Nr 1 (163) 2012 ISSN 1731-8157

FUTURE CYBERSPACE WAR AND ITS IMPACT ON POLISH ARMED FORCES

Włodzimierz CHOJNACKI*

* *Faculty of Security Sciences, Gen. Tadeusz Kosciuszko Military Academy of Land Forces*
e-mail: wchojnacki2@interia.pl

Received on 20 December 2011; accepted in revised form in March 2012

In this article, an attempt is made to create new concepts, definitions as well as the levels and security pillars due to which it is possible to better explain the importance of threats resulting from cyberterrorism in various dimensions. The groundwork for my considerations is to include the quantitative and qualitative results from the comparative studies conducted both in the sphere of cyber war theory and its implementation. Moreover, the analysis of many special documents and professional literature is closely related to the advance of sophisticated information technology and its application in achieving political, economic and military purposes. The knowledge collected this way enabled the author to describe, explain and elaborate on the outline of changes in strategic concepts, legal acts as well as the procedures indispensable for preemptive actions connected with waging cyber war. In the opinion of the author, knowledge created this way will be mainly of future character. A hypothesis is proposed that a contemporary researcher should be a futurist possessing interdisciplinary knowledge and long-term experience on waging cyber war and thinking in the analytical and innovative way. A good example is a terrorist attack of 9/11, which dramatically enlarged our imagination and perception of the risk and threat even on the part of minor terrorist groups asymmetrically operating in the non-conventional way.

Keywords: *security, futuristic thinking, cyberspace, cyberterrorism, asymmetric operations, sophisticated information technology, modernization, transformation, professionalization of armed forces.*

1. FUTURE WARS AND ARMED CONFLICTS

Career soldiers, especially commanders, have to posses knowledge not only about historical and contemporary military threats, but first of all they should concentrate on elaborating strategic concepts for future war conflicts. As a result, they should be more futurists than conservatively thinking historians[1]. They ought to prove thinking in the category of futurology about the place and role of particular branches of military forces in the long-term programs of the Armed Forces modernization and development. Above

[1] W. Chojnacki, *Społeczne, edukacyjne i militarne problemy ery globalizacji*, [in:] „Kwartalnik BELLONA", No 1/2011, Warszawa 2011, pp. 170-185.

all, they should posses interdisciplinary knowledge and military experience in the area of modernization, transformation, restructurization and professionalization of the Army. Such way of thinking should be obligatory subjected diagnosis of officers, especially senior officers and generals performing their duties in headquarters, general staff and at logistic posts. This diagnosis should respect the skill of future thinking related to the defined level of command. This poses a new challenge for recruitment, education and training in the military system. Prior to implementing these changes, it is necessary to answer an important question. **What has to be the officer`s, NCO`s and career soldier's contemporary vocational characteristics?**

The experiences of the US and other countries from the last decade of fighting on terror evidently show that the present professional training system preparing soldiers for waging war operations in Iraq and Afghanistan did not meet expectations of top ranking DoD representatives[2]. The specificity of military actions in Iraq and Afghanistan at tactical, operational and strategic levels is far apart from the specificity of war actions in Europe. The comparative studies based on qualitative methods (interviews and narrations) indicated that the majority of military and civilian authorities presented conservative and conformist attitudes both among the top ranking officers and politicians contrary to younger officers and NCOs during the war in Iraq and Afghanistan. This evident division of attitudes can be explained through the burden of experiences and presentation of the self-preserved attitudes. But this explanation seems to be too simple, because the essence of this division is probably deeper and more complex. It is possible to assume that this cause exists in future thinking and bold activities.

The events from September 11 transparently made civil and military security experts aware how important it is to prepare alternative strategic solutions for the army and other services responsible for homeland security[3]. Present experience indicates that even the US did not have alternative plans of strategic character. In the opinion of Stephen Peter Rosen, prior to September 11 in the Pentagon, the future was considered in terms of the Iraqi war from 1991 and limiting peacekeeping operations in this region[4]. But right after September 11 a sudden change of paradigm occurred. The main reason for changing paradigm was futuristic thinking of terrorists anticipating thinking of outstanding civil and military experts and even restraining vigilance of many officers from special services. A routine and schematic way of thinking as well as not appreciating the weak signals from the terrorists getting prepared for the attack. In consequence, conservative and schematic way thinking led to the tragedy of September11 as well as the wars in Iraq and Afghanistan. It is necessary to assume with a high degree of probability that this way of activities on the part of terrorist groups can be innovatively repeated. However, terrorists are aware that they must search for new solutions to be able to surprise special services. One cannot evade that the common denominator of all the future attacks will be an innovative way of thinking and surprising action as well as the opti-

---

[2] W. Chojnacki, *Changes in Global Fighting on Terror from Bush to Obama Strategies*, Published by European Sociology Association, Lisboa 2009.

[3] W. Chojnacki, *Outline of New Model for Sociological research concerning Tangible and Intangible Security Measurment*, [in:] *An Interdisciplinary Journal TRANSFORAMCJE*, Kozminski University, Warsaw 2010, pp. 96-115.

[4] S. M. Convertino, L.A. DeMattei, T. M. Knierim, *Flying and Fighting in Cyberspace*, Air War College, Air University Press Alabama, July 2007, pp. 23-26.

mal utilization of both civil and military resources and means. At present, it is possible more and more to monitor links between terrorist groups and their sympathizers as well as the interest groups which are engaged in their instrumental use for implementing their own purposes. In addition, the problem is much more complex than could be imagined because it is possible that in many intelligence agencies there are some people who at least sympathize with the groups having the targets difficult to clarify and define.

The effective way of solving the abovementioned problems is to define the main development trends occurring in the area of armies, societies and states on the basis of historical comparative analysis, contemporary important facts and occurrences. It is worth emphasizing that the ongoing processes are defined not only by the continuity of historical facts but also through the qualitative changes which are difficult to compare. The qualitative changes are mutually intertwined and require interdisciplinary knowledge and rich experience from researchers.

A good example is the demography which evidently indicates that in poor countries where GDP is very low, the birth rate is very high despite the high percentage of newborn death rate. But in highly developed countries the demographic situation is diametrically different. Russia is the most typical example where one can observe for a few decades a dramatic and progressive drop in population. This negative process is accompanied by the low level of medical care as well as the high index of divorces and alcohol consumption. This demographic analysis has a strategic significance for national security and in this case has a global dimension, since it indicates the possibility of existing destabilization in this important region of the world where the Orthodox Christian and Chinese civilizations come into crash. In this context the ageing and shrinking of European, Russian and Japanese populations are also easy to be felt at present, and in the future what makes these two civilizations very weak in regards to social and economic issues is China. The demographic situation of European countries is especially essential for Poland because of its strategic and geographic location. It is easy to notice that the growth in birthrate occur mainly in the countries of the Mediterranean Basin. This demographic rise in the Islamic population results mainly in people migrating from Northern Sub-Saharan Africa and a growth in child birthrate in Islamic families living in Europe.

Contrary to a decrease in population numbers, the development of information technology is growing rapidly. In the opinion of Andrew Marshall, the director of the Pentagon Net Assessment Office, the significance of analysis and long-term planning connected with rapid improvement in information technologies make it possible to find military systems such as air bases, aircraft carriers and tanks as well to destroy quickly whatever one can find. A good example is the war in Afghanistan where small teams of soldiers supported by high-tech sensors and highly accurate missiles protected military bases. At the same time unmanned aerial vehicles called *Predators* surveilled the selected military targets, when gathering information data and sending them to Cyber Command Centers. In spite of that, the US possesses such impressive military technology and the greatest threat for them is terrorism and proliferation of nuclear weapons[5].

[5] Por. M. Hillegas, *The Future as Nightamare. H.G. Wells and the Anti-Utopians*, Oxford University Press, New York 1967.

It is worth mentioning that geography and technology are not the only war triggers, since politics is the main perpetrator, and for this reason it should be analyzed in detail. But an objective assessment of its own policy, economy and the army is very difficult. A good example is the US whose military spending exceeds sevenfold the spending of other world powers combined. Their declared goal is not combating a rival but maintaining their imperial position and world order. The acknowledgment of this process limits the number of waging imperial wars with simultaneous leaving of garrisons and military bases in many flashing points of the world. At present China is an emerging challenge for the US but still faces many major economic, military, political, religious grievances which may lead to internal disorders in the near future.

2. THE FUTURE CYBER WARS

At present cyberspace should be understood as a fundamental fighting component in cyber war that utilizes transferring signals, data, information, knowledge and intelligence between the sender and recipient through the channels and networks of the information systems. The main areas of waging cyberspace operations are internal and external determinants. The external factors include such domains as: cooperation in the framework of military, political and economic alliance. But the internal factors have a great impact on the efficacy of waged operations focused around cooperation of such main entities as: government institutions and agencies, private economic sectors and the society. Within the framework of government institutions, a very important role is played by the Department of Defense (DoD). Moreover, cooperation between DoD and particular branches of the Armed Forces (Air Force, Army, Navy and Special Forces) is indispensable for accomplishing the accepted strategy of operations in cyber war. Waging cyber war requires fulfilling many conditions like:

- information-technology infrastructure is indispensable to public and private sector activities on international and global scale;
- vulnerability of our information-technology infrastructure to risk and threat on the part of terrorist groups capable of mounting Cyber attacks.

It is worth mentioning that cyber wars have not taken place in the past but many recent premises have indicated that this kind of war is now being waged by cyber commands and staffs of the major world powers[6]. At present the level of resources and modern technology engaged in waging cyber war authorizes one to formulate a hypothesis that such a way of waging war will be mainly undertaken on a bigger scale in the near future. For this reason, it is necessary to elaborate not only on the outline, but the strategic concept that should make up the basis for waging cyber war. Nowadays, one can show the following three levels of activity escalation featuring cyber war:

- difficulty in identifying individuals, groups and centers located in and beyond the country, inspiring hackers to carry out cyber attacks against data bases which are at the disposal of states, armed forces, investigation labs and Internet services;

[6] W. Chojnacki, J. Świniarski, *Podstawy cybernetyczno-technologicznej wiedzy o bezpieczeństwie*, [in:] *Bezpieczeństwo w teorii i badaniach naukowych*, pod red. B. Wiśniewski WSPol, Szczytno 2011, pp. 79-87.

– transparently, politically inspired and guided cyber terrorist attacks oriented at strongly guarded servers and data bases constituting the important link in waging cyber war;
– increasing role of cyber war in achieving political, economic and military targets by a given state through system computer network attacks supported by intelligence agencies.

The evident premise to make the presentation of the entire picture difficult indicates that the efforts made by national defense departments are meagerly exposed because of their concealed character. But the question is being raised to what extent the information on cyber war can be concealed. Therefore, it is essential for the reason of cooperation between DOD and local civil authorities. It is worth mentioning that this problem is existing in the armed forces themselves – among the Army, the Navy and the Air Force. The synergic effects of both civilian and military effort might provide our state with the capability of defending our technological infrastructure by extensive enlargement[7]. The announcement of William Lynn, the US Deputy Defense Secretary, indicates that the US possesses a Cyber Command capable of deterring any cyber attack. At the same time, W. Lynn strongly underlines the defensive character of the US cyber war strategy. In his opinion, this strategy bases upon five pillars: treat cyber as a domain, employ more alternative active defense operations, support the Department of Homeland Security in protecting critical infrastructure networks, practice collective defense with allies and international partners, and reduce the advantages attackers have on the Internet[8]. Such a high level of developing the Cyber Command by the US evoked a genuine chain response, since in 2009 South and North Korea as well as Great Britain assumed activities oriented at organizing a Cyber Warfare Command. In 2010 the US created the first Cyber Warfare Intelligence Center and in response to this fact China announced the creation of a defensive cyber command and information security department[9].

FIGHTING IN CYBERSPACE – CONCLUSIONS FOR THE POLISH ARMED FORCES

The Polish MoD must understand that cyberspace is at present a fundamental component in the future war waged at all levels from tactical to strategic military action. For this reason, the Polish Armed Forces should work out cyberspace standard definitions for each kind of military branch, doctrines and strategic concepts. Following the pattern of the US and Great Britain, one ought to establish a Polish Cyber Command composed of several service elements: an Army Cyber Command, a Naval Cyber Command, an Air Force Space Command and a Special Service Cyber Command. Each of these elements will form a link of a Joint Command for fighting in cyberspace[10]. Every Cyber

[7] *New Cyber Warfare Branch Proposed*, [online]. [dostęp: 2011]. Dostępny w Internecie: http:/blogs. govinfosecurity.com

[8] E. Nakashima, *Dismantling of Saudi-CIA Web site illustrates Reed for clearer Cyber war Policies* [online]. [dostęp: 2011]. Dostępny w Internecie: http:/www. washingtonpost.com/wp

[9] S. P. Rosen, *The Future of War and the American Military*, [online]. [dostęp: 2011]. Dostępny w Internecie: http://harvardmagazine.com/2011/11/the future-of-war-and -th.html.

[10] Chief of Naval Operations, *Fleet Cyber Command/ Commander Tenth Fleet Implementation Plan, Memorandum*, United States Navy, 2009 [online]. [dostęp: 2011]. Dostępny w Internecie: http://en.wikipedia.org/Wiki/United States Cyber Command.

Command should define the standard and its own participation in cyberspace fighting. This standard ought to fulfill the following requirements:

- implementing its own cyberspace concept and training system with a particular respect to the configuration of computer tools, secure information networks and servers;
- defining its own participation in military operations within the framework of cyberspace fighting;
- understanding the role in security strategy of its homeland as well as being in ongoing combat readiness to deter and repulse any cyber-attack;
- systematic applying new information technology and improving network security systems;
- building solid foundations in the area of organization and institutionalization oriented at cyber-mindedness as well as shaping capabilities needed in future cyber war.

Many international experts think that the cause of cyberspace appearance is the synergy of information with network environment, which should be treated as a new revolution in the military affairs (RMA). In the opinion of Jeffrey R. Cooper, one can say at present about the impact for information warfare, which is shown in Fig.1.

The model presented above indicates mutual relations occurring between the revolutionary changes in information and the changes in homeland security[11]. The main advantage of this model is a transparent presentation of the impact of information revolution on military affairs in the cyberspace domain. Present-day practice shows that cyber intelligence, surveillance, reconnaissance, cyber defense and offence should be understood as basic cyber capabilities. These capabilities are especially important when a given country strives for achieving its tactical, operational and strategic targets. In such a situation the state ought to make a diagnosis of its security level and own interests, simultaneously mainly paying attention to the following:

- level of advance in technology in military affairs, including the effectiveness of networks and servers management as well as the vulnerability to cyberspace attacks;
- level of system assurance and its capability to reconstruct, either destroy or damage, the elements of this system;
- level of possibility in quick and precise execution of attack against the most vulnerable cyberspace network systems of the enemy.

Achieving tactical, strategic and operational targets in cyberspace through information networks requires implementation of changes at each level of using sophisticated information technology both in civilian and military areas. This approach provides for the full integration of computer network tools with cyber space operations and assumed targets. Regarding the military sphere, the main components of this integrated information system managed by the US Cyber Command are: satellite stations, strategic intelligence aviation, early warning system of AWACS, drones, unmanned (helicopters, tanks, armored vehicles) and smart breaching fighting fields system. Recent news con-

[11] Por. W. Chojnacki, B. Kaczmarczyk, *Optymalizacja procesów zarządzania kryzysowego*, Lubań 2011.

cerning intercepting a US drone over the Iranian territory by the army indicates not only that they are in possession of effective information systems enabling one to pull a drone down to earth, but that the very important component of cyber system information requires rapid modernization. Since the Iranians gained access to new information technology, it is possible that other countries will also soon acquire this technology.

At present, in Poland, in the abovementioned areas, the new trends of the development in the Polish Armed Forces have been defined by President B. Komorowski and detailed by S. Koziej, the chief of Homeland Security Office. In the framework of the new development program of the Armed Forces for the years 2013-2022, the Armed Forces are to be mobile and ready to defend the territory of our country on land, at sea, in the air and cyberspace. For this purpose, organizational changes will be made in commands and military education centers. The commands are to be established: one responsible for combat readiness of the Armed Forces, the other one for commanding the Armed Forces in crisis situations, threats, armed conflicts and wars.

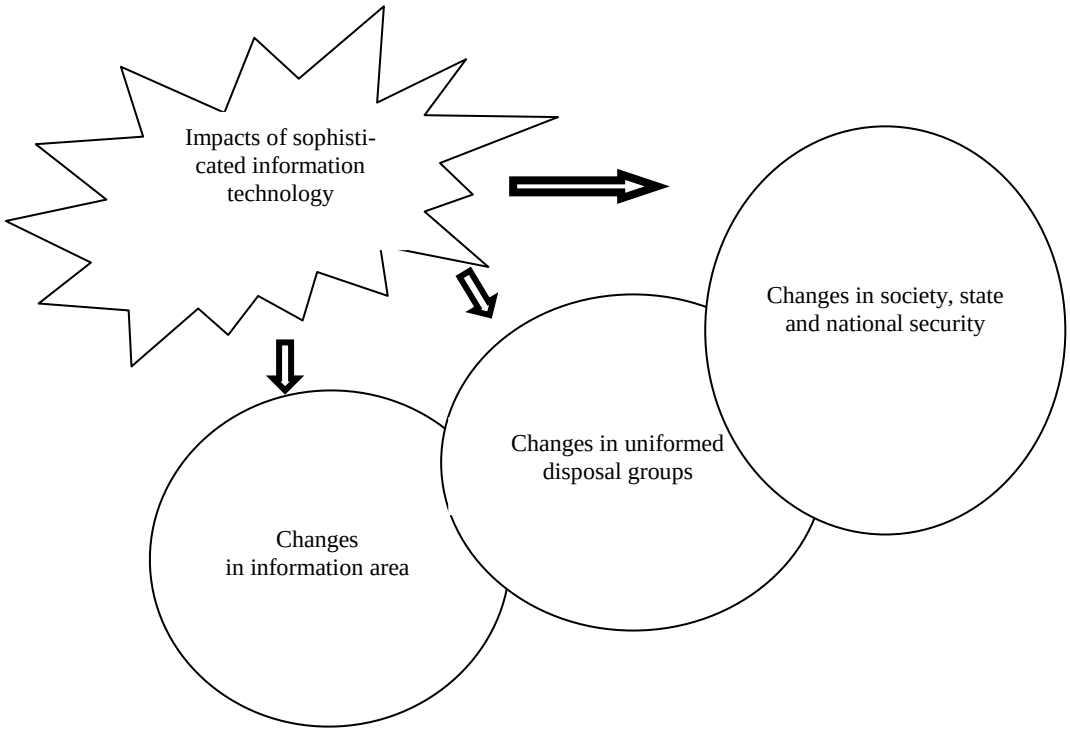

Fig. 1. The impact of sophisticated information technology on warfare and homeland security

Source: Own sources

REFERENCES

1. Chief of Naval Operations, *Fleet Cyber Command/ Commander Tenth Fleet Implementation Plan, Memorandum*, United States Navy, 2009 [online]. [dostęp: 2011]. Dostępny w Internecie: http:// en.wikipedia.org/Wiki/United States Cyber Command.
2. Chojnacki W., *Outline of New Model for Sociological research concerning Tangible and Intangible Security Measurment*, [in:] "An Interdisciplinary Journal TRANSFORAMATIONS", Kozminski University, Warsaw 2010.

3. Chojnacki W., B. Kaczmarczyk, *Optymalizacja procesów zarządzania kryzysowego*, Lubań 2011.
4. Chojnacki W., *Społeczne, edukacyjne i militarne problemy ery globalizacji*, [in:] „Kwartalnik BELLONA", No 1/2011, Warszawa 2011.
5. Chojnacki W., *Changes in Global Fighting on Terror from Bush to Obama Strategies*, Published by European Sociology Association, Lisboa 2009.
6. Chojnacki W., Świniarski J., *Podstawy cybernetyczno-technologicznej wiedzy o bezpieczeństwie*, [in:] *Bezpieczeństwo w teorii i badaniach naukowych*, pod red. Wiśniewski B., WSPol, Szczytno 2011.
7. Convertino S. M., DeMattei L.A., Knierim T.M., *Flying and Fighting in Cyberspace*, Air War College, Air University Press Alabama, July 2007.
8. De Wijk R., *NATO on the Brink of The New Millennium. The Battle for Consensus*, Brassey`s London-Washington 2000.
9. Hillegas M., *The Future as Nightamare. H.G. Wells and the Anti-Utopians*, Oxford University Press, New York 1967.
10. Horyń W., *Education of Officers in Selected NATO Armies*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2006.
11. *International Security* January-June, Publishers of the Police Academy in Szczytno 2011.
12. Jacoby W., *The Enlargement of the European Union and NATO. Ordering from the Menu in Central Europe*, Cambridge University Press, Edinburgh 2004.
13. Krć M., *Military Expenditures During and After the Cold War*, Ministry of Foreign Affairs of the Czech Republic, Prague 2000.
14. Nakashima E., *Dismantling of Saudi-CIA Web site illustrates Reed for clearer Cyber war Policies*, [online]. [dostęp: 2011]. Dostępny w Internecie: http:/www.washingtonpost.com/wp.
15. *New Cyber Warfare Branch Proposed*, [online]. [dostęp: 2011]. Dostępny w Internecie: http:/blogs.govinfosecurity.com.
16. Rosen S. P., *The Future of War and the American Military*, [online]. [dostęp: 2011]. Dostępny w Internecie: http://harvardmagazine.com/2011/11/the future-of-war-and -th.html.
17. Sloan E. C., *The Revolution in Military Affairs. Implications for Canada and NATO*, McGill_Queen's University Press 2002.

PRZYSZŁA WOJNA W CYBERPRZESTRZENI A JEJ WPŁYW NA WOJSKO POLSKIE

Streszczenie

W artykule podjęto próbę przedstawienia zarysu przyszłej strategii cyberwojny oraz określenia jej głównych poziomów i filarów, dzięki którym możliwe będzie lepsze wyjaśnienie

nowych zagrożeń i ryzyka wynikających z cyberterroryzmu w jego różnych wymiarach. Rozważania autora ogniskują się wokół ilościowych i jakościowych wyników badań porównawczych prowadzonych zarówno w obszarze teorii, jak i praktyki ściśle związanych z cyberryzykiem, zagrożeniami i wojną. Analiza wielu raportów, studiów i materiałów oraz specjalistycznej literatury wskazuje, zdaniem autora, na ścisłe związki zachodzące pomiędzy wysoko zaawansowanymi technologiami informatycznymi a ich wykorzystaniem do realizacji celów politycznych, ekonomicznych i militarnych, w tym działań o charakterze terrorystycznym. Zgromadzona w ten sposób wiedza umożliwiła opis, wyjaśnienie i opracowanie zarysu zmian, jakie należy wprowadzić w strategicznych koncepcjach cyberwojny, aktach prawnych i procedurach niezbędnych do podejmowania działań związanych z jej przygotowaniem i prowadzeniem. W opinii autora, kreowana współcześnie wiedza będzie posiadała głównie walor futurystyczny zarówno w obszarze teorii, jak i praktycznych modeli i procedur oraz będzie opierała się na interdyscyplinarnej wiedzy, długoletnich doświadczeniach w prowadzeniu tego typu działań, a także futurystycznym myśleniu analitycznym i innowacyjnym. Dobrym przykładem jest tragiczny w skutkach atak terrorystyczny z 11 września, który w sposób dramatyczny poszerzył horyzonty naszej wyobraźni i percepcji postrzegania ryzyka i zagrożeń ze strony małych grup terrorystycznych przygotowanych do podejmowania działań asymetrycznych w sposób niekonwencjonalny nawet na terytorium USA.

Słowa kluczowe: *bezpieczeństwo, myślenie futurystyczne, cyberprzestrzeń, cyberterroryzm, działania asymetryczne, wysoko zaawansowana technologia informatyczna, modernizacja, transformacja, profesjonalizacja sił zbrojnych*