Computer Science and Information Technology 6(1): 11-20, 2018 http://www.hrpub.org
DOI: 10.13189/csit.2018.060102

Cyberconflicts as a Threat for the Modern State

Marek Górka

Faculty of Humanistic, the Koszalin University of Technology, Poland

Copyright©2018 by authors, all rights reserved. Authors agree that this article remains permanently open access under the terms of the Creative Commons Attribution License 4.0 International License

Abstract The Internet quite naturally is becoming a 'new battlefield' or 'offers a new dimension' (the fifth to the: land, sea, air, and stratosphere) to the conflict. Cyberwar is another way of being in conflict in the long history of military technology, which forces new tactical and operational concepts. Global awareness of cyberwar has risen considerably in the last few years and many national states are preparing for defence and offensive operations. In fact, cyberwar is a part of the evolution of conventional war, which, on the other hand is related to the changes in the social, political and mainly technological sphere. What is being stressed is the need to examine the ethical implications, which lead to further questions and doubts whether the use of the techniques of cyber war may result in shorter and less bloody and consequently more 'ethical' conflicts? Cyber-attack doesn't need to kill anyone or cause material loses, but it is still considered dangerous.

Keywords Cyberwar, Cyberspace, Cyberterrorism, Hacking (Computer Security), Computer Hackers

1. Introduction

Cyberwar, cyberterrorism, cyberattacks are very popular concepts in public debate. Despite their key significance for the security of the state and its citizens, they still leave much opportunity for research and analysis. Many events with international significance prove very clearly that the phenomenon of conflict hybridization - with the use of IT technologies - will remain a permanent way of managing foreign affairs.

The aforementioned phenomena are an opportunity for scientific considerations. The purpose of the article is to reflect upon key issues concerning cyber-security. The scientific analysis will allow to explain and determine the meaning of the aforementioned phenomena, whose functioning will be demonstrated basing on the events occurring in international politics. This paper also attempts to indicate the difference between traditional and modern warfare. It is therefore worth to consider whether a new phenomenon of military conflict is emerging now? Will future wars be fought without any spilling of blood?

An important challenge for modern political sciences is to understand (to the best possible extent), the core of information warfare, and also to develop methods of defence against the aggression that democratic societies and institutions are particularly prone to.

Within the last few years cyberwar has been universally recognised – next to terrorism – as one of the greatest military threats [1, 2]. It is also surprising how quickly cyberconflicts managed to dominate global security policy discourse.

Information revolution assumes the existence of cyberwar where neither the quantity nor the mobility of the army decides about the outcome of the conflict; instead the party who has more ability of manipulating the information will have a definite advantage [3].

Nowadays, the modern state is more than ever dependent on the internet communication. National security and economic stability depend on the flow of information where technology is the main tool. However, even the most advanced technology becomes useless in case of hardware or software failure, which very often is the result of the activity of hackers, cyber criminals or cyber terrorists. The existing aspects of conventional war like time or distance lose their importance.

Cyberwar is a notion that redefines the formula of military conflicts and puts them in the context of the disturbances in information systems. The contemporary world is so immersed in technology that actions in the cyberspace have become inextricably linked to the everyday business, education, administration and military operations. Online activities influence the real world activities and *vice versa*. Thus, it is impossible to separate the real world activities from the virtual ones and cyberwar has become deeply embedded in the contemporary military practices.

Cyberwar can be defined as the activities carried out by the States and non-State entities to penetrate computers or networks with the use of cybernetic weapons in order to destroy, falsify or destroy data or systems. It may also refer to acts of espionage crime and economic war and includes activities supporting military operations on tactical and operational levels of war as well as independent activities to achieve strategic effects.

In the 21st century almost everything is prone to cyberattack. Sudden, unpredictable and obviously adverse events in the banks or financial exchanges stir the financial sector of many countries; the electric failure may cripple or even close the whole city. The long term consequences of a cyber-attack may be even worse than momentary inconvenience. A cyber-attack on a hospital may lead to a crisis where doctors will have to work in the darkness or to the failure of machines responsible for supporting the patients' lives. If the hackers distract the mechanism of the nuclear facilities, they may cause a catastrophe on a global scale.

This makes us ask a question about the threat the cyberwar poses; whether it is limited only to such activities as espionage or sabotage, or maybe it goes beyond single episodes? Global awareness of cyberwar has risen considerably in the last few years and many national states are preparing for defence and offensive operations. In fact, cyberwar is a part of the evolution of conventional war, which, on the other hand is related to the changes in the social, political and mainly technological sphere. What is being stressed is the need to examine the ethical implications, which lead to further questions and doubts whether the use of the techniques of cyber war may result in shorter and less bloody and consequently more "ethical" conflicts? Cyber-attack doesn't need to kill anyone or cause material loses to be still considered dangerous. Summing up, cyber actions force enemies to certain activities and consequently the boundary between war and peace begins to blur.

Poor understanding of the dangers or insufficient knowledge of "cyberanxiety" may have adverse effects. On the one hand individuals and organizations may not be willing to use innovative technology in fear of a cyberattack; on the other hand they may get involved in risky actions, which may lead to a catastrophe [4].

Cyber terrorism and cybercrime are the most frequent threats for national security. As in the case of analysing classical criminal groups and terrorist organisations the basic difference between these categories is motivation (financial as far as the criminal groups and political/ideological in case of criminal organisations).

Cybercrime is usually defined as all illegal activities with the use of information technology, whose aim is to get rich. The most popular types of cybercrime are: stealing personal data, fraud, skimming credit cards, phishing (phishing for sensitive data in order to make commercial and financial operations on behalf of the persons from whom such data is defrauded), dissemination, distributing and promotion of child pornography, software piracy and illegal marketing of intellectual property and software [5].

Cyberterrorism is defined (in a simplified version) as a combination of terrorist activities with the use of IT technology. The distinguishing feature is the use of IT tools to carry out attacks bearing the hallmarks of the terrorist attacks. The most prone to the cyberterrorist attacks is the critical infrastructure of the States based largely on information and communication systems, which can directly lead to dangerous situations such as airline disaster or network failures [6].

Hacking can be described as an activity done to verify one's abilities; however, it may be used by crime and terrorist groups. Hacktivism with political intentions is different from cyber terrorism. The activity of hackers is directed at getting and disclosing sensitive data, often to ridicule their ideological opponents [7, 8].

2. Technology as a Cyber-weapon

Cyberwarfare could in fact be the tool that allows weaker nations to offset America's military might, compromising major defense systems by altering target information, changing surveillance data, corrupting intricate unit deployment schedules, falsifying readiness conditions and misdirecting key personnel. Since military logistics are increasingly designed to deliver enough support, just in time" rather than pushing mountains of equipment and supplies forward, the sabotage of software that changes priorities, destinations and timelines could halt or paralyze military operations [9].

Modern technological development has contributed to a situation where the borders between the countries are losing on their significance and the same applies to descriptive categories related to warfare. Modern conflicts have little in common with declaring war and signing a peace treaty. It is therefore difficult to say without doubt whether we are living in the times of peace or in the times of war? The borders between the countries and the lines separating the virtual and the real world are losing in their significance. Developing technology has resulted in the fact that most of the military tasks are assigned by people to robots. In such circumstances, it is also difficult to say what the borderlines of the responsibility for attacking the opponent are.

Besides, the scientific and technological progress raises certain doubts as to the level of applying force. Is launching a rocket worth several thousand dollars against a group of terrorists hidden in a tent worth a couple of dollar an adequate reaction? Therefore, which methods must be used that with prove to be effective against the terrorists? The borderlines have become blurry, as the cyber terrorists, theoretically, are able to carry out their attack from any place in the world. Besides, liquidating or dispersing or separating terrorist groups does not give any result, because such organisations, using the Internet, are able to mobilise and recreate their structures very quickly.

In the war with terrorism, the entire world is the battlefield. The reason for such state of affairs is the fact that the terrorists come from many countries and continents, and do not represent the politics of any country, they may also reside in any region of the world, and countries and institutions that are fighting against them are only responsible for their attacks. So, who is the terrorist in the cyberspace?

Every country in the world is still looking for new strategies that will protect national security. Hundreds of years ago, cannons were the pinnacle of technological development. Then there appeared better rifles, tanks, vessels and planes carrying missiles. Nowadays national security tools seem to come straight out of science fiction. The American army is at the forefront in the development of cybertools which will help to maintain the security of the troops and provide a tactical advantage over the enemy. New technologies offer the precision of an unknown scale in the previous decade.

The most sophisticated computer networks in the world are endangered. The Department of Defense repels tens, and sometimes hundreds of cyberattacks per day. Despite the rate of cyber-attacks –there is no consensus as to where and when a cyberattack becomes an official cyberwar.

Collection of information with the use of long-range electronic signals, geolocation, sensors, lasers and other technologies have long been a part of the collection of information. Thanks to these tools, many countries can avoid sending people to dangerous regions in order to collect information, for example drones now work without a person on board. Advances in technology will continue to accelerate, and cyber-technology and its increased use is quickly going to become the norm. The technological progress can be used as an effective way to reduce the number of victims, but it increases the dependence of her defences on it and creates an asymmetric gap.

The hypothesis that there is a possibility of causing a conflict with the help of a computer and the Internet seems to be extremely attractive, because there are several factors involved. Information has both a cognitive dimension and the dimension of beliefs- accreditation. First, however, as a preliminary condition of manipulation, it has to skillfully attract attention [10].

Today, almost everybody was at least once subjected to a cyberattack, often a relatively mild form of malicious attack on software. Even if there has been only a minor damage (it takes a few hours to find a solution for this failure), each person has a feeling that the enemy forces attack and disrupt the functioning of the device. And even though, for one person it was only a couple of hours lost; the fact is that this was irritating. But in the case of larger global attacks such a paralysis can have dramatic consequences for the services provided by the countries and international organizations. So it is understandable that cyber security is an important issue and involves a huge budget for each country. You can also imagine the chaos in the population that is dependent on electronic network

The term cyberwars is spreading through the media, which associate this concept with economic espionage, sabotage it or even cyber terrorism. Every four months, on average media inform about some cyberattacks on the Western information systems. On such an occasion, it is often said that they come from Russia or China and they are severe enough to cause diplomatic problems.

The Internet quite naturally is becoming a "new battlefield" or "offers a new dimension" (the fifth to the: land, sea, air, and stratosphere) to the conflict. Terrorists use the Internet to express themselves, as well as to promote their own ideas, or to instruct their specific-supporters. Obviously, such websites are also an important source of information for all the departments and institutions to fight against terrorism

Scientists have long sought to understand the permanence and universality of international conflicts [11]. They have a theory that wars arise from imbalances of declining empires, nations, ethnic or religious antipathy and even attempts to divert attention from local or internal problems [12,13]. There seems to arise a question whether the technology really means a new era of conflict in the world? One should also consider whether the existing causes of wars are analogous and similar to the possible causes of cyberwars? It seems that almost any war is possible when the environment is convinced about the great benefits from the start of the attack.

Every innovation in the armaments industry affects not only the fate of the war, but of the whole world as well. This is best illustrated by an example of an extremely light and durable AK-47, which contributed to reverse the fate of wars in the 20th century. The assault rifle proved to be a weapon so deadly and so simple to use and reliable, that every able-bodied person could take to the fight.

Cyberwar is another way of being in conflict in the long history of military technology, which forces new tactical and operational concepts. It is a serious threat, partly due to the easy access to armament-computers, even very small, can be purchased and connected to the network and cause great damage. Unfortunately, in some cases the users may not even be aware that they are one of the hundreds or thousands of elements that make up the attack

When David Ronfeldt introduced the concept of cyberwar more than 20 years ago, many professionals defined this phenomenon primarily in terms of acquiring some knowledge about their opponent. Today, the armed forces grow stronger depending on the safe, the current flows of vast amounts of information, the disturbance of which can quickly have a crippling impact on their ability to fight; the enemy forces will not be able to control their units and to monitor their status and position, and thus will not be able to continue the battle or to lead the campaign. So, in the future the military offensive that will cause such interference can be sure of quick victories similarly to the success of German troops in the early years of using the Blitzkrieg tactics.

In the literature of the subject cyberattacks are seen in the same light as special operations, as well as tools that are able to solve international crisis or at least temporarily lead to disarmament without the need for a declaration of war. For example, a computer virus Stuxnet and the attack on Iranian uranium enrichment processes may temporarily slow down Tehran's efforts in the production of atomic weapons.

Cyberattacks may be mean conscription prior to the conflict, or may be used to keep two conflicted parties ready to open conflict; a good example may be the operation "Allied Force" in Kosovo, in 1999. The Serbian hackers broke into the NATO in the retaliation for the military action taken in their country. The result of this provocation was the decision about the implementation of the programme of cyber defence and an attempt to improve the reaction network taken at the Prague Summit in 2002 [14].

Estonia experienced what a great threat may such an attack constitute, where on April 27, 2007 the government servers, web sites, web services, banks, some Internet service providers and telecommunications services were totally paralyzed by a fully coordinated, previously prepared, coming from outside attacks on the network at the same time threatening the security of the state. It was a response to the decision of the authorities to transfer of the monument commemorating the Red Army soldiers. Today, we know that the initiator of the action was the Russian group "Ours" cooperating with Moscow [15].

Sceptics of cyber offensive activities indicate some limitations in conducting this type of conflict. They claim that such attacks striking civilian infrastructure do not contribute to the more effective fight of the army. They are generally willing to admit that the temporary energy or oil cut is not likely to break the people's will to fight and resist the enemy. There is a lot of historical evidence of huge public resistance after numerous bombardments. Nevertheless, there will still be war campaigns, with the aim of disturbing the flow of information, the operation of the infrastructure (including water and power stations) and their control. However, cyberattacks can cause the escalation of more deadly forms of war.

There are also doubts about the response to cyberattacks. What should be done if the cyber aggressor is one of the main or dominant states in possession of nuclear-weapon and has a wide range of ready-made actions? And what if the attacker is a team of hackers?

The cyber-attacks in Estonia, Georgia and Iran that shattered the public opinion prove that more and more often such conflicts will be used by different countries to solve their problems. Many governments unofficially admit that cyber war is very practical in crisis situations. Will this mean shorter and less bloody-wars?

Due to the unpredictable nature of cyberwar and events related to it at the beginning there may appear acts of hacking activities or financial cybercrime. One should be aware that such actions can quickly motivate and escalate into something much more serious and can endanger the national security. Modern technology is becoming more and more indispensible part of everyday life. The popular use of website information and communication serves as a factor of economic innovation but it is also a source of asymmetric division of the world.

3. Future Conflicts

Over the past decade, information technologies have been used to improve the functioning of governments, increase military effectiveness, develop new commercial services, increase productivity and produce goods and services of superior quality. Yet, along with these benefits, reliance upon these technologies has created new vulnerabilities. If they permit efficient national and global monitoring and control of critical infrastructures, they also multiply the points of entry through which hostile parties – be they anarchist "hackers", transnational terrorists, or hostile states – can attack them. Moreover, "cyberattacks" circumvent many of the logistical challenges of traditional armed conflict: computer viruses like the, I Love You" and "Mother's Day" strains that infected millions of computers world-wide in early 2000 require no airlift or sealift capability [16].

In the context of the numerous applications of the Internet and of the new technologies, the military conflicts in the nearest future will contain or already contain a permanent "cyber" element. The threats originating from the use of the Internet in everyday life may prove catastrophic both for the people and for business entities or governmental institutions. This applies to personal data protection of to personal privacy. Another manifestation of this is certain activities in the area of industrial espionage, which may be directed against nations, corporations, universities or other organisations.

A key challenge for national security is cyber-attacks that may be directed against the critical infrastructure. They may also intentionally block computers and Internet networks used in highly sensitive places such as hospital, public transport or air transport. Events of that type may also be an element of cyber terrorism.

All of the phenomena listed above, combined with military actions that aim at gaining advantage on the battlefield or increasing own military power may be called cyber warfare. What links cyber terrorism and cyber-warfare is the willingness to make the opponent suffer real damage.

Undoubtedly, there can be observed a gradual process of departing from the conventional way of conducting the war. Are cyber threats the side effects the technical progress and development?

Terrorism will continue to be a threat and it will become even more problematic when knowledge and skills become commonplace for extremists, who will use the weak points of the state The key problem is that technology increasingly dominates both in the economy and in society, and this dominance is the ultimate foundation of cyberwar.

The disruption of computer systems can cause tremendous damage; there are some spheres where the communication system between the central government and the local authorities is very complicated and complex, and thus the consequences in case of an attack or some crisis may be much bigger. The same is true the flow of sensitive information where the administration, economy and business meet. The data security system seems to be really weak and thus is much more vulnerable to disruption. A lot of our home appliances e.g. lighting, elevators, fire alarms use new technologies [17].

Cyberwar opens a wide range of instruments of coercion and destruction of information potential and the infrastructure. In the cyber world the fight takes place through action that can come from anywhere and can reach any point in the world, which clearly surpasses the traditional war actions. Although digital technology plays a significant role in contemporary armed conflicts, it should be emphasized that intelligence and electronic information war is not able to completely replace people.

No one moves the big battalions here and strategic location has no meaning. The fight moves from one address to another, not from the province to the province or from the centre to the periphery. The power is not measured by the number of missile warheads, but by millions of infected computers. Even espionage today is to a large extent based on information technology, which is to prevent access of foreign information services and ensure secrecy and confidentiality.

In a conventional conflict, everything happens according to established and well-known principles, and thus is predictable. The army or the missile moves from one point to another to conquer or destroy the enemy. The strategy is, therefore, thought through lie in the game of chess. The winner is the one who will lead his troops to the right place and on time, and the loser is the one who realizes that all this is done at his expense.

Cyberwar gives the advantage to the attacker, it forces you to think in terms of defensive position, yet the effects are difficult to predict. There is also a problem who should we turn to with a message or to negotiate when the other party is not known? In the traditional conflict the threats, moves, initiatives and responses were somehow predictable; there was an element of justification for the use of force. In case of cyberwar one just doesn't know anything. This primarily concerns international organizations and states that must assess whether it is an act of war, repression, counterattack, etc.

A conventional war is based on movements of troops, weapons from one border of a country to another. In case of information conflict, such moves are not visible, and its purpose may be to damage things or to change or select pieces of information, to influence people, to harass them, shock or cause chaos, but killing is not the direct goal.

Today nobody doubts that technology together with conventional weapons in a great way helps you to win battles, especially in the conflict between two powers with similar technological developments.

Another phenomenon associated with modern armed conflicts is the idea of hybrid, understood as a new approach in the study of armed conflict [18]. It is seen as the coexistence of both *old* and *new* elements of wars, the classic armed conflicts and modern wars, battles of the national armed forces and asymmetric conflicts, super modern military technology and primitive tools, fight for territories and natural resources and conflicts of identity and values [18]. Hybridization may include both sides fighting (the countries, informal groups, irregular armed groups), the space of the conflict, the causes and nature of the conflict [18]. The main feature of hybridization in modern wars is simultaneous existence of two main planes of conflict: territorial and virtual. The territorial plane refers to the classic understanding of the country or ethnic groups living permanently in the territory. The virtual plane refers to communication within the network disregarding territories promoting values, principles and ideas [18].

The distinguishing feature of an information war is saving the use of violence through manipulation of information, as well as transferring the conflict from military operations to the use of technology. Information war can have several meanings ranging from lies, propaganda to manipulation. This is done according to a pattern where both parties will blame each other, e.g. the Israelis and the Palestinians- who is responsible for the poisoning of the Western journalists, or inventing fake victims or mass graves.

Information war has destabilizing influence on the functioning of public institutions, and consequently on the level of national security. It involves accusing state institutions of getting involved in operations embarrassing state institutions, for example in the negotiations. Such operations are often carried out by specialized support organizations cooperating with a foreign country [19]. This type of war is characteristic for industrial espionage or national military industry where sabotage or compromising foreign partners before the authorities or before international organizations often takes place.

Information war is nothing else but a war with the use of information, which means actions that are illegal, but still aggressive and which are intended to: weaken the rival by rumors and attacks that can damage his image, or can be used to acquire knowledge in order to gain control over the market, technology, which obviously makes carrying out military operations much easier. Not without significance are also attacks whose aim is to overload the administrative institution's website or plant in a virus or other malicious software.

There are four types of information management, which may prove to be an effective tool of war, i.e.: 1. Secrecy, in order to make your own intentions and capabilities incomprehensible to the enemy and rival; 2. Stealing secrets from the other party, or search for information, to know what your opponent may want to do; 3. Promotion of information in order to trick the enemy, or to make them take wrong decisions; 4. Promote positive or negative beliefs in order to stimulate the activists, and to discourage those who sympathize or those who are so far neutral towards their rival [20].

In most cases, keeping and preserving secrets becomes a matter of cryptography, algorithms, software, firewalls, passwords, and other devices that are both sophisticated and dematerialized (in contrast to e.g. the master secret encoded). Today more and more rarely attempts are taken to break into safes or wade through the hallways of the buildings to discover secrets. Malware, such as Trojans, duplicate and lead out sensitive data or simulate a seizure of power.

Hackers have become a huge threat, for example, by including an infected computer in the network of a public administration, they organize something like an invisible coup d'état. In such case, a single machine or entire network no longer perform commands of their real owner, but are remotely manipulated by a pirate.

By destroying the enemy's means of communication or transport, we disable him to execute orders, to coordinate the work of state institutions or deprives of access and contact with reality, which may lead to taking risky decisions. In such cases, the damage can cause chaos in emergency systems, airports, energy supply, etc., and finally lead to death through a chain of consequences: digitally paralysing departments and institutions.

4. Cyber-attack as Disinformation

How can one distinguish between a cyberattack and cyberwar? According to a popular definition in the academic community, a cyber-attack can constitute a cyberwar when it is part of a real military conflict or conforms to particular standards given no physical war happening. Though views on the particular standards differ, the degree of damage is universally agreed upon as primary judgment criteria. Military experts have shown unanimous concern over the much more disastrous consequences cyberattacks could bring to humankind than traditional wars given the fragility of cyberspace and its close link with people's lives--for instance, the possible nuclear disasters caused by cyberattacks [21].

An increase in the use of Internet has become one of the most amazing phenomena in the history of the mankind. It is not only a means of communication, but also a centre of global information infrastructure, which has an impact on real-time culture. This phenomenon has changed the functioning of each element of everyday life, starting from the standards of writing, communication, financial transactions, up to the medical practice. The Internet has, therefore, become a universal space for social interactions, trade, doing politics, and carrying out certain activities aimed against the security of a state and its citizens.

The national security expert and former advisor to the White House on matters of terrorism, Richard Clarke defines cyberwar as "activity of penetrating computers or network of another nation aimed at causing damage or disruption" [22]. The method of controlling information for political and strategic benefits is not new. Manipulation of computer networks provides a new way to achieve such goals. Individuals, companies and governments can manipulate computer networks for the purposes of propaganda, to collect and classify information, paralyze or destroy key infrastructure installations.

Professor Matthew c. Waxman defines cyberattacks as "an effort to change, destruct, degradation or destruction of computer systems and networks, and the information or programs on the computers of the enemy" [23]. Professor Michael N. Schmitt notes that network attacks "can be activities of individual hackers or of organized group" [23]. These broad terms and their definitions reflect the massive application of technology in the defensive and offensive strategy.

Collecting information is necessary for each country, in time of peace or conflict. However, can the use of computer networks in order to infiltrate another country be considered as the use of force? Certainly, the awareness of technological advantage can provide a tool to influence another country. Attempts to pressurize are part of international geopolitics; they may compel or encourage adhering to terms and agreements between the countries. Here, the role for the cyberwar. Impersonation is one of the easiest ways to access the Internet network. American agents took part in online communities of Jihad activists in order to gather information about them.

The law of war restricts the use of computer attacks. For example, there is the principle of distinction, which is about the avoidance of damage and harm to the civilian population, and it is still valid a computer and must be used only for legitimate military purposes. To sum up, cyber-attacks need to ensure the avoidance of additional damage and necessary precautions must be taken to protect neutral people and civilians.

Cyberattacks, are notoriously anonymous, often identifying the sender is extremely difficult or entirely impossible. Even assuming that identifying the attacker is possible, often the attack ends up so fast that it is not always clear whether the use of force to self-defence was justifiable. There several factors such as: the severity, immediacy, invasiveness, measurability, the alleged legitimatization that make it possible to assess if the attack meets the criteria. For example, in the 2007 Israel bombarded the alleged nuclear reactor, the North Korean experts participated in it; it is located in the territory of Syria. The bombing was undoubtedly with the use of force.

Sometimes the effects of cyberattacks are similar to those of initialized coercion or harmful actions that are not traditionally and universally regarded as a use of force; they are for example, economic sanctions, espionage or some action under cover. Some operations may cause inconvenience or disturbance. Today, with the use of the modern means of communication the government can use social networks or information services to promote certain principles.

Modern technology provides more effective means to achieve goals, usually accomplished through military action. The easiness of hiding behind the network encourages the development of covert action. Technical measures help to keep international humanitarian principles, avoiding mass destruction during conventional conflicts. When using coercion or interference, you must be sure not to take actions too far. One of the most dramatic examples are the sanctions the UN imposed on Iraq to stop the development of nuclear weapons. These sanctions did not include humanitarian assistance; however the complex issues and the long duration of the sanctions and administrative procedures all caused extreme damage among the civilian population. Cyberweapon can create a similar disaster. A simple error in the computer code can destroy essential public services for the entire state.

5. Cyberwar and Global War

Unlike physical reality, cyberspace has a completely different makeup that affects the mix of offense and defense. It is impossible to “take and hold” cyberspace, to invoke a term often used in land warfare. Cyberspace more closely resembles the space domains where powerful countries are able to monitor, patrol, exert influence and deter aggression, but cannot exercise territorial control in the way it is traditionally conceived of during ground conflicts. Cyber sharpshooters cannot control a section of cyberspace, and should not be asked to do so. Indeed, cyberspace is a dynamic system in constant motion where clocks run at superhuman tempo close to the speed of light. Time and space are different in cyberspace. There is no “there” there, and humans are intolerably slow. Nor is there an isolated battlefield on the Internet. Instead the battlefield will necessarily involve civilian systems of every stripe because targets are spread far and wide throughout the modern world and not controlled or defended by governments. In the final analysis, the threat of cyber war is very real but is also grossly overstated. Even acts amounting to cyber war have thus far never led to military conflict in the real world [24].

Cyber war is possible in the sense that cyber-attacks could constitute acts of war. This point only becomes evident, however, if we are clear about what is encompassed by the terms “force” and “violence”, and about their relationship with the matter of lethality. Acts of war involve the application of force in order to produce violent effects. These violent effects need not be lethal in character: they can break things, rather than kill people, and still fall under the rubric of war. Moreover, the mediating influence of technology means that small acts of force – such as tapping a keyboard – can result in large amounts of violence, lethal or otherwise [25].

Cyberwar, like every conflict is linked with the strategy based on the possession of specific information. Its participants every time must answer the questions that have long occupied the Greek sophists and Chinese generals: how are actions taken, is their execution is based on real information, or just on convincing data, in other words to what extent is our reasoning appropriate, or is it based on the manipulation of the enemy? How can we know what he knows? Or how do we know what he is doing? What action should be taken to become elusive for the enemy, and his decisions and actions became predictable? Solutions to these issues have been sought for ever, however, technological progress has no definite answers, because on the one hand it makes it easier and on the other it complicates the construction of military strategy.

Contemporary armed conflicts are based-next to the traditional sources of information- on electronic data. In this area there has been a significant revolution in military affairs; the innovations are, among others: the computerization of the channels of communication and weapons, obtaining significant intelligence data on the basis of satellite images and preventive actions or sabotage in the cybernet.

What follows is a change of offensive action techniques such as; paralysis of critical infrastructure, which includes among others: communication, financial markets, public administration and the production and supply of energy, raw materials and fuel. In addition, the information and communication networks support hospitals, transport or water supply, as well as nuclear power plants, and therefore a failure or any disorder of these areas can bring serious consequence for public safety.

In addition, the technological advantage makes it easy to recognize the objectives, data transmission, the coordination of armed forces, smart management, arms, etc., which gives the governments of the most accurate and global picture of the situation, allowing instantaneous and appropriate strategic decisions, while the opponent is running in “the fog of ignorance” [26].

It must be assumed that the equipment and structure of the military-industrial complex, as well as beliefs and mentality will conform to the information revolution. Another hypothesis is that today's conflicts rely exclusively on knowledge. So they will be carried out in order to obtain global information and maintain dominant position not only in technological, but also in cultural cyberspace. The global nature of the conflict means therefore that it covers the political-military, techno-economic and ideological-cultural sphere.

Wars activate important elements in the field of information and communication. The possibility of applying them in the battlefield or action guarantees a military success. Cold war spy systems, such as the “Echelon”, have been transformed and applied also to fight in acquiring information in the field of economy and innovation [27]. Therefore, industry, technology, culture, diplomacy and war are included in the same geopolitical project. “Information war” is, therefore, an action which covers all types of goods. Following Edward Waltz, it can be concluded that this war covers the measures taken in order to preserve the integrity and protection of your computer system against the exploration, damage or disturbance in order to achieve information superiority [21].

Information war is mainly inflicting damages to your opponent or competitor using fonts and symbols instead of strength. The goal is to manipulate the available knowledge and gain a monopoly on the possession of relevant information. This objective can be achieved through espionage activities, electronic surveillance or sabotage.

In the latter case, the objective is to reduce the opponent's freedom of action through discrediting him in the eyes of his allies. In other words, the fight is done by changing the image of the enemy by giving his allies of the means to get to know, instead of means to act [21]. The effective value of information therefore depends not on its veracity, but in fact from the way it spreads. It is effective, as far as is considered true by others who adopt this point of view and values.

The perception of international relations and understanding of military strategy come from the experience of the 19th and 20th centuries, and so it relates to assumptions, that the states are competent subjects in world politics, and that the agreements between the states, reduce the risk of war. This traditional understanding of politics respects national borders and territorial integrity, and assumes that the cross-border crimes are exceptions. But some characteristics of cyberspace do not correspond with the traditional logic of functioning of the system of the state. Cyberspace has created new ways to global tensions and new possibilities in order to avoid conflict. New patterns of cyberwars are in contradiction with the existing kinds of conflict [28].

Cyber threats are serious; there is a growing threat of instability at both the regional and global levels. Dissuasive theories and strategies developed and applied during the cold war are not easily accepted in the virtual world.

Political reactions remain far behind in relation to the events in virtual reality. The scale and scope of cyber threats are simply not well understood. To a large extend it is due to the rapidly changing characteristics of cyberspace, the full extent and impact of cyber interaction and the potential and the possibility of a possible aggressor.

For the first time in human history, an advance in information and communication technologies is potentially available to most of the world's population. This allows almost anyone to disseminate messages, which means that many units have the potential to bypass official channels of communication, to discredit the authority of the state and non-state participants. International relations in the 21st century include a large number of new countries created at the end of the cold war, as well as a wide range of non-state subjects.

6. Suggested Directions of Minimizing Further Cyber Threats

Spontaneous growth of the Internet forced the state to interfere. Many documents, also known as the strategies for cyber security, are prepared by the government. Those documents share a few common fields. The first one is state infrastructure responsible for communication and providing Internet-based services. The second one is e-services, constantly gaining more importance in everyday life. The third one deals with digital competence and the state trying to reach various social groups to spread the knowledge concerning digitization [29].

An important issue, which is emphasized by almost every country, is preventing attacks that aim at stealing data, and fighting against any form of disinformation which gives the society a wrong and distorted image of the state.

Many European governments constantly talk with Google and Facebook. The idea of big Internet platforms is one of the basic strategies of a unified digital market. Issues such as misinformation and deleting of unwanted content (which incites people to violence) are connected with that market.

The biggest social networking sites or search engines have such strong positions on the market that, quite often, the state or international organizations cannot compete with them. Even large, international companies (of the automotive industry, for instance, and which have quite a capital) that wanted to form some alternatives were not able to do that, and have to use the platforms which already exist.

This issue is important because the digital platforms are often more prominent than economies of many countries and can influence the reality, politics and economy greatly. The Danes have realized that and appointed an ambassador for technology and digitization (‘Tech Ambassador’) who is responsible for contacts with big social platforms. This governmental post has functioned since July 1st 2017 and is based in San Francisco, USA. The ambassador (on behalf of the Kingdom of Denmark) is in touch only with major companies of the Internet industry: Twitter, Facebook and Google [30].

Maintaining balance between the companies’ rights and the rights of the users has become a challenge because of the issues of deliberate misinforming or banning some users' accounts with regard to their beliefs or to what they say. Guaranteeing the users their freedom of speech along with their rights in the Internet seems to be quite demanding as all the parties should be satisfied: social networking sites administrators, the citizens and the state.

It has to be mentioned that it is (and will be) common to combine the politics of cyber security with economics. It results from the fact that a stable financial system is one of the basics of a state and is, therefore, in danger of being attacked by cyber terrorists. Moreover, cyber security systems in financial institutions can be quite successfully implemented into other bodies of the state.

A quick digital development was the result of Internet banking, online shopping and social networking. High-frequency trading, financial robo-advisors and damage resulting from cyber-attacks are the main parts of a technological time-bomb that is ticking as we speak.

According to experts, attacks on industrial systems are not just hackers' pastime because they are too expensive and complicated. [31] Well-paid groups of specialists are usually behind such operations and their main motive is usually money. Security systems of the crucial state institutions become more effective and so do the attackers; these are not just amateurs, who try to break into vital institutions, but well-prepared and organized groups of professionals.

The future of fighting against cybercrime is creating new models of security teams in companies, the so-called security centers with a new type of specialists: threat hunters [32]. Thanks to them it is possible to review the way employees meet the security standards in a company, react to any inside or outside incidents, seek any anomalies and constantly, automatically analyse millions of potential cyber-attack scenarios.

Microsoft sees those trends. The company has formed a special group of international experts under the name of Microsoft Enterprise Security Group whose main task is to provide the company with solutions, expert evaluation and service concerning Internet security. Microsoft has also created a special unit - Digital Crimes Unit – a cyber-security center which operates in real time.[33] Digital Crimes Unit is comprised of lawyers, web security experts and computer forensics experts. Microsoft DCU operates with such international law enforcement bodies as: FBI, Europol and Interpol. The result of Digital Crimes Unit activity is the Enterprise Customers Cyber Threat Intelligence Program (ECCTIP), which welcomed as its first European member PKO Bank Polski [34]. ECCTIP's aim is increasing cyber security level through information exchange. Cooperation with the program's participants allows an effective information exchange and the analysis of submitted malware. Thanks to the exchange of information and experience with DCU, the bank experts are able to counteract before a potential threat spreads all over the other countries.

The human factor and the structure of organization play a major part in cyber security. Lately, there have been more cases of employees revealing classified contract data, putting many companies at risk of making considerable losses. The most effective method of securing any data is the cautious approach towards both outsourcing companies and the company's own employees.

Summing up, the organizations have to work out a plan and be aware that they are going to be attacked by cyber terrorists. The threat hunters allow being a step ahead of cybercrime but will succeed only when the human-machine interaction is effective in eliminating the threats.

It may be assumed that the direction of future research on cyber security will evolve towards separating different fields, but the common area will be the functioning of technology. Technology will determine the functioning of such fields as politics, law, economics or the way public institutions operate.

REFERENCES

[1] Clarke R., Knake R., Cyber War: The Next Threat to National Security and What To Do About It, New York 2010, p.1-12.

[2] Kaiser R., The birth of cyberwar, "Political Geography", 2015, vol. 46, p. 11.

[3] Arquilla J., Ronfeldt D., Cyberwar is coming!, "Comparative Strategy", 1993, vol. 12/2, p. 141.

[4] Lukasik S. J., A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible 99 Declaratory Policies for These Domains, [in:] Proceedings of a Workshop on Deterring Cyber-attacks. Informing Strategies and Developing Options for U.S. Policy, Washington 2010, p. 99-122.

[5] Górka M., Lies chat. Virtual threats and the real problem, [in:] Cyber security as the basis for a secure state and society in the twenty-first century, (ed.), M. Górka, Warsaw 2014, p.148-157.

[6] Wall D., Cybercrimes and the Internet, [in:] Crime and the Intenet, ed., D. S. Wall, London-New York 2001, p.1-18; M. Yar, Cybercrime and society, London 2006, p. 9-11.

[7] Jordan T., Taylor P. A., Hacktivism and Cyberwars Rebels with a cause?, London- New York 2014, p.1-19; J. Titcomb, Hacktivism is rising threat to firms' security, "City A.M.", 10 December 2012, p. 12.

[8] Wilmink Ch., Culture of 'hacktivism' very dangerous for teenagers, "North Bay Nugget", 20 June 2001, p. B4.

[9] CyberWar: Point Counterpoint, "Defense Daily International", 2000 r., vol. 1/35, p.1.

[10] Ventre D., Cyberconflict: Stakes of Power, [in:] Cyberwar and Information Warfare, (ed.), D. Ventre, London 2011, p. 213-230.

[11] Libicki M. C., Cyber-deterrence and Cyberwar, RAND Corporation, 2009, pp. 179-181.

[12] Arquilla J., The Computer Mouse that Roared: Cyberwar in the Twenty-First Century, "Brown Journal of World Affairs", 2011, vol. 18, p.39.

[13] Mehan J. E., CyberWar, CyberTerror, CyberCrime, IT Governance, 2009, pp.19-48.

[14] Czulda R., The attack in wirtualu, "Polish Armed", 2013, vol. 11, p. 26.

[15] Dereń J., Rabiak A., NATO and safety aspects in cyberspace, [in:] Cyber security as the basis for secure state and society in the twenty-first century, op. cit., pp. 202-221.

[16] Grove G. D., Goodman S. E., Lukasik S. J., Cyber-attacks and International Law, "Survival", 2000, vol. 42/3, s. 89-104.

[17] Pearson I., Cyberwar threats are all too real, assures futurologist, "Engineering & Technology", 2010, vol. 5, pp.25-26.

[18] Gruszczak A., Hybridity of contemporary armed conflicts - Critical analysis, [in:] Asymmetry and hybridity - the old army against new conflicts, (ed.), B. Zapała, W. Sokała, Warsaw 2011, pp. 9-17.

[19] Dela P., The struggle for information in cyberspace, [in:] Cyber security as the basis for secure state and society in the twenty-first century, op. cit., pp. 267-268.

[20] Sienkiewicz P., Information superiority in combat and business, [in:] 10 lectures, National Defence Academy, Warsaw 2005, p.86.

[21] Wlatz E., Information Warfare, Principles and Operations, Norwood: Artech House Boston, London 1998, p. 85.

[22] Li Y., Is a Cyberwar Coming? - The alleged Sony hacking warns of the grave consequences of cyberwarfare, "Beijing Review", 15 January 2015.

[23] Feil J. A., Cyberwar and Unmanned Aerial. Vehicles: Using New. Technologies, from Espionage to. Action, "Case Western Reserve Journal of International", 2012, vol. 45, p. 518.

[24] McGraw G., Cyber War is Inevitable (Unless We Build Security In), "Journal of Strategic Studies", 2013, vol. 36/1, p. 109-119.

[25] Stone J., Cyber War Will Take Place!, "Journal of Strategic Studies", 2013, Vol. 36/1, s. 101-108.

[26] Ventre D., Cyberwar and Information Warfare, Wiley - ISTE, London 2011, p.6.

[27] Suissa R., Military Resilience in Low-Intensity Conflict: A Comparative Study of New Directions Worldwide, Lexington Books, Plymouth 2012, pp. 9-30.

[28] Choucri N., Goldsmith D., Lost in cyberspace: Harnessing the Internet, international relations, and global security, "Bulletin of the Atomic Scientists", 2012, vol. 68/2, pp.70–77.

[29] Haeussler U., Cyber Strategy and the Law of Armed Conflict, "Journal of Information Warfare", 2011, vol. 10/2, pp. 38-47.

[30] Waeschenbach J., Denmark to appoint digital ambassador as tech firms wield more power, "DPA International", 27 January 2017.

[31] Faria J. R., The Economics of Technology in Terrorist Organizations, "The Brown Journal of World Affairs", 2014, Vol. 20/2, pp. 285-296.

[32] Seffers G. I., The Evolution of the Cyber Hunter, "Signal", 2017, Vol. 71/10, pp. 17-18.

[33] Sunnyvale C., Fortinet Expands Technology Alliance with Microsoft to Deliver Cloud Security at Scale for Global Enterprise Customers, "NASDAQ OMX's News Release Distribution Channel", 26 June 2017.

[34] Oltsik J., FireEye Myth and Reality, "Network World", 15 October 2015.