CYBER GLOBALIZATION AS AN IN/STABILITY FACTOR

Ilina Armencheva[1], Natalia Atanasova[2], Ivaylo Ivanov[3]

[1]Assoc. Prof. Dr. National Defense College, Sofia, Bulgaria, ilina_arm@abv.bg
[2]Prof. Ph.D., National Defense College, Sofia, Bulgaria, nataliab@abv.bg
[3]Asst. Prof. Dr., National Defense College, Sofia, Bulgaria, ivo2003@abv.bg

Abstract

While the world is becoming increasingly interdependent, the countries are evermore dependent on information systems, high-speed communications and artificial intelligence. That is increasing the risks and threats to citizens' privacy, global trade, the resilient of critical infrastructure and even the readiness of the armed forces. Traditional security measures are lagging behind new challenges and they are insufficient to prevent emerging risks.

The potential damage that these threats can inflict on security and economy grows tremendously, but countermeasures needs to be sophisticated and thus difficult for implementation. The 21st century instead to be the era of technologies and information revolutions is becoming of synonymous of global risks and uncertainty. This article explore the transformation of relations in cyberspace as a result of globalization and the development of information technologies, that create preconditions for new forms of criminal activity - cyberwar, cyber terrorism and cybercrime.

The globalization of social and political processes lead to globalization of crime, which now is transnational. Today becomes more and more obvious the need for conceptual clarity and innovative approaches in security study for cyber threats in modern society. Understanding of interconnection between globalization in cyberspace and increasing insecurity in it as a consequence of that globalization and the relation between new information technology and emerging threats coning with their use is crucial for security of our societies.

The article explore cyber security as one of the biggest challenges for today's interconnected world and how to achieve it resilient development and progress.

Keywords: cyber security, cyber globalization, stability.

1. INTRODUCTION

In the information age, all key sectors of the survival of mankind such as security, policy, management, business, finance, transport, infrastructure, post services, telecommunications, medicine and science are closely dependent on information and communication technology (ICT). This gives grounds to assert that the Internet increasingly acquires the characteristics of the "central nervous system of human society" and is

inextricably linked with people's daily lives. Striking examples of this are the social networks that can rapidly affect the values, ideas and behavior of large social groups. In practice, internet gives unlimited possibilities for distribution of various ideologies and ideas related to democratic transformations of social relations and human rights (Armencheva, Smolenov, 2015a).

The information revolution and the emerging threats set different from the current requirements for countries. In order to fulfill its functions, and particularly those related to national security, is required a construction and development of new capabilities for control and protection of information and communications from attacks by criminal gangs or by attempts to penetrate the systems of critical national information infrastructure. Moreover, individuals, guided by different motives can cause large, damage to critical infrastructure, which seriously challenge the power of institutions of large and small countries in their efforts to protect national security.

Besides great physical potential and immediate financial losses, the very threat of possible future cyberattacks impunity breeds distrust and reluctance to work with the new technologies in society, which in turn leads to negative attitudes in the public opinion and questions the reliability of electronic, financial and medical resources and services. Even the loss of confidence itself can lead to enormous social and economic disruption.

At the same time, new technologies and the Internet make different malicious impacts on critical infrastructure of individual countries (through the collection and use of confidential information related to national security and the deployment of information wars) easily accessible and create opportunities for criminal activities and attacks against both the interests of various public organizations and those of individual citizens (Zhelev, 2017a).

2. CONTEMPORARY CYBER SPACE AND GLOBAL (IN)SECURITY

Cyber space is not safer than the real world. Besides advantages that it gives in forms of virtual reality and entertainment, digital economy and market and more opportunities for citizens involvement in government decisions, cyber space has and another “dark side” – different forms of criminal activities, manipulation of public opinion and the new way of war - cyber wars.

In the era of nation-states before the emergence of the global society, power relations and political leadership were based mostly on economic and military superiority of the various entities at the national and international level. Government and international organizations have created and imposed legal and social norms and values by laws and treaties, to regulate in some extent the emerging armed conflicts. The basic principle has been linked to the inviolability of national borders and territorial integrity of the Contracting Parties. Aiming more successful realization of this principle, different countries have developed, and continue to develop various military and economic capabilities in land, air and sea domains.

The processes of globalization are completely new stage in development of human societies and that creates new dynamism in international relations. They change structure of international relation, centers of power and transform basic features of nation state. The old paradigm of ideological confrontation is not valid anymore because digital technologies create new forms of development in almost every sphere (political, economic, social and military), new habits and norms and new challenges. That enforce scholars to reanalyze the essence of globalization and it cyber space dimension or the emergence of cyber globalization. From philosophical point of view globalization is a new stage of evolution of humankind which inherited features are high- degree of self-organization and adjustability (Marinov, 2018a). Development of that evolution is a product from activities of public subjects and that makes it sort of purposeful common effort. The most prominent feature of that kind of efforts is governance. Although tools and mechanisms of the processes of cyber globalization are „details” they are important especially when it comes to ideological, political, economic and military dimensions.

Is there contradiction between the evolutional and governance aspect of cyber globalization processes? From evolutional aspect cyber globalization doesn`t fulfill the aim of creating integrated cyber space and equality between actors that operate within it. The evidence is actually opposite - the results are divisions and differentiations. From governance aspect the result is shift from universal, common to all mankind goals towards particular that serve to the interests of most powerful actors in cyberspace. At this stage of human development innovations create new global environment for interactions but in reality it is further development of classic colonialism which from economic and social after World War 2 become “technological” today. The result is that to economic and social underdevelopment of 80% of world population cyber globalization add and technological or another dividing line between rich and poor societies.

Influence of cyber globalization on politics, new geopolitical realties and interconnections between big political actors can`t be neglected. Despite that political and power relations are complex, global world is strongly influenced by rapid technological changes and determinism. The information revolution and internationalization are transforming contemporary security environment. One of the challenges that nation state faces in global cyber space is that most of things that happens in it are not under government control. Like it or not information revolution is changing the nature of power relations and make them more diffuse. Nowadays states operate in global information environment where new principals of political cooperation, competition and confrontation are established. In that environment political processes are happening in real-time, physical state borders disappear and the concept of geopolitics are changing. Nation states are still primary political actors on the world stage but their power steadily decrease so they are seeking to acquire new tools for power and influence based on access and possession of valuable or sensitive information and supremacy in information domain.

3. THE INFORMATION REVOLUTION AS FACTOR OF DESTABILIZATION

The information resolution that is happening today is based on progress in ICT and it is often called “Fourth Industrial Revolution”. It builds up on the foundation of digital revolution adding variety of technologies that creates unprecedented changes in economy, society and life of every person (Schwab, 2017b). These new technologies fuse physical, digital and biological components which create simultaneously huge opportunities and potential threats. According to expert from political planning division of US Department of States rapid proliferation of information is as dangerous as illegal traffic of weapons. The speed, scope and depth of this revolution have deep impact on world economy, policy, societies and people. Information is power and it possession is the ultimate goal that everyone want to achieve.

Data transferring speed and high performance computing technology are growing extremely fast and at the same time quantity of digital information are growing approximately tenfold in every four–five years. These two sides of the coin demonstrate the need for new approaches to govern processes in cyber space in order to guarantee it stability, security and sustainable development.

Example of innovative development are high-tech Asia countries Japan, Singapore, Thailand and China implementing their own concepts and models to govern information revolution like „Society 5.0”, “Smart Society”, „Thailand 4.0” and global project „One Belt One Road” called also “New Silk Road” important element of which is “Space Information Corridor”. In that situation many scholars conclude that new type of human skills is key for future development – creativity, innovation, self-motivation and self-management.

In his article “The Information Revolution GETS Political” Joseph Nye Jr. says that in contrast to proliferation of information that doesn`t need lots of resources, collecting and extracting new information needs considerable resources (Nye, 2013a). In competitive environment the key for information superiority is ability of collecting of raw data, processing it and extracting new information with high-speed. At the same time Stuxnet and Edward Snowden's revelations show the need of rethinking cyber security concepts that lay in strategic documents for cyber protection and security. These cases illustrate that the center of gravity have to shift from defense of critical infrastructure towards cyber espionage defense and against collecting of intelligence data operation run by corporations, various organization or nation states.

NEW FACE OF OLD THREATS IN CYBER SPACE

From data theft towards modification and change

The new tendency is cyber criminals not just to steal data but to modify it. Hacking attack statistic revels that their goal is not only data theft but to change it. Except to use their skills to penetrate information systems for profit cyber criminals aim is long term discreditation of information system security. Those kind of threats are not limited only to governments and states and can be much more global and worrisome. In the last few years famous companies were victims of cyber attacks not only for profit but to change public attitude towards them and harm their image.

Consumer devices became cyber hostage

Growing number of devices whit Internet of Things (IoT) function gives new life to old ransom business with crypto viruses. Cyber criminals have changed their approach and now they block entire accesses to devices. At first glance that is not a big problem but actually is very serious and can have devastating consequences – imagine situation in which hacker blocks air conditioning system in data center. Manufacturers, providers and consumers has to look at IoT devices security very seriously. Unfortunately in reality huge number of IoT devices are extremely vulnerable to hacking attack. Trying to match consumer demand for IoT devices and

looking only in the profits manufacturers and providers supply millions of them overlooking the question of security. The result is that most are not protected, software can`t be updated and upgraded and that makes them vulnerable for hacking attack. When IoT devices are secure they can be accepted like any other IT system that needs long term effective protection.

Artificial intelligence as a cyber weapon

Artificial intelligence (AI) gives countless opportunities for society and common digital market but it can be used for harmful activities and complex and prolonged cyber attacks (Spiegeleire, Maas, Sweijs, 2017c). So artificial intelligence is a double-edged sword – it can help to protect and defeat cyber attacks but it can be used as a tool for such attacks. The fact that artificial intelligence is becoming a cyber weapon is worrisome and at the same time underlines not only that more scientific research and developments in that field is needed but also how artificial intelligence can be applied in cyber security. The most advanced algorithms for machine learning offer reliability and protection against increasingly complex cyber threats (Russell, Norvigt, 2010a). Artificial intelligence is very effective to solve particular problems but if it is used for another purposes it can create serious problems. At the beginning AI can be employed in cyber security to eliminate human experience, intuition and judgement. But scientists are warning about consequences of further unrestricted development of AI capabilities. Very advanced AI can be used or alone to decide to act in harmful way and effective control over it uses is a challenging task if it is possible at all. Greatest disadvantage of AI is its unpredictable use (Harini, Dharani, Vidhya, 2017d) for wrong or maleficent activities but that “dark side” of it is just a reflection of the “dark side” of the human nature.

Information warfare and manipulation

With mass proliferation of web 2.0 and web 3.0 technology social networks and media are not only platforms for entertainment and business but actively participate or are used by different actors in propaganda activities, manipulation of public opinion and disseminating of fake news. The speed with fake news reach the audience and lacks of any regulation make them the newest challenge to security. According to many researches fake news spread six time faster than normal news (Zhelev, 2017e). They are few types as follow: attractive offers to earn money and traffic; disinformation or manipulation of public opinion; political party fake news that are tarnishing the party or politician image and the last one are satire and parody. Agents employed to influence public debates in internet are trolls, bloggers, vloggers and different types of hacking attacks (Dimitrov, 2018b).

Trolls are publishing contradictuary, conflicting, provoking or off-topic comments in on-line forums, blogs, news agency or papers and official institutions sites. Their goal is to shape public opinion in particular direction and to provoke emotional response to events, persons, groups of people, institutions or states. Depending on topic trolls activities can be divided to social and political. Overriding others people will and opinion and non-compliance with generally accepted moral and ethical norms are the most visible feature of their behavior. The consequences of their activities are doubt, uncertainty, confusion, lack of trust, rejection and frustration. Modern technology gives almost unprecedented potential for executing information operations in order to shape or change public opinion. The result of that is constantly increasing stream of information that individuals can`t handle and engaging them in differnet processes in which dominant feeling is sense of helplessness and lack of control.

Big Data and web 4.0

The next step of web technology development that has implications for security is web 4.0, it is based on extended or augmented reality and Big data. The latter describes extremely vast array of data that is so complex that it is impossible to be proccessing with common applications and methods (Agrawal, Bernstein, Bertino, Davidson, 2012a). Big data is one of the most perspective trends in IT. It is deeply affecting the way companies, government’s agencies and scientists analize their information resurces. Big data gives opportunities for even more strict control over information and that wil have implications not only for digital market but to reality that surround us.Collected data combined with enough computing power and right algorithms can be analaized and arranged according to logical sequence. In that process algorithms are extremely important because they can extract logic from the chaos and discover invisible and unknown links and models (Yiu, 2012b). Utilizing Big data has implications for everyone. Using right algorithms and methods organizations and governments can exploit Big data to solve different problems or take preventive measures. But here again like in other innovations there is a risk Big data to be used for malicious activities – state and corporative espionage, unauthorized obtaining of information or eavesdrop people and restricting their freedom.

4. THE IMPACT OF CIBER GLOBALIZATION ON POLITICS AND INTERNATIONAL RELATIONS

Governments have always shown concern in regard to control on information float. They clearly recognize that information revolution has led to general change in the proportion between the impact of small and large in size countries in cyberspace and has considerably increased the influence of small and non-governmental participants. Some of the researchers of the globalization processes have highly rated the tendency to see a decrease in the authority of the sovereign states and have predicted that digitalization will transform the bureaucratic hexarchy with networking ones. The virtual societies will be able to cross legal territorial borders, develop and expand their governing models, while the states will gradually decrease their leading empowering function. Cyber globalization is now irreversible process, which cannot slowdown from its current course. The process is transnational and creates all sorts for dependencies in every aspect of our lives, which is closely related to national safety. Still, we should clearly understand that freedom in virtual reality is only relative and not physically real.

The contemporary information media changes faster than the political understanding of the process, and the political reaction cannot adapt with the same speed of action to all the changes. Re(volution) and all new discoveries in the information technologies slowly destroy and transform the existing dogmas, existing behavior, mentality, paradigms, values and relationships. Humanity is at the brink of new geopolitical reality of chaos due to storm coming new ideology of the technological determinism. At the same time the leading actors on the global political arena, as they aim to gain information and financial dominance, suppress to a large extent the main rules on which the democratic societies have been based.

The current conditions create potential opportunities equally suitable for economic growth, political freedom and peace encouragement, just as well as for social segregation and direct aggression on critical infrastructure and general brutal conflicts and solical violence. The threats and the ricks for general security have grown of larger scale and increase their territory, while the consequences become much more complicated for any decent prediction. According to Henry Kissinger, the main reason for global destabilization lays with the technological factors and their development in the nearl future. It has been predicted that the technological abilities of many countries will be equalized and it is the technologies that will be the key factor in the world domination.

All of these (re)evolutionary changes often can trigger events and circumstances, leading to conflicts and following crisis. However, cyberspace, information float and contemporary technologies, being inter connected, are the best vehicles to approach personal ambitions. Global leadership, access to strategic resources are the aims in perusing information dominance.

5. THE SECRET PLAYERS IN CYBERSPACE – CHINA, USA, RUSSIA

Due to its abstract and invisible nature, in the 21-st sentry cyberspace creates new potentials for the occurrence of asymmetric, spy and propaganda war actions. Cyberspace has become a new war field of most contemporary conflicts. Most of the world's super powers create cyber power of their won and compete in building stronger cyber capacity and in their abilities to be in control at all times.

Furthermore, to the struggle for information superiority, national states are adding new spy strategies, mass manipulation, censorship and building up additional powers. While cyberspace is just a medium, cyber powers of the national states are measured by their capabilities of extracting direct advantages and they are measured by their technological advancement in general protection (offensive and defensive).

Cyber powers are multi-layer structure of activities, unique hybrid scheme of physical and virtual elements with three main advantages: they can penetrate everywhere; they support all other military fields and they can remain fully anonymous. This is why cyber powers as supplementary element are the most powerful instrument over the last 20 years; together with cyber space are the basis for new concepts and war leading doctrines.

Offensive abilities are usually within the capabilities of governments, military, security services, professional gangsters, script kiddies and hackers, while the offensive capacity involves cyber surveillance, hacking methods for system distraction, including computer worms.

Defensive abilities are being distinguished by their areas of use: governments, armed forces and security services and all the way to private trade for personal purposes. Such examples could be methods for attack prevention, response to incidents, as well as the CERT teams for reaction to computer incidents.

Nowadays a great deal of the cyber conflicts are taking action in accordance with the rules, established by

the great political players – the US and their allies and on the opposite side – China and Russia. The active domination struggle in economic, as well as in purely military aspect includes activation and organizing the entire technological and information arsenal for surveillance and cyber-attacks. During the last decade the cyber weaponry has actively began the use of conflicts between ideologies, religions and national states. There is no secret that the US and their most devoted allies have been in constant state of cyber war with enemies like Russia, China, Iran and other countries, where considerable amounts of natural wealth is available. This contradiction has been layed at the bottom of the new US defense strategy at the beginning of 2018, whereas main enemies of the US are listed China and Russia and even North Korea as a subject with rising nuclear power (2018c).

If we aim our attention to the Chinese defense strategy, it is clear that it depends more on its geo-political proximity to the two Asian allies Russia and Iran. For these countries it is vitally important to maintain their civilization structures in the era of globalization. One of the ways to achieve this aim is the creation of information or disinformation campaign, which should protect inviolability. The lack of cyber-attacks between rival countries is a sight of reaching peace and agreement. Russia, China and many of the countries of in Central Asia, as well as countries like Iran, have been coordinated in Internet through the Shanghai Cooperation Organization (SCO). Once of the global aims of SCO is counteraction to the American impact in Middle Asia.

In the scientific area Chinese and Iranian scholars have been actively cooperating in the field of digital technologies. The relations between these countries are under the impact of joined past history. They have been feeling isolated from the regional and global politics and do not approve the domination of the US. Iran has been oriented mainly to control of digital certificates, communication protection and critical infrastructure, as well as attack prevention, especially after Stuxnet.

In regard to the state politics in the field cyber security, China has adopted several rather important documents over the past coulle of years: National Cyber Security Strategy (2016), International Strategy of Cooperation on Cyberspace (2017), Cyber Security Law of the People's Republic of China (2016). In the very first for China National Cyber Security Strategy are being structured the main priorities and aims of China in regard to the development of cyber space and security. The main agenda for China is to become cyber power and at the same time encourages the organized, secured and open cyber space and defends the national sovereignty. The Cyber security Strategy looks at the concept as of “new theory of national sovereignty” and plans the future actions to achieve more effective cyber control (2016a). The analysis of the Chinese cyber strategy shows that Beijing will gain maximum advantage of cyber power used for active economic spying and intelligence against their competitors.

China has been transforming from economic super power into one of the leading factors in the world’s geopolitics not as consumer but as generator of (in) security in regional and global aspect. The Chinese government and army are believed to be accountable for some of the grandest cyber spy cases in the modern digital era. A good example would be Titan Rain – the code name of a serious of coordinated cyber-attacks against the Department of Defense of the USA and especially against NIPR Net (unclassified IP military net). Although there is no convincing evidence for the involvement of the Chinese government, it is widely believed that it has taken an active role in supporting the hackers groups, who performed the attacks.

The common grounds on building strategies on cyber security between the US and China is the concentration on cyber spying and cyber war. During the last two years the two countries have been modernizing their armies and develop their technological potential. During a possible mass attack towards any of the major global powers, the financial and technological collapse on one of the countries will be crucial on the other. And while real cyber war between them seems like rather unlikely scenario, cyber spying is now a reality. The Beijing’s efforts have been focused mostly on maintaining a wide range of capabilities on prevention, data extraction of economic and technological data, attacks on military systems and penetrating critical information structures of other independent countries. By developing their space and cyber potential, China has the ambition to compete with the US in aiming for dominance on the information arena. The serious threat comes from the specific interaction and the antagonism between the US and China and their potential conflict.

Both super powers China and the US have well developed offensive abilities as national states, war establishment and security. Publically both countries maintain their proper diplomatic relationship but in fact the competition between the two largest economies on the planet, competing for geo-political supremacy keeps growing. The trade between the two countries goes up to hundreds of billions of US Dollars each year. But the US is constantly facing the never-ending struggle with intellectual theft and counter measures against the economic intelligence of the Chinese.

The cyber capacity of the Agency of National Security and of the Cyber Command of the US became known in 2013, after the publishing of classified papers by the former INS employee Edward Snowden. One of the most striking evidence was the computer worm Stuxnet, which caused automatic destruction of the nuclear weapons of Iran in 2010.

In 2015, Russia and China sign an agreement for cyber security, which says that Russia and China agree to protect each other of cyber-attacks and together to stand against technologies that might lead to "destabilization of the international political, social and economic environment". Furthermore, both countries agreed that their legal bodies would exchange information and technologies for the guarantee of information security.

Despite the well-established position of China as most clearly recognized transnational aggressor, seems that the better equipped and smarter acting player in cyber space remains Russia. The Eurasian leader has developed over the course of years its hacker capacity and it was the reason why possible involvement of Russia in the American election is still being disputed. Russia has well developed concept for leading information wars, which include counter intelligence, disinformation, electronic wars, weakling of communications, disturbance in navigation and destruction of information systems.

One of the strongest sides of the Russian security policies is the wide of defensive systems, by which is guaranteed the critical infrastructure. Russia is rather cautious in regard to attacks on information systems and production infrastructure. This becomes clear by the fact that in Russia only five percent of all systems for control and data extraction SCADA (By the author - SCADA systems are an aggregation of programmes and technical means, which give the possibility for local or remote control of parameters of atomized technological processes in a variety of businesses. They allow complex monitoring, data collection in real time and file records as logs) are accessible online and the other part are fully isolated, while in the US, UK and South Korea, as well as other developed countries, these systems are connected online, which inevitably increases the potential risks.

Russia is getting closer and closer to the American capacity and capabilities. The Russian government has been regarded as number one in using complicated malware and fishing techniques (identity theft). The Russian experts have been regarded as producers of some of the most modern cyber weapons and have created some of the most memorable attacks during the last years: The Red October and it satellite software Sputnik and the crypto virus Not Petya; the harmful software Crash Overdrive, which can sabotage electrical systems; the new spoofing cyber weapon against GPS navigations, the harmful software StalinScreamer, which blocks all functions of an operation system and so on.

According to an American investigation report, China and Russia are amongst most active states, using the means of cyber spying for the sake of reaching intellectual property, commercial, technological and classified military information from American companies. The US, on their own account, uses cyber-attacks in order to achieve specific results for military and other purposes.

6. ESTABLISHING PEACE AND STABILITY IN CYBERSPACE

The newly established threats for the international security and stability, based on cyber armor, require the implementation of new effective actions for control and counter measures. The invention of such measures contradicts with some conceptual problems. Such example is the lack international consensus on defining what would be called cyber weapon, cyber conflict and cyber war. These problems are up to the expertise of various experts in the field of international relations and demands long and rather complicated negotiations. These would be the first steps towards the decrease of treats of conflicts or war in this rather sensitive area of the human relations (Armencheva, Smolenov, 2015b).

In such context we should be seeking all possibilities for the creation of international regulations in regard to cyber conflicts with the mutual agreement on all issues from the international community, which should adapt according rules and sanctions.

These regulations should include quite a number of responsibilities on behalf of all countries that include the control of various non-governmental organizations and their networks. The establishment of such regulations could be based on the proven experience of countries in the area of counteraction against attacks on their critical information infrastructure. Currently in many countries their legal frame has been changed, expanding with specific texts on cyber-crime.

The next possible steps towards effective regulation on possible cyber conflicts is reaching widely accepted agreement of creating a necessary level of security, based on minimum required communications. Adopting

all necessary legal frames would avoid unnecessary destruction and suffering of people involved and would be used as guarantee of protection to those, who are not part of the conflict.

The effective regulation of rising and existing cyber conflicts should also be addressed to the aggressive actions, taken on private initiative, such as terrorist attacks. In such case, the general difficulty is with identifying the perpetrators, who should get the according sanctions.

If the attack has been committed on a territory of a country, which was harmed, the sanctions could be taken from the good practices of the international humanitarian law (IHL). In such cases, when illegal actions were taken and IHL has been violated, the perpetrators can be sanctioned accordingly with the existing legal frame of the country on which territory the case has occurred.

In the specific case of cyber-attack, committed by another neutral country, the offenders could be deported to the country, which was under attack or be held legally responsible in the country, where the crime was committed. Naturally, the choice of action depends on creating balance in the relation of objective desire of the international community ot deal with such crimes and the existence of the necessary legal frame, as well as creating zero tolerance in the international community towards terrorist actions in the information space.

Truly effective international legal system, related to conflict management in cyber space is seriously challenged by the fact that most developed countries have no common understanding of the bases of cyber-crime as such and which action and what particular cyber behavior could be classified as cyber-crime.

Naturally, there are other subjective reasons, which complicate international cooperation in the disclosure of cyber-crimes or generally speaking – crimes, committed in cyber space. In order to harmonize various opinions, in 2001 the Council of Europe created the Convention of Cybercrime, which aim was to become the ground for an international law on cybercrime. By the end of 2018 it has been ratified by 62 states. It is worth mentioning that the Convention on cybercrime of the Council of Europe does not provide a general definition of cybercrime, which further complicates actions against such occurrences.

One of the rather serious issues is that there are no international agreements in regard to the rules on development, distribution and use of cyber weapons. The lack of agreements extends to legal frames, regarding harmful software for military purposes. There is no legal frame also in restricting investigative agencies or how military will invest and lead cyber weapons testing.

Recently, the International Telecommunication Union (ITU) formulated five principles that would ensure peace and stability in cyberspace. They establish specific actions and obligations and have the following idea:

Each government should provide its citizens with access to communications;

Each government is committed to protect citizens in cyberspace;

Each country should undertake the obligation to ban the hiding on their territory of cyber terrorists / criminals;

Each country undertake the obligation not to be the first to make the cyber attack against other countries;

Each country should cooperate with other countries in the framework of international cooperation for peace in cyberspace.

Together with the Union, the World Organization of Scientists also engages in discussion and supplementing the above list of universal UN principles. As a result of this activity, in 2009, the principles of cyber peace are described in a brief statement in which is stressed that ICT can be a tool for the benefit of people and building a cyber peace as well as a powerful tool for creating conflicts. These principles read as follows (2009a):

All governments should recognize that international law guarantees people free access to information and ideas and these guarantees also apply to cyberspace. Restrictions should only be imposed as necessary and accompanying measure in order to provide legal expertise;

All countries should cooperate in order to create a common code of conduct in cyberspace and harmonize the legal framework worldwide (incl. rules of procedure for assistance and cooperation in the investigation, but operating under privacy and human rights). All governments, service providers and users, should support international efforts to ensure the rule of law in the field of cybercrime;

All users, service providers and governments should support their efforts to ensure the privacy of users in cyberspace;

Governments, organizations and the private sector, including the citizens themselves should implement and maintain comprehensive security programs based on best practices and standards in the use of IT to ensure privacy and security;

People that make software and hardware should strive to develop secure technologies resistant to vulnerabilities that allow a recovery to a sustainable state;

Governments should actively participate in the UN programs to ensure global cyber security, cyber peace and prevention from conflicts in cyberspace.

These principles and particularly the latter, require the commitment of governments not to use the potential of IT for conflicts in cyberspace.

As an extension of the initiatives concerning cyber peace, in 2011 was published the book “In Search for cyber peace” (2011a). It offers a broad understanding of cyber peace as a founding principle of the creation of a universal order in cyberspace. The next year a new initiative is proposed by the UN – “Sustainable Peace for a Sustainable Future". Its aim is to promote the understanding that sustainable peace can be built and maintained only on the basis of sustainable development (Casciano, 2005a; Clarke, 2010b; 2006a; 2010c; Elliot, 2010d; Kaspersky, 2015c; Kausch, 2017f; Nye, 2013b; Perkovich, Levite, 2017g; Slatinski, 2014a; Spiegeleire, Maas, Sweijs, 2017h; Hildreth, 2001a; 2010e; 1999a; Petkov, 2018n; Terziev, Petkov, Krastev, 2018d-m; Terziev, Stefanov, Banabakova, 2018o-p; Stefanov, Terziev, Banabakova, 2018q-r)

7. CONCLUSION

Cyber space creates new context and challenges that define relations between global powers like US, Russia and China. Using their political and economic weight they can dictate trends and norms in contemporary cyber space. The era of global communications creates new form of interconnections between those powers in which they are simultaneously strategic partners and rivals. Confrontation between them is already reality and they are waging a war virtually with new kind of weapons – cyber weapons. In that context, with growing insecurity in cyber space, all countries and alliances should rethink their policies and make an effort towards building common alert system and security measures against cyber threats in order to decrease volatility and guarantee peace and stability in cyber space.

The future geopolitical posture will be defined in parts on the influence that each country has in cyber space. The most powerful players will be states and other actors with best intellectual and technological capabilities in ICT.

REFERENCE LIST

Armencheva, I., Smolenov, S. (2015a). From Real Cyber Conflict through Wishful Cyber Security to (un) Likely Cyber Peace, Revista Academiei Fortelor Terestre NR. 3 (79) /2015, p. 260, 2015.

Zhelev, Z. (2017a). Dezinformaciata v savremennite konflikti, Voenna academia, br.1, s. 113-118, 2017.

Marinov, G. (2018a). Globalization as a geopolitics for global domination. https://geopolitica.eu/spisanie-geopolitika/170-2018/broy-4-2018/2871-globalizatsiyata-kato-geopolitika-za-globalna-dominatsiya.

Schwab, K. (2017b). The Fourth Industrial Revolution, Crown Publishing Group.

Nye, J. (2013a) The Information Revolution Gets Political, https://www.project-syndicate.org/commentary/information-t nology-s-political-implications-by-joseph-s-nye.

Spiegeleire, S., Maas, M., Sweijs, T. (2017c). Artificial Intelligence and the Future of Defense, The Hague Centre for Strategic Studies (HCSS), ISBN/EAN: 978-94-92102-54-6, 2017.

Russell, S., Norvigt, P. (2010a). Artificial Intelligence: A Modern Approach, Third Edition, 2010.

Harini M Rajan, Dharani S, Vidhya Sagar. (2017d). Artificial Intelligence in Cyber Security – an Investigation, International Research Journal of Computer Science (IRJCS) ISSN: 2393-9842, Issue 09, Volume 4, 2017.

Zhelev, Z. (2017e). Informatzionni operacii I informatzionno vazdeystvie, Voenna akademia, s.53-58, 2017.

Dimitrov, D. (2018b). Operatcii za vliyanie: mehanizam na deiystvie i protivodeystvie, sp. "Voenen jurnal", br.2, s.46-63, 2018.

Agrawal, D., Bernstein, P., Bertino, E., Davidson, S. (2012a), Challenges and Opportunities with Big Data: A white paper prepared for the Computing Community Consortium committee of the Computing Research Association, 2012, http://cra.org/ccc/resources/ccc-led-whitepapers/.

Yiu, Chris. (2012b). The Big Data, Opportunity Making government faster, smarter and more personal, Policy Exchange Clutha House, London, 2012.

Summary of the National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge. (2018c). https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

China's National Cybersecurity Strategy, (2016a). https://ccdcoe.org/cyber-security-strategy-documents.html.

Armencheva, I., Smolenov, S.(2015b). From Real Cyber Conflict through Wishful Cyber Security to (un) Likely Cyber Peace, Revista Academiei Fortelor Terestre NR. 3 (79)/2015, pp 262-263.

World Federation of Scientist. (2009a). The Quest for Cyber Peace, Erice Declaration on Principlec for Stability and Cyber Peace, https://itu-ilibrary.org/science-and-technology/the-quest-for-cyber-peace_pub.

Mezhdunarodnii soyuz elektrosvyazi i Vsemirnaya federatsiya uchenykh, (2011a), V poiskakh kibermira, http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF- R.pdf.

Casciano, John. (2005a). Threat Considerations and the Law of Armed Conflict, 2015.

Clarke, Richard. (2010b), Cyber War, Harper Collins, 2010.

Congressional Research Service (CRS) Report, RL31787, (2006a), Information Operations, Electronic Warfare and Cyberwar, 2006, http://www.fas.org/irp/crs/RL31787.pdf.

Economist. (2010c). Cyberwar: War in the Fifth Domain, available at http://www.economist.com/node/16481504?story_id=16481504&source=features_box1.

Elliot, S. (2010d). Analysis on Defense and Cyberwars, Infosec Island, https://infosecisland.com/blogview/5160-Analysis-on-Defense-and-Cyber-Warfare.html.

Kaspersky, Eugene. (2015c). Flame, kotoroy izmenil mir", http://eugene.kaspersky.ru/2012/06/14/flame-that-changed-the-world.

Kausch, Kristina. (2017f), Cheap Havoc: How Cyber-Geopolitics Will Destabilize the Middle East, German Marshall Fund, http://www.gmfus.org/.

Nye, J. (2013b). Is the Information Revolution Transforming Power?, https://www.weforum.org/agenda/2013/02/is-the-information-revolution-transforming-power.

Perkovich, G., Levite, A. (2017g). Understanding Cyber Conflict, 2017, ISBN: 9781626164970.

Slatinski, N. (2014a). Sigurnostta - zhivotat na mrezhata, Voenno izdatelstvo, 2014.

Spiegeleire, S., Maas, M., Sweijs, T., (2017h). Artificial Intelligence and the Future of Defense, The Hague Centre for Strategic Studies (HCSS), 2017, ISBN/EAN: 978-94-92102-54-6.

Stephen, A. Hildreth, (2001a), Cyberwarfare, Congressional Research Service Report, https://fas.org/sgp/crs/intel/RL30735.pdf.

UN Chief proposes int'l accord to prevent cyber war. (2010e). http://www.thepoc.net/breakingnews/world/3930-un-chief-proposes-intl-a.

United Nations, General Assembly, Resolution 53/243, (1999a). Declaration and Programme of Action on a Culture of Peace, 1999.

Terziev, V., Petkov, M., Krastev, D. (2018d). Operative mode for police cooperation between the member states of the European Union. // Proceedings of SOCIOINT 2018- 5th International Conference on Education, Social Sciences and Humanities, 2-4 July 2018- Dubai, U.A.E, International Organization Center of Academic Research, www.ocerints.org, pp.473-476, ISBN: 978-605-82433-3-0.

Terziev, V., Petkov, M., Krastev, D. (2018e). European arrest warrant: appearance and preferences for

fulfillment. // Proceedings of SOCIOINT 2018- 5th International Conference on Education, Social Sciences and Humanities, 2-4 July 2018- Dubai, U.A.E, International Organization Center of Academic Research, www.ocerints.org, pp. 477-481, ISBN: 978-605-82433-3-0.

Terziev, V., Petkov, M., Krastev, D. (2018f). Eurojust casework on mafia-type criminal organisations. // Proceedings of SOCIOINT 2018- 5th International Conference on Education, Social Sciences and Humanities, 2-4 July 2018- Dubai, U.A.E, International Organization Center of Academic Research, www.ocerints.org, pp.487-491, ISBN: 978-605-82433-3-0.

Terziev, V., Petkov, M., Krastev, D. (2018g). Concept of joint investigation teams. // Proceedings of SOCIOINT 2018- 5th International Conference on Education, Social Sciences and Humanities, 2-4 July 2018- Dubai, U.A.E, International Organization Center of Academic Research, www.ocerints.org, pp.492-496, ISBN: 978-605-82433-3-0.

Terziev, V., Petkov, M., Krastev, D. (2018h). European arrest warrant and human rights of the accused. // Proceedings of SOCIOINT 2018- 5th International Conference on Education, Social Sciences and Humanities, 2-4 July 2018- Dubai, U.A.E, International Organization Center of Academic Research, www.ocerints.org, pp.501-504, ISBN: 978-605-82433-3-0.

Terziev, V., Petkov, M., Krastev, D. (2018i). Pumps for the action on the European Union in the scope of the European agenda on security. // Proceedings of SOCIOINT 2018- 5th International Conference on Education, Social Sciences and Humanities, 2-4 July 2018- Dubai, U.A.E, International Organization Center of Academic Research, www.ocerints.org, pp.497- 500, ISBN: 978-605-82433-3-0.

Terziev, V., Petkov, M., Krastev, D. (2018j). The process of forming a criminal policy of the European Union. // Proceedings of SOCIOINT 2018- 5th International Conference on Education, Social Sciences and Humanities, 2-4 July 2018- Dubai, U.A.E, International Organization Center of Academic Research, www.ocerints.org, pp.505-510, ISBN: 978-605-82433-3-0.

Terziev, V., Petkov, M., Krastev, D. (2018k). Organization on the European Union in the sphere of penal preparation. // Proceedings of SOCIOINT 2018- 5th International Conference on Education, Social Sciences and Humanities, 2-4 July 2018- Dubai, U.A.E, International Organization Center of Academic Research, www.ocerints.org, pp.482-486, ISBN: 978-605-82433-3-0.

Terziev, V., Petkov, M., Krastev, D. (2018l). Sources of European Union law. // Proceedings of SOCIOINT 2018- 5th International Conference on Education, Social Sciences and Humanities, 2-4 July 2018- Dubai, U.A.E, International Organization Center of Academic Research, www.ocerints.org, pp.511-516, ISBN: 978-605-82433-3-0.

Terziev, V., Petkov, M., Krastev, D. (2018m). The „Source of law“ category. // Proceedings of SOCIOINT 2018- 5th International Conference on Education, Social Sciences and Humanities, 2-4 July 2018- Dubai, U.A.E, International Organization Center of Academic Research, www.ocerints.org, pp.517-521, ISBN: 978-605-82433-3-0.

Petkov, Marin. (2018n). The national security system. // XIX International Scientific Conference Knowledge in practice (14 - 16 december, 2018, Bansko, Bulgaria), International journal scientific papers, IKM – Skopje, Macedonia, 28, 2018, 6, pp. 1849-1854, ISSN 1857- 923X (for e-version), ISSN 2545 – 4439 (for printed version).

Terziev, V., Stefanov, S., Banabakova, V. (2018o). Common european security and defence policy. // ADVED 2018- 4th International Conference on Advances in Education and Social Sciences Abstracts & Proceedings, 15-17 October 2018- Istanbul, Turkey, International Organization Center of Academic Research, www.ocerints.org, Istanbul, Turkey, 2018, pp. 132-148, ISBN: 978-605-82433-4-7.

Terziev, V., Stefanov, S., Banabakova, V. (2018p). Implementattion of the common european security and defence policy in the context of its military aspect. // ADVED 2018- 4th International Conference on Advances in Education and Social Sciences Abstracts & Proceedings, 15-17 October 2018- Istanbul, Turkey, International Organization Center of Academic Research, www.ocerints.org, Istanbul, Turkey, 2018, pp. 120-131, ISBN: 978-605-82433-4-7.

Stefanov, S., Terziev, V., Banabakova, V. (2018q). Levels of security and postmodern society. // ADVED 2018- 4th International Conference on Advances in Education and Social Sciences Abstracts & Proceedings, 15-17 October 2018- Istanbul, Turkey, International Organization Center of Academic Research, www.ocerints.org, Istanbul, Turkey, 2018, pp. 111-119, ISBN: 978-605-82433-4-7.

Stefanov, S., Terziev, V., Banabakova, V. (2018r). The undertsanding of security in the postmodern society. // ADVED 2018- 4th International Conference on Advances in Education and Social Sciences Abstracts & Proceedings, 15-17 October 2018- Istanbul, Turkey, International Organization Center of Academic Research, www.ocerints.org, Istanbul, Turkey, 2018, pp. 93-102, ISBN: 978-605-82433-4-7.