyberspace has rapidly become militarized, and the number of cyber attacks on military and civilian targets is sharply increasing; cyber warfare has become part of the modern warfare arsenal [1, 2]. The first small-scale interstate cyber wars were organized in 2007–2008 (against Estonia and Georgia) [3, 4].

The military, economic, diplomatic, political, cultural and biological sovereignty of the country, and its information sovereignty, have become a national security issue [5]. Some states already consider the information space (along with air, land, sea and space) as the field of battle. One of the measures taken against cyber warfare threats is the creation of special troops: cyber-troops [6]. Cyber-troops are formed to combat military cyber-threats within the armed forces.

Cyber-troops have been in existence since the 2000s in the United States, and many other countries are planning to develop fully prepared cyber-troops in the coming years [7]. Some reports claim that 140 countries have created or expanded cyber-troops, many of which perform attacks. From the military point of view, cyber wars seem attractive and enticing, and do not put the military's troops at risk; it is not necessarily possible to trace the attacker, and the source of the attack may be impossible to determine [7].

This paper analyses the issues involved in developing cyber-troops and studies the experience of developed countries and the international military organizations in this field using publicly available data. The paper analyses the main aspects of cyber-troops' formation, objectives and functions; the structural and organizational models of cyber-command; and cyber-troops' weapons arsenals and human potential. The paper also discusses international cooperation issues in the development of cyber-troops to ensure the sovereignty of each country in cyberspace.

Definitions and terms

To determine the purpose and function of cyber-troops, a number of essential concepts and terms must be agreed upon in advance. The following terms are used in the rest of the article [8]:

Cyber weapons: information technology-based systems (hardware, software, and communications) developed to damage the structure and operations of the other information technology-based systems.

Cyber incident: an incident causing (or enabling) an unacceptable deviation in the structure and operations of the information system. Cyber-incidents can be intentional or accidental. Individuals, groups of individuals, companies or governments can be actors in cyber-incidents.

All possible combinations of the parties attacking each other with cyber weapons reflect the different scenarios, and they can be called cybercrime offenses, industrial espionage, cyber-terror, cyber-conflicts and cyber wars depending on their characteristics.

Cyber attack: deliberate use of a cyber weapon or the system used as a cyber weapon against information systems to cause a cyber incident.

Cyber espionage: the use of cyber attacks to violate the confidentiality of the target system.

Cyber conflicts: the use of cyber attacks to achieve political goals (including attacks against the availability and comprehensiveness of target system). Here, the concept of cyber conflicts is used in a narrow sense. In a broad sense, cyber conflict, in general, is defined as the use of cyberspace to gain supremacy.

In cyber conflicts there are three main operations: conflict avoidance, prevention and resolution in the digital arena. However, some countries do not exclude the options to respond adequately to the conflicts occurring in the virtual space with the methods applicable to real wars.

Cyber war: cyber conflicts between countries, namely cyber warfare, refer to a military operation in the cyberspace. This includes both military attacks against the armed forces of the state (e.g., failure of critically important communication channels of the enemy), and the attacks against the civilian population. The concept of cyber war started to be widely used after the attacks against the servers of the US Embassy in Estonia, the Estonian ministries, banks, and mass media organizations in the spring of 2007 [3].

Cyber war is part of a broader concept of information warfare, and the concept of cyber-troops is part of the concept of information troops. Information warfare is an action focused on gaining information dominance by damaging information, information processes and systems of the opponent, seizing economic and military resources, and changing people's behavior by affecting the public consciousness through information [9]. M.Libicki defines seven forms of information warfare [10]: (1) command-and-control warfare; (2) intelligence-based warfare; (3) electronic warfare; (4) psychological warfare; (5) hacker warfare or virtual sabotage operations aimed at civilian objects; (6) economic information warfare; and (7) cyber warfare, operations aimed at physical parameters of the system and facilities that ensures the normal operation of the network and computer.

From small teams to cyber-troops

Cyber-troops were founded with the emergence and development of small teams: teams of hackers, "red" and "blue" teams and the Computer Emergency Response Team (CERT) [11]. The officers used the services of these teams to resolve information security. The more complex and intense the problems were, the more the issue of establishing cyber-troops came up. The main duty of the cyber-troops is defined as combating the cyber attacks aimed at military systems, which are often organized as CERT. However, different approaches, functions, and operations (including the cyber espionage) exist. For example, the main duty of US cyber-troops is to control and defend military computer networks of the country, and to implement cyber war operations in a centralized manner.

The status of cyber-troops has not been defined yet, and they are considered to be a new type of troop, the main duty of which is to combat cyber threats [5.6]. The process of forming cyber-troops as a separate type of troop requires alternative resources and staffing. The US approach of Doctrine, Organization, Training, Material, Leadership and education, Personnel and Facilities (DOTmLPF) is used to develop cyber-troops [7]. Usually, the cyber-troop's strategies are of defence character, and the three main operations of conflict avoidance, prevention and resolution are part of this. However, some countries do not exclude the use of applicable methods from real warfare to respond adequately to cyber conflicts (the US Presidential Policy Directive 20) [12].

Information (computer) technology is widely used in modern military equipment and in the weapons and control systems of the troops. The widespread use of foreign devices in military

facilities and possible hidden fingerprints are the Achilles' heel of modern weapons. Along with cyber attack prevention, the duties of cyber troops include the detection of malicious software and the search for possible hidden fingerprints in military equipment. The cyber-troops of some countries focus on the disruption of the functioning of control systems of potential enemy troops.

The arsenal of weapons of cyber-troops

The arsenal of weapons of cyber-troops can be divided into two groups: regular cyber weapons and advanced cyber weapons. Regular cyber weapons are the hacker tools intended to perform all operations in the "Cyber Kill Chain" offered by Lockheed Martin Company employees [13], most of which are available on the Internet. Currently, the arsenal includes hundreds of tools (for example, *BackTrack Linux* has more than 300 open- source security tool packages). Recently, new tools were exhibited at *BlackHat Arsenal* events within the framework of the *BlackHat* annual hackers' conference. Here are a few of the most common tools: Metasploit exploits platforms (for the open-source graphical interface *Armitage*); breaking passwords (HashCat; Cain & Abel); sniffer (Wireshark); wireless networks attacks (Wifite); social engineering tools (SET); a web applications vulnerability scanner (OWASP ZAP - Zed Attack Proxy Project); a network scanner (Nmap); Black Energy 2 botnet tool (used in a cyber attack against Georgia in 2008; some functions such as spam sending, data capture, and proxy servers were added to the second version).

Advanced cyber weapons differ from the usual viruses and Trojans in that they have some of the following features, which significantly complicate their identification and elimination:

- self-change of malware shape;
- e-scheme destruction capabilities;
- malware self-encryption (decoding);
- opportunities to violate wireless networks remotely;
- use of widespread, undisclosed commercial software vulnerabilities.

It is very important to pay attention to cyber attack and cyber espionage tools targeted at Supervisory Control and Data Acquisition (SCADA). Society is highly dependent on electricity, water, transportation, communication, banking and other infrastructures. These critical infrastructures are available through SCADA systems and accessed from anywhere. The most popular malicious software targeted at critical technological processes is the *Stuxnet* virus discovered by the Belarus antivirus company *BlockAde* in 2010. The *Stuxnet* virus targeted nuclear centres of Iran in 2010. The analyses show that the virus was written in 2009 and spread with flash disks, and uses fourzero-day vulnerabilities[14]. Here are a few most common tools: Metasploit exploits platform (for *Armitage* open-source graphical interface); breaking passwords (HashCat; Cain & Abel); sniffer (Wireshark); Wireless networks attack (Wifite); social engineering tools (SET); web applications vulnerability scanner (OWASP ZAP - Zed Attack Proxy Project); network scanner (Nmap); Black Energy 2 botnet tool (used in cyber attack against Georgia in 2008, some functions as spam sending, data capture, and proxy server were added to the second version).

After *Stuxnet*, other viruses (*Duqu, Flame, Gauss*) known as perfect cyber espionage tools (*Advanced Persistent Threat, APT*) attacked nuclear power stations or other industrial control systems delivering critical infrastructure services or targeted confidential information. The*Duqu* virus, which was spread by email, collected information about Iran's nuclear facilities using *Microsoft Word* security vulnerability. The developers of *Duqu* were whether the developers of *Stuxnet*, or they could explore the original source code of *Stuxnet*. Compared with *Stuxnet*, the *Flame* virus has a much more complex structure. *Flame* encrypts itself using five different encryption algorithms to be invisible in the computer, where it breaks into. The capacity of *Flame*, which consists of 20 different modules, equals 20 MB. *Iranian CERT (Maher)* reports that 43 antivirus programs could not detect it. The virus was identified through the human analysis. According to *Kaspersky Lab* experts, decoding of the virus requires a few years [15].

Gauss targeted certain countries to steal large amounts of banking and financial data. Security experts claim that the virus has been designed and programmed for five years, developed by a highly skilled team, and a certain state stands behind it. The analysis of *Stuxnet* and its successors (*Flame, Gauss, Duqu*) shows that such malicious applications are not created by a hacker group but a state-sponsored organization(s). It is believed that millions of dollars are spent on the development of the viruses. These viruses are so complex that a large group of specialists would be needed to produce them over the course of a few years [15].

The Elderwood Project confirms that cyber weapons are developed by industrial methods, and intelligence and cyber attacks are automated in cyberspace [16].A variable that determines where to find the attack code is called Elderwood. For this reason, the platform and the project are called Elderwood. In its report on the Elderwood Project, Symantec shows that the relatively large number of zero-day vulnerabilities is a distinctive feature of the Elderwood platform [16].

Large-scale scientific studies (X Plan) are being conducted on the development, planning and implementation of new technologies that allow large-scale attack operations in the dynamic network infrastructure of cyberspace in real time. Along with purely technical purposes, the X Plan was developed by the US Department of Defence's DARPA and involves the development of the nature, strategies and fundamental tactics of cyber war [17]. The following four main areas are crucial for the provision of supremacy in cyber warfare:

1. development of automated analysis methods for cyber operation planning;
2. development of automated cyber operation control technologies;
3. development of operating systems and specific platforms for certain operations in hostile environments;
4. large-scale interactive visualization of the cyber battlefield.

Cyber-troop potential of countries

Several open sources about the analysis of cyber-troop potential of North Korea are available [18]. The cyber-troop of this country consists of 3,000 elite hackers in cyber departments (*Office 91, Unit 121, Lab 110, Unit 35, Unit 204).*

Office 91 is the headquarters of North Korean hacking operations; and the majority of hackers belong to *Unit 121*. Most of the hacking operations and network leaks are performed by *Unit 121*. Its operations are performed outside of North Korea, and it has offices abroad, particularly in Chinese cities.

Lab 110 also performs similar operations. There are a few cyber departments under other branches of the government.

Unit 35 is responsible for cyber agents' training, and it controls internal cyber investigations and operations.

Unit 204 is involved in online espionage and psychological warfare.

Office 225 conducts training of agents to work in South Korea, sometimes with a cyber component.

In 2009 North Korea organized six large cyber attacks against South Korea, which caused damage estimated at 780 million USD. In response, in 2010 South Korea established its Cyber Defence Command. South Korea is planning to double its cyber defence and reach 1,000 units by 2030.

China began to prepare for network war in1999. Chinese hacker actions aimed at the theft of production technologies of American companies have long been a source of controversy between the two countries. American experts claim that the damages caused by China's economic espionage amounts to more than 300 billion USD. China persistently denies the accusations about cyber espionage against American companies and cyber attacks against the critical infrastructures of the country. According to experts, at present, cyber-troops of China consist of nearly 6,000hackers [19]. Some mass media call all these happenings "cold cyber warfare".

"The Science of Military Strategy" published in 2005 by the research institute of the Chinese People's Liberation Army, showed the cyber-troops within the troops of the People's Republic of China for the first time [20]. Chinese encyclopaedia distinguishes three classes of cyber-troops. "Paramilitary special computer troops" focus on cyber attacks protection, and carry out cyber attacks. The second class includes civilian experts (20,000 "patriot hackers") who have the right to carry out "network combat operations". Finally, the third class includes non-government "external elements", which can be mobilised to perform malicious actions in networks (about two million agents).

Israel plans to establish a digital "Iron Dome" to protect vital infrastructures from cyber attacks, and it invests significant resources toward that end. Within the framework of the program,16 to 18-year-old talented students master the art of cyber attack prevention during three-year courses.

The Spanish Cyber Defence Command is expected to be fully functional with 70 experts (Retamares military base near Madrid). The Command is responsible for providing the integrity and confidentiality of the data of the armed forces, and it is in charge of coordinating and directing the performance of the information security incidents processing centre.

There is serious competition for authority in the field of cyber security between US intelligence services and military structures. In 2002 the Strategic Command was in charge of establishing the United Cyber Command for all military activities in cyberspace, but in fact, the military operations in the network were implemented by the Military Air Forces, and the first Cyber Command was established on the Military Air Forces (MAF) base (Barksdale, Louisiana) in 2007.The obvious dominance of MAF was not accepted in other troop structures. After long negotiations, it was decided to establish a structure which integrated the actions of the troops, and in June 2009, US CyberCom was created under the US Strategic Cyber Command. Its main duty is to ensure the freedom of the US and its allies and to implement operations to reduce the freedom of enemies in cyberspace. The structural and organizational model of the US Cyber Command can be an example for other countries. In 2013, US CyberCom planned to increase the number of cyber-troops five-fold from 900 to 4,900. Establishment of the Cyber Warfare Intelligence Centre was the next step in the development of US cyber-troops.

By 2014, Russia planned to establish a Cyber Command responsible for military information security, according to the US and NATO models (some sources indicate an extension of this period up to 2016). Cyber-troops are expected to recruit mathematicians, programmers, engineers, cryptographs, communicators, radio-electronic combat specialists, translators and other highly qualified specialists. The press publicised the establishment of a prospective defense research fund similar to the US agency DARPA.

In 2008, the NATO Cyber Defence Centre was established in Tallinn, and it was given the status of an international military organization. In 2009, NATO shifted from a "cyber security" term to "cyber defence", and increased the budget allocated for cyber projects by 40 times. NATO's new strategic concept adopted in November 2010 defined cyber defence as one of the priority areas. Prompt response forces were planned to be established for the defence of cyber communication systems and infrastructure, and the necessary assistance and support to countries affected by cyber attacks was planned. At the beginning of June 2013, the NATO Defence Ministers Assembly decided to establish cyber-troops. The General Cyber Defence system was scheduled to be launched by autumn 2013. In the next phase, the necessary resources were planned to be developed to support communication systems and infrastructure.

Features of cyber weapons

Conventional weapons significantly differ from cyber weapons in terms of creation, distribution, testing, use, aging and costs [21]. A cyber weapon is an application code based on knowledge about the vulnerabilities of a target system, or an interaction between the vulnerable

system and the user. Cyber attacks are possible only if the potential vulnerabilities are hidden. If the vulnerability of the target system used by the cyber weapon is discovered and removed, then the cyber weapon becomes useless. Expansion of the cyber weapon arsenal requires seeking new vulnerabilities. In this regard, the specialists in identifying the vulnerabilities in the software are the most valuable human resources in the cyber-troop.

Knowledge of the vulnerabilities and the skills to exploit them are of particular importance for any form of cyber-conflict. Obviously, if there were no exploited vulnerabilities, the cyber attacks would be limited to the users' manipulation through social engineering for denial of service (DoS) attacks, which are not based on the vulnerabilities of target systems; they reduce the availability of the system by weakening the communication channel bandwidth, the central processor or another limited resource.

Both available (disclosed) vulnerabilities and undisclosed vulnerabilities (zero-day vulnerabilities) are used for cyber weapons' creation. On average, the number of zero-day vulnerabilities discovered over the years is low. According to Symantec reports, eight zero-day vulnerabilities were disclosed in 2011 [22]. Zero-day vulnerabilities are of particular importance for the production of cyber weapons; however, disclosed vulnerabilities are widely used as well. Some vulnerabilities remain unresolved ten years after their disclosure [21].

There are several strategies for disclosure of discovered vulnerabilities (e.g., RFPolicy) [11], and "black market" vulnerabilities also exist. Typically, after the vulnerability is discovered, the software manufacturer develops some adjustments ("patches") as soon as possible to eliminate the vulnerability and makes the patch available to users. These adjustments must be tracked and installed by users in a timely manner. Due to the dynamic nature of information technology, gaps vary and new vulnerabilities are disclosed daily. A number of databases, message lists, and paid or free data services about the known vulnerabilities are available. The Vulnerability Database founded by the US National Institute of Standards and Technology is considered the authoritative source on the vulnerabilities [11].Vulnerabilities vary in severity. Some vulnerabilities allow organized cyber attacks against the target system of the enemy, but some do not bring profit for the attacker. The CVSS system provides a method to assess the severity of the vulnerabilities according to their unique characteristics and behavior [11].

Cyber weapons' production costs are mainly related to the human resources involved. The initial investment in research and design is necessary, but the success of individual hackers and small groups (for example, *Anonymous, Lulzsec*) shows that much can be achieved with limited resources. Compared with the creation of modern conventional weapons, the production of cyber weapons is less expensive for states. Cyber weapons are based on human knowledge and relatively inexpensive computer equipment. Knowledge (and skills) in software engineering and penetration tests are the origin of cyber attacks. Involvement of properly chosen specialists and expansion of their knowledge is an essential investment to maintain and increase the arsenal of cyber weapons. Being aware of the target's vulnerabilities and their use is very important for attackers, and this knowledge is very important to build an effective defence.

This leads to the first paradox of cyber weapons [21]: cyber weapons decline over time. If the cyber weapon exploits a certain vulnerability, its effectiveness continues as long as the vulnerability exists in the target system. The second paradox of cyber weapons [21] is that the use of cyber weapons can lead to the strengthening of the protection of the target system. After the application of the cyber weapon, the target can detect the attack and analyse how it is implemented. The first attack can be successful, but after that, the defence will be much higher, which makes the cyber weapon useless.

Testing imposes certain restrictions on cyber weapons; after a cyber weapon test, the target will be aware and find a way to be protected from the attack. Like other files, these cyber weapons may be copied without expenses, and therefore the number of cyber weapons is incredibly high. Storage and transportation of cyber weapons are easier than of conventional

ones. Cyber weapons can be held beyond the country's borders by hiding its copy or all cyber weapon arsenals in various parts of the Internet. Cyber weapons do not have a physical nature; they contain data and knowledge. The data should be delivered to the attacked target to use the cyber weapon. This is achieved, for example, by typing a command or application, automating it and making it sustainable in the information system.

Development of human resources for cyber-troops

The article "How to build a cyber army to attack the US" [23] offers the following professional staff for cyber-troops (the number of people is shown in brackets): vulnerability analysts (10), exploit programmers (70), remote staff (20), bot collectors (60), bot servants (220), operators (60), programmers (40), testers (15), technical consultants (20), system administrators (10), and managers (57).One of the biggest challenges in the formation of cyber-troops is a staff provisioning. There is a lack of specialists, and the government cannot compete with private entities by offering favourable terms for information security experts to work in public institutions. The problem is common to most countries. The number and quality of students studying in science, technology, engineering, and mathematics (STEM) is an important indicator for the development of human resources for cyber-troops.

The US Naval Academy (Annapolis) trains specialists on cyber-operations (the first class will graduate in 2016). The Academy managers are believed to have spent about five years developing the course curriculum. The future professionals are trained in cyber technologies and attend compulsory courses covering cyber policy and economy. The students will have the opportunity to practice in civilian information technology companies and government agencies such as the National Security Agency and the Federal Bureau of Investigation.

The systems for certification of knowledge in information security. The systems for certification of knowledge of specialists of universities and a number of companies (SANS Institute, Microsoft, Cisco, etc.) and international consortiums (ISACA, ICS 2, EC-Council etc.) play an important role in staff training on information security. More information about certification systems in information security is available at [11] including information about Certified Ethical Hackers (CEH).

The CEHv8 exam of the E-Commerce Council (EC-Council) is one of the most important systems in the certification of knowledge of experts in the field of information security, and it is approved by the US Department of Defence. The certificate confirms an appropriate level of knowledge in the field of network security.

CEH-certified ethical hackers are experts in the field of network security and use hackers' knowledge and tools to discover system vulnerabilities. The CEHv8 certification exam covers the vulnerabilities of network protocols, operating systems, and application programs, Trojans, viruses, rout kits, data collection, network scanning and resource inventory, hacking web-servers and wireless networks, deception of information security tools, penetration tests, DoS attacks, SQL injection attacks, sessions seizure, and so on.

Competitions on information security. Participating in information security competitions is a valuable opportunity to gain experience and to train in information security. Currently, a variety of events are organized:

- website security (Hack This Site);
- competition among VSFI system administrators;
- cyber security competitions (US Cyber Challenge);
- cyber warfare games (Over The Wire, DC3, NetWars);
- Capture the Flag (CTF)

CTF-type team competitions are the most popular ones. As a rule, the competitions require skills in reverse engineering, network management, network and protocol analysis, programming and crypto-analysis. A CTF-type competition was first held at the DEFCON hacker conference

(1996, 4th DEFCON). An international competition for university students, UCSB iCTF, was first hosted by the University of California, Santa Barbara, in2004. In Russia, CTF competitions were organized by the HackerDom Ural State University team in 2008. Since 2009, the international RuCTF competitions have been held among students. Currently, CTF competitions are hosted by many universities (e.g., RwthCTF, CSAW CTF, CTF Hust, MIT/LL CTF, RuCTF), and some companies and organizations (e.g., Mozilla CTF, Phdays CTF, OWASP Global CTF, CODEGATE). CTF competitions among high school students also occur (Codegate Global Junior CTF).

Cybersecurity trainings. At present, large-scale cyber security trainings are organized in a number of countries. Cyber Storm is a large-scale and real-time cyber-training held in the United States biennially since 2006. The training enables the participants to assess their own capabilities about awareness, defence and response to the cyber attacks. Similar trainings have been held in Europe since 2010 (Cyber Europe 2010). During the trainings, a mock global DDoS attack on critical elements of e-governance infrastructure in the EU was executed. The aim of the trainings was to verify the level of preparedness for the failure of communication between critical elements of digital infrastructure in the EU states.

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE, located in Tallinn) has held one-year cyber-trainings in information technology since 2008. In 2013, Locked Shields trainings monitored the effectiveness of protection against cyber attacks, and the trainings were attended by 250 specialists from nine European countries. In 2011, the EU and the US held the first cyber security training, Cyber Atlantic 2011. The training was attended by the experts from 20 EU countries and about 100 from the US. Two scenarios were used there: 1) an advanced persistent threat (APT) attack aimed at accessing and publishing confidential information of the EU member states; 2) failure of the industrial SCADA-systems used in power supply units. Interaction methods between the EU and the US were tested within the framework of the trainings.

International cooperation and coordination issues in the field of cyber security

At present, the departments dealing with cyber security have been established in other government agencies to ensure that the responsibility for cyber security is shared between several entities. These entities function alone, and sometimes there is a risk that they will act based on their own interests. Therefore, it is very important to ensure the coordination of cyber security in all areas. A National Cyber Defence Centre is proposed to be established, which coordinates the work of various structures, and acts as the central unit of decision making and implementation of public policy.

State policies regarding cyber security should be formulated, and common legal documents that determine responsibility for cyber security and the authority of government agencies should be adopted. The solutions to some problems concerning state sovereignty can only be made possible with the development of international and regional cooperation, the unification of the efforts of countries and the adequate assessment of risks.

The defensive nature of disarmament, cyber security strategies, stopping rapid armaments and adopting the Digital Geneva Convention are also pressing issues: the vital infrastructures of the civilian population such as electricity, water, and healthcare should not be attacked as. The violation of the Convention should be considered a war crime.

Conclusion

New divisions should be established to combat cyber-threats in the armed forces to safeguard the national interests of the country in rapidly changing cyberspace. It is important to protect the information security of the armed forces and the entire country. Cyber-command

formation, determination of its functional duties, and staff recruitment require significant governance efforts, human resources and the highest level of scientific research.

References

1. Alguliyev R.M., Imamverdiyev Y.N. E-government, information security: Actual research directions // Problems of Information Society, 2010, No 1, pp. 3-13.
2. Clarke R.A., Knake R. Cyber War: The next threat to national security and what to do about it. Harper Collins 2010, 304 p.
3. Evron G. Battling botnets and online mobs. Estonia's defense efforts during the Internet War // Georgetown Journal of International Affairs, 2008, vol. 9, no. 1, pp. 121-126.
4. Hollis D. Cyberwar case study: Georgia 2008 // Small Wars Journal blog, 2010, http://www.smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf
5. Gumahad A. T. Cyber troops and net war: The profession of arms in the information age. BiblioScholar, 2012. 68 p.
6. Conti G., Surdu "Buck" J. Army, navy, air force, cyber: is it time for a cyberwarfare branch of the military? // Information Assurance Newsletter, 2009, vol. 12, no. 1, pp. 14-18.
7. Owens W.A., Dam K.W, Lin H. S. (eds.) Technology, policy, law, and ethics regarding U.S. acquisition and use of cyberattack capabilities. National Academies Press, 2009, 390 p.
8. Geers K. Strategic cyber security. CCD COE Publication, Tallinn, Estonia, 2011, 168 p.
9. Alakbarova I.Y. Information warfare technologies. Express-information. Information Society series. "Information Technologies" Publishing House, 2012, p.108.
10. Libicki M. What is information warfare? // National Defense University, 1995, 110 p.
11. Alguliyev R.M., Imamverdiyev Y.N. Information security incidents. Baku: Information Technology, 2012, p.212
12. Floridi L., Taddeo M. The ethics of information warfare. Springer. 2014, 145 p.
13. Hutchins E. M., Cloppert M. J., Amin R. M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare and Security Research, 2011, pp. 78-104.
14. Langner R. Stuxnet: dissecting a cyberwarfare weapon // IEEE Security & Privacy, 2011, vol. 9, no. 3, pp. 49-51.
15. Gostev A. The Flame: questions and answers. 2012, http://www.securelist.com/blog/incidents/34344/the-flame-questions-and-answers-51
16. O'Gorman G., McDonald G. Symantec security response report: The Elderwood Project. September, 2012, 137 p.
17. DARPA Information Innovation Office Programs: Plan X, http://www.darpa.mil/Our_Work/I2O/Programs/Plan_X.aspx
18. HP Security Briefing - Episode 16 "Profiling an enigma: The mystery of North Korea's cyber threat landscape," August 2014.
19. Mandiant. APT1: Exposing one of China's cyber espionage units. February, 2013.
20. Peng G., Yao Y. (editors) The Science of Military Strategy. China Military Science Publishing House, 2005, 504 p.
21. Czosseck C., Podins K. A vulnerability-based model of cyber weapons and its implications for cyber conflict // International Journal of Cyber Warfare and Terrorism, 2012, vol. 2, no. 1, pp.14-26.
22. Dumitras T., Bilge L. Before we knew it: An empirical study of zero-day attacks in the real world / ACM Conference on Computer and Communications Security, 2012, pp. 833-844.
23. Miller C. Kim Jong-il and me: How to build a cyber army to attack the U.S., DefCon 18, 2010,http://www.defcon.org/images/defcon-18/dc-18-presentations/Miller/DEFCON-18-Miller-Cyberwar.pdf