CYBERSPACE – A MAN MADE DOMAIN FOR WARS

Tawhidur Rahman
PCSS EnCE CCISO ACE,CFIP SCCISP,CCTA
Senior Technical Specialist(Digital Security & Diplomacy),
BGD e-Gov CIRT
Bangladesh Computer Council
Ministry of Posts, Telecommunication and Information Technology

Internet can be considered as one of the greatest achievements of humanity of the last century, which connected the entire world. It created a new space for connections, information and communications, as well as cooperation. Thus, it created also a new platform for conflicts that involved not only individuals but also states. The invention of the twentieth century, the Internet, has become another sphere for international relations, and a new space for defensive and offensive policies for regulating and balancing those affairs. The space called cyberspace has become a platform for interactions not only between individuals, but also between states. The interactions on their side were not only developed in a positive manner, but were also transformed into attacks, which pose a real threat to the security of states. Thus, the following questions arise:

Can cyberspace be considered a new sphere for war? Can conflicts and offensive and defensive operations in cyberspace be considered a real war?

The aim of this article is to specify offensive and defensive actions occurring in cyberspace and to explain the differences and similarities between them and the classical approach to war present in other spheres: land, water, air, and space. Despite the overgrowth of offensive interactions in cyberspace and defensive strategies for enriching the cyber arsenal of states, military specialists have concerns over the reality of cyberwars in general. Parallels are drawn to show the similarities and differences between definitions and perceptions of war, and whether concepts from the classical approach can be transferred to describe wars in the cyber sphere. This research puts cyberwars in line with other wars, thus analyzing their peculiarities, whilst Cyberspace is seen as another sphere for war and international re lations in addition to the existing spheres of land, water, air, and space

Internet's Two Sides of the Coin: From Good to Threat.

The Internet that we use today, is based on the Transmission Control Protocol or just Internet Protocol commenced in 1973. The network became operational in January 1983. For the first two decades of its existence, it was the preserve of a technological, academic, and research elite. From the early 1990s, it began to percolate into mainstream society and is widely regarded as a General-Purpose Technology (GPT) without which modern society could not function. [1, pp 5-28]

Only half a century ago it was difficult to imagine that human interactions would be developed in a manmade sphere, totally virtual and artificial. It must have been impossible to imagine that it would penetrate our lives so closely that it would cover everyday life, from communication and information sharing to purchasing products and regulating temperature at home.

Now Internet has connected the entire world breaking the land borders that previously lined geographically differentiating the places where people live. It substituted land borders with digital ones, making it possible to connect the entire world into one sphere.

With the start of the World Wide Web in 19931, the greatest accretion of communication came into existence. Since then, information being secret for a limited groups or organizations that were historically used for military purposes as an intellectual advantage, soon became available for masses.

Moreover, equal access to information for all, one of the ultimate achievements of humanity and one of the supreme advantages of the internet, has started to provide information not only for good will, having also provoked irregular warfare.

These chaotic interactions, which Garnett called "fourth generation warfare" [1, pg. 202] (4GW), through networks would become a wave of social reactions and pressure that would provide an opportunity for an asymmetric warfare. The tendency is obviously dangerous since not only states possess these "digital" weapons but also non-state actors including terrorist networks. Basically, the Internet allows anyone to join digitally and to be a force or power that could have a significant impact on states' policies.

The sphere were those actions take place with the usage or within the system of information and communication technologies is broadly named cyberspace and the actions that take place in this sphere get their terminology accordingly; cyber-attacks, cyberwar, etc. Though states

have various definitions of a cyberspace and with the scope it covers, it is meant to be a non-physical Information and telecommunication technologies environment (ICT). [5, c 17] The term cybersecurity has been emerging from the US since the mid-1990s, which later have become widely used in other countries and international organizations such as United Nations (UN), Organization for Security and Co-operation in Europe (OSCE), Organization for Economic Co-operation and Development (OECD), North-Atlantic Treaty Organization (NATO), the Council of Europe (CE), BRICS, Shanghai Cooperation Organization (SCO) and many others.

A cyber-attack is not an end in itself, but a powerful means to a wide variety of ends, from propaganda to espionage, from denial of services to the destruction of critical infrastructure.

From the prism of threat, they may cause, cyberattacks can be implemented using methods, such as malicious programs, that can penetrate systems of specific or not specified group of people or entities causing dysfunctions of computer operations, stealing personal information, phishing stealing passwords of the user as well as infecting computer systems to slow down specific processes, etc. In current internet-run infrastructure a single penetration can be fatal for a society and become a threat for a state. A penetration into the command-control system of critical infrastructures, for example, can cut the supply of energy, change the chemical construction of water thus making it poisoned, etc. and the anonymity can stand as an advantage as cyberattacks are still not attributable through international humanitarian law. Moreover, in a cyber conflict, the terrestrial distance between adversaries can be irrelevant so cyber weapon can reach its target much beyond its borders.

The advance of technology made it possible to give room for clashes between States and non-states actors involved in operations in cyberspace. These clashes have become a real threat for international security. As compared with kinetic weapons that are relatively expensive to obtain, as well as possible to detect their origin, malicious programs are available to download or buy and even create if there is a good specialist of it: even a teenager can formulate it.

Therefore, it is becoming nearly impossible to patrol all the purchase and supply chain of the cyber arsenal. Malicious viruses or programs can penetrate various computer systems of public and private usage and cause dysfunctions, changing the primary command-control systems, slowing their base speed of operation and causing very costly problems for state security.

Per media reports, the group which rampaged through and besieged part of Mumbai in November 2008 made use of readily available cellular and satellite phones, as well as overhead imagery from Google Earth, to coordinate and plan their attack. [1, pg. 204]

However, this invention is an issue of arguments among scientist from the prism of war definition.

Theoretical Dilemma of Cyberwars and Cyber Reality

Despite different conflicts occurring in cyberspace between state and non- state actors, state-sponsored operations, and developments in international relations, military specialists argue about the exact definition of cyberspace, whether to evaluate it as real war or not, and as whether to count operations in cyberspace as a real war between parties involved.

Various conflicts in cyberspace including attacks of regular and irregular origin performing symmetric or asymmetric tactic, do not correspond with the classical approach of the war including only some or one or even missing any aspect of the war characterization. Despite of the current actions and bilateral, multilateral etc., agreements signed by states and international organizations, associations on the cybersecurity issues and despite of the threats the world overcomes or will overcome in cyberspace, theorists have certain disbelieves while defining or accepting cyberspace as a new sphere for wars as well as cyberwars as already occurring facts.

The issue is that there had not been a single verifiable case of cyber terrorism nor has there been any human casualty caused by cyber-attacks, giving grounds for disbelief.

Thomas Rid, a specialist of war, is among those scientists and experts who see debates about cyber wars exaggerated, moreover, he expresses mistrusts related to cyberspace as a new space for war in a classical approach of war definition. He believes that "Cyber war has never happened in the past, it is not occurring on the present and it is highly unlikely that will disturb the future." [3, p 77]

The fact that computer and Internet assisted attacked may penetrate the operating systems of targets stealing data or causing dysfunction of potentiality of operations Rid, however, in this respect differentiates between sabotage operations and direct physical harm.

Rid refers to Carl von Clausewitz, a nineteenth-century Prussian military theorist, who defines war according to three criteria, "First, all acts of war are violent or potentially violent. Second, an act of war is always instrumental: physical violence or the threat of force is a means to compel the enemy to accept the attacker's will. Finally, to qualify as an act of war, an attack must have political goal or intention." [3, p 77-79]

Theoretical description of war through centuries might have changed its primary strategies and instruments, while his goal is always the same. Within this respect, it is important to observe this definition on a broad way: Of course, computer warm or virus cannot kill directly a person, like it could have a sword, but it can cut the energy supply of a hospital causing a chain of violence, or it can penetrate the command control of the Airplane system and change the direction of the plane or to cause and a catastrophe.

In contrary to classical approach of war, the reality of cyber war is supported by those who believe that cyber wars have already occurred, are occurring and will, possibly, continue to occur in future, thus cyber strategies must be implemented.

In July 2016, Allies reaffirmed NATO's defensive mandate and recognized cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea.2

Former U.S. President Obama speaking about cybersecurity mentioned: "America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for

the free exchange of ideas". 3

Thomas Reed, a former staffer on the US National Security Council argues that Cyber wars are even new. They occurred in past, in Cold War Era, and had devastating results. As an example, he mentions about the first ever cyber-attack- a massive pipeline explosion in the Soviet Union in June 1982, counting as the most violent cyber-attack ever. "According to Reed, a covert US operation used rigged software to engineer a massive explosion in the Urengoy-Surgut-Chelyabinsk pipeline, which connected Siberian natural gas fields to Europe. Reed claims that Central Intelligence Agency (CIA) managed to insert malicious code into the software that controlled the pipeline's pumps and valves. The rigger valves supposedly resulted in an explosion that the US Air Force rated at three kilotons, equivalent to the force of a small nuclear device." [3, p.78]

Although, neither there are factual evidence of accident being a cyber-attack confirmed or supported by the official U.S, nor there are any Soviet media reports from 1983 also confirming that Reed's mentioned explosion took place. Though Soviet Union media regularly reported about accidents and pipeline explosions at the time. [3, p 79] In case of cyber-attacks, it is not an easy task to investigate fully and in a short period of time. Forensic examination is needed which presupposes experts and conditions for objective examination. Under the condition of Cold war, the parties would hardly agree to do such an investigation that will reveal secrets about their technical capabilities and the real cause of the explosion. Incase Reed's claims are true, then the massive violence it could have done would theoretically rank cyber weapons among extremely dangerous means and cyber wars would have been defined accordingly.

Another example that speaks about possible cyberattack that will "suit" to the description of war can be considered the 2008th cyberattacks on Georgian most prominent websites, including those of the country's national bank and the Ministry of Foreign Affairs. In August 2008, in the period of the military conflict over South Ossetia, Georgian Government blamed the Kremlin, but Russia denied sponsoring the attackers,4 and later NATO investigation found no conclusive "proof" of who had carried them out. The fact that the "proof" is not found can illustrate two possible judgments: first, the attacker is technically equipped well enough so it is hard to distinguish him, second: a potential suspect did not carry out the attack. However, the situation can be judged by the following viewpoint: you are innocent unless your guilt is proved. And because the anonymity is a priority in cyber wars, so it is highly efficient especially for states to use it in hybrid war strategies.

In cyberspace the sides, that are involved in the attacks or counterattacks can be distinguished only in two ways: first, by their own wish (which may occur rarely, or even impossible to happen especially when attacks are carried out by States rather than other subjects) or, according to the evidence. The last one is directly connected with the technical capabilities of an attacker as well as technical competences of an attacked side to be able to detect.

According to Oleg Demidov, a Cybersecurity expert at the Russian Centre for Policy studies (PIR Center), the overview of the NATO experts suspecting Russia in attacking Estonian infrastructure in 2007, Georgian government and private sector networks in 2008, and U.S. financial institutions and private companies in 2014 Spring, as not fundamental, because there was no practical evidence of the proof of the attacker, or lack of technical capabilities to be able to define the source of the attacker. [2, p.39-40]

In his contribution "Global Internet Governance and International Security in The Field of ICT Use", Demidov stresses high possibility and risk of an international conflict between nuclear-weapon states. As he mentioned: "In the event of lighting-fats cyber-attack that imitates the 'signature' of Russian perpetrators (for example, Cyrillic code fragments and other linguistic patters) and targets the infrastructure of NATO countries using servers in Russian territory, there is a risk of NATO military retaliation against Russia. In accordance with NATO doctrine, retaliatory measures may include the use of kinetic weapons and the involvement of all NATO members in a retaliatory strike". [2, p.40]

These two cyber incidents- the Georgian cyber-attacks and Estonian cyberattacks, are regarded by the U.S. and other Western nations as causes for great attention and much reflection. [4]

The Estonian cyber incidents were followed by the establishment of cyber strategies for national and system level for EU members and partners.

Particularly, in 2008, a year after the attacks, NATO set up the Cooperative Cyber Defense Centre of Excellence (CCD COE) in Tallinn. The military-defense usage of Information and Communication Technology (ICT) is one of the main purposes of the center.5 The center is technically equipped well enough to protect its members by providing technical support and human resource to protect Internet infrastructure.

Another well-known and destructive cyber program that processed a worldwide discussion over the reality of cyber wars is the "Operation Olympic Games", a large operation, that included the "development, testing, and use of malware against specific targets to collect information about the Iranian Nuclear program, as well as to sabotage it and slow it down as much as possible. It included such malware as Stuxnet, Duqu, Flame, and Guass (all of them targeting special operation for espionage and sabotage), active in between 2007-2013. [4, p29] The US presidential administration and Israeli secret services have been named as perpetrators.

Ex-head of the Foreign Relations Committee of Iran's Supreme National Security Council Seyed Hossein Mousavian, in his "The Iranian Nuclear Crisis: memoir confirms Stuxnet as a malicious computer warm developed to target the computer system that control Iran's huge enrichment plant at Natanz. Moreover, according to Mousavian, Ali Akbar Salehi, Iran's Representative to the International Atomic Energy Organization (IAEA) at that time confirmed that Iran was experiencing espionage at its nuclear plants. According to the IAEA, there was a big decrease in the amount of the operating centrifuges caused by the Stuxnet with a vivid decline to more than 100 - from 4920 in May 2009 to 3772 in August 2010. Despite of the Fact that Ahmadinejad mentioned about the problems directly related to the computer software, installed by the spies to slow down centrifuge's operation, nevertheless, Mousavian does not think that this could have cause a big problem and an obstacle for enriching the centrifuges. [5, p24-26]

In fact, Stuxnet did affect the nuclear enrichment system, and did make problems for Iran's nuclear program. The computer worm was operating inside the system for quite a long time unnoticed, slowing down the operational capabilities of both

experts and technical equipment. If we note the fact that it successfully slowed down the system's operation, then we can conclude that operations reached a certain level much later then they could have without the worm Now that sanctions have hit Iran's economy and forced it to make concessions, we can conclude that the situation would have been different if Stuxnet had not affected Iranian programs; Iran would have finished its program faster, before sanctions could devastate its economy.But since Iran discovered the problem much later and the whole process was slowly altered by the worm, we can see that Stuxnet led to a longer timeframe for enrichment, and subsequently longer terms for sanctions.

The action brought not only psychological damage, as would be named and labeled by Israel and U.S. specialist, but it brought also to economical, technical (human resources as well as technical capabilities) crises.

As the Armenian researcherMherSahakyan mentions: "…sanctions were hard and maybe they were the main reason why Iran agreed to the Interim agreement. Though Iranian leaders like to mention that sanctions were not problem, but the Iranian economy had been effectively hit hard by these sanctions. Iranian economy mostly declined when EU member states imposed an oil embargo on Iran. China also reduced its average oil import levels from Iran in a disagreement on Iran's nuclear program. The depreciation of Iranian Rial, reduction of oil exports and shortages of foreign currency created hard social-economic situation in Iran. So sanctions were hard and maybe they were the main reason why Iran agreed to the Interim agreement." [6.p58]

It is evident that, not directly but indirectly cyber war may influence politics of a specific State. Today cyber-attacks can target political leadership, military systems, and average citizens anywhere in the world, during peacetime or war, with the added benefit of attacker anonymity.

Stuxnet influenced the Iranians' centrifuges, causing them to overload an intelligence program. This is a new type of and reason for war. While the basic definition of war presupposes physical violence, Stuxnet presupposes a psychological intent. In addition to the technical harm it did, it also influenced the psychology of those who had encountered the undiscovered cyber worm. Regarding the first, undiscovered phase of the computer worm, imagine a specialist working on the program, who faced long-lasting technical problems, becoming filled with doubt towards their personal professional skills and also doubting the capability of Iran in general to develop its program. This is a new approach in the definition of war, as it dramatically shifts the choice of instruments that can cause harm to a State.

From Wars with Swords to Cyber Wars: State Security is Still a Priority

Nevertheless, the war in cyberspace is real, it has happened in the past, it is happening now and it will certainly happen in future.

The classical approach to war sees physical violence carried out by military operations. Cyberwar presupposes physical violence as well as bringing a new, psychological violence, which may cause no less harm. Ideas and things important for state security have changed over the centuries, as have the instruments and measurements of security, but the problem of state security is still a priority. Maybe unexpected ships won't attack from the sea, but cyber-attacks will come.

In past centuries, population size was an important issue for the state in maintaining its governance. It determined the size of the workforce and the size of the army, and the strength of armies was measured by the quantity of troops.

Centuries ago, a human, a good soldier was to aim to harm the opposing side. To conquer the army was to win the war. Afterwards, the period of weapons and technology began, and would enable opposing sides measure their technical and tactical capabilities to win. At that time, to mobilize technical capabilities was to conquer the army. Due to growing population and technological achievements, in addition to the number of troops, now the amount of military equipment is of much importance. A single-pilot jet may cause greater harm than 1000 troops on the same territory. Nowadays unmanned aircraft can jeopardize enemies' strategic targets in specific cases even without any physical violence, because in a certain situation to harm a strategic unit even without causing physical violence from neither attaching side nor from the attacked still may have fatal result for the states being attacked.

In current stage, the military parades mostly demonstrating technical capability of a certain state, will alarm a possible harm while attack or attacking. Aside from the traditional military spheres like land, sea, and air (added later), an epoch of adding a new sphere, cyberspace, has begun, in which technical capabilities do no less harm than in a traditional war. One of the ultimate advantages of cyberwars is the anonymity of the attacker, which makes it a reasonable choice for state's foreign policy.

In addition to the traditionally distinguished types of harm for a state security, cyberwar brings the conception of psychological trauma for the sates making it doubt its capabilities on a certain level. In the case of Stuxnet, the attack was "emotional" and technical.

The definition of the emotional damage through cyberwars was used to describe Russia's so-called internet interference in 2016. "The NewYorker" expresses viewpoints of national-security officials who believed that those series of cyber hackings were directed to destabilize the conception of democracy in the States. For many national-security officials, the e-mail hacks were part of a larger, and deeply troubling, picture: Putin's desire to damage American confidence and to undermine the Western alliances—diplomatic, financial, and military—that have shaped the postwar world.6

To technically dysfunction a system just causing a technical harm is a small incident, while targeting CI with technically destabilizing them already has grown into a political scandal.

In turn, cyberattack may cause harm on a specific target without involving other sides especially in case of state sponsored attacks, as it remains undiscovered for a while and the stereotypes and cliché of the traditional war definition will empower the attacker to have "excuses" for the attack. Cyberwars will become more dangerous, if not included and named as war and not struggled as traditional wars.

Cyber Arm race has started.

Despite of the distrust and interpretation of cyberwars within the framework of classical approach of war, states are accelerating cyber arms race. This development has several political and strategic implications that pose the need to find specifically political answers. What is often forgotten or neglected is the increasing importance of

understanding cyberspace as a political domain and cyber politics is needed more than ever before. [7, 50-60]

While experts are debating over the exact description and definition of cyberwar, States are enriching their State defensive arsenal with cyber equipment and technical staff for better governance in cyberspace, as well as regulations and doctrines that will define the strategy for the defensive and offensive operations for ICT threat.

In November 2011, the Department of Defense of the U.S. issued a report to Congress confirming, that it was ready to add cyberspace to sea, land, air, and space as the latest domain of warfare – the military would, if necessary, use force to protect the nation from cyberattacks. [8] This statement shape the interactions in cyberspace on the same level with other spheres making them equally important and in case of need, changeable and cooperative.

By this, next to the traditional war spheres: ground, sea, air, space, a new battlefield-the cyberspace is differentiated.

With the technological developments, nearly every aspect of our lives is technically run, so it becomes very sensitive to any cyberattack, since any non-functioning in a technical field may cause human harm, economic harm, and be a serious problem for the entire National security. In this regard, the former Secretary of Homeland Security of the U.S. Jeh Johnson at The White House Cybersecurity Framework Event on February 12, 2014, specifying the seriousness of the cyberattacks on electrical substations specifically, mentioned: "What the public needs to understand is that today the disruption of a critical public service like an electrical substation need not occur with guns and knives. A cyberattack could cause similar, and in some cases far greater, damage by taking several facilities offline simultaneously, and potentially leaving millions of Americans in the dark". 7

The focus was on the electrical substations but it may refer to other sectors too: telecommunication, hospitals, libraries and federal departments courts and prisons. Any entity that is functioning with technology may be in a real attack risk.

The technological developments of the last century bring the automated industrial control systems as well as most Critical Infrastructure (CI), the list of which may vary from state to state but have similarities, under possible cyber-attack that may be fatal for national defense. The range of facilities on the list of CIs may include but not limited to nuclear industry, electricity, telecommunication, water supply, transport system on ground, sea and air, governmental buildings and their communication facilities, the financial and banking system, healthcare and defensive facilities etc. In 2017, the USA Department of Homeland security announced about its decision to include also election infrastructures into the list of Critically Important infrastructure for the State.8

The cyber- defensive policy of states becomes an urgent issue and States are engaged in implementing special cybersecurity projects on national level to defend the CI of their countries.

Many states, for instance the U.S., Russia, China, Germany, UK, France etc. are enriching their cyber arsenals and developing cyber security system for defensive operations for their countries. Not only states are engaged in national mechanisms but they also are involved in developing global cooperative platforms for better and clean cyber environment of the World. Specifically, it would be interesting to mention U.S. Russia, China cyber triangle and their input of cyberspace as a significant priority for a State development and Security. The countries are involved in various discussions and cooperation agreements to maintain cooperation and peace in cyberspace globally. Despite of ideological differences in cyberspace and the attitudes of maintaining the policy for it, however these three cyber powers found a common ground for mutual understanding and possible fundamental cooperation. United Nations (UN) Governmental Group of Experts is one of the examples of that which is currently the only platform that has united the U.S. Russia, and China with commonly acceptable norms and suggestions.9 Since the scope of interests in cyberspace includes all groupings of society including governmental and federal entities private and public sectors as well as common citizens on a national level, private supra-powers regulation beyond borders and being responsible for larger audiences, there is an urgent need to focus on cooperation and establishment of fundamental rights in cyberspace as well as mechanism to establish security in this sphere.

Conclusion

Can a cyber-attack pose a serious threat to national security?

With the clear majority of undergone, ongoing and possible cyberattacks and with the current defensive strategy of the states, the cyberwar is nothing than a real threat for states' national security as well as private sector. It enflames not only regular warfare which can cause as much harm as it is assumed to have by traditional approach of the war, it may also provoke irregular warfare with the privilege of the equal information access and anonymity. The technological invention of twentieth century may considered to be a disaster along with such scientific invention as atomic energy. It may give a good, but it may harm severely.

The difficulty of cyberwar falls also on the lack of common norms and definitions as well as specifically composed legislation equally acceptable for all states for peaceful and collaborative regulations of problematic issues on this field.

I do believe that cooperation on this issue is of great importance. Joint legislation, understanding and definition of conceptual ideas, common cooperative grounds will bring to a better and secure life, eliminating or declining the possibility of occurring private or non-state organizational subjects to be involved in irregular warfare destabilizing the peaceful cooperation of states and people on internet sphere for a good and productive will. The classical approach of war definition should be able to include a new sphere of violence before a certain violence occurs rather than defining right after it occurs, as mostly happens in historical approach. Aside from the traditional military spheres like land, sea, and air (added later), an epoch of adding a new sphere, cyberspace, has begun, in which technical capabilities do no less harm than in a traditional war.

Cybersecurity is an urgent, necessary strategy, which will lead to a secure sphere for cooperation, free and secure access to and sharing of information, and, due to its technical capabilities, to a more comfortable and economically developed way of life.

While Cybersecurity is an issue for the whole world, strategies for the development of cybersecurity may vary from state to state, in some cases occurring a national level, while in

others limited to certain federal entities.

I believe that Cyberspace is very much like the environment; it is a digital environment, and just as a virus that penetrates a certain country is spread worldwide if not stopped, so is a computer virus. Just as pollution in one part of the world pollutes air or water that we all share, a cyberattack may cause a global problem. Networking, sharing information, and a global security approach are mustsfor a safe and productive global cyber environment and maintenance of all roads for better digital development for the sake of humanity.

1World Wide Web foundation "The History of the Web", available online http://webfoundation.org/about/vision/history-of-the-web/, last accessed on January 04, 2017.

22017. The official website of NATO. But we have Kurds as always. Cyberdefence. Available online http://www.nato.int/cps/en/natohq/topics_78170.htm. Last accessed on March 17, 2017.

3The White House. Archive of former president Barack Obama. Cybersecurity. Available at: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity. Last accessed on 10 August 2016.

4Izvestia, analytical online journal. "The Russian Foreign Ministry denied accusations of involvement in the cyber attack on the Pentagon, 2008, 4 Dec. Available online. Last accessed on 21. April 2017. http://izvestia.ru/news/440465

5The Official webpage of the NATO Cooperative Cyber Defense Centre of Excellence Tallinn, Estonia. About the CCD COE, available at https://ccdcoe.org/about-us.html Last accessed on 29 February 2016.

6Osnos E., Remnick D., Yaffa J. "Trump, Putin, and the New Cold War. What lay behind Russia's Interference in the 2016 election-and what lies ahead?" NewYorker, online publication, available at http://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war , last accessed in Feb, 2017.

7The White House Cybersecurity Framework event of February 12, 2014, Remarks by the Secretary of Homeland Security Jeh Johnson, The White House, Washington DC. Available at https://www.dhs.gov/news/2014/02/12/remarks-secretary-homeland-security-jeh-johnson-white-house-cybe... (accessed at August 2, 2016)

8Homeland Security News Wire. "DHS designate U.S. election infrastructure as a Critical Infrastructure Subsector". 9 Jan, 2017, Electronic Journal, available at http://www.homelandsecuritynewswire.com/dr20170109-dhs-designate-u-s-election-infrastructure-as-a-cr.... Last accessed on March 9, 2017.

9 Krutskikh, A. V, «Намудалосьдоговоритьсявусловияхконфронтацииисанкций» We succeeded in reaching agreements under conditions of confrontations and sanctions, "Komersant", 08, October, 2015, available at http://www.kommersant.ru/doc/2790234, (accessed on August , 15, 2016) July, 2017

References and Literature

1. Baylis J, Wirtz J, Gray S. C. Strategy in the Contemporary World: an Introduction to Strategic Studies/ Garnett J. The Causes of War and the Condition of Peace. Oxford University Press, 2013.
2. Demidov O., Global Internet Governance and International Security in the Field of ICT Use, "PIR Press". 2015, Moscow-Geneva,
3. Rid Th., Cyberwar and Peace; Hacking Can Reduce Real-World Violence. "Foreign Affairs", November/December 2015, p. 77-79
4. Zhang Li, A Chinese Perspective on Cyber War, "International review of the Red Cross". Volume 94, Number 886, 2012.
5. Mousavian, S.H. The Iranian Nuclear Crisis. A Memoir, Carnegie Endowment for International Peace, Washington DC, 2012.
6. Sahakyan M., The USA Policy on Iranian Nuclear Issue (2000-2014), "21st Century", No. 2 (16), 2014.
7. Limnéll J, The cyber arms race is accelerating – what are the consequences?, "The Journal of Cyber Policy", Volume 1, Number 1, 2016, pp 50-60.
8. Collins G, The Obama Administration and DHS Move to Secure the Nation's Digital Homeland, "Homeland Cybersecurity" 2012. Available at: http://www.defensemedianetwork.com/stories/homeland-cybersecurity/2/ accessed on 1 August 2016.