Nerijus Maliukevičius*
Institute of International Relations and Political Science of the University of Vilnius

Military Conflict in the Information Age and Lithuania's Preparedness

The information revolution is changing the international system and the security environment in which we live. The state is loosing its monopoly of power in a global information space where, with the help of new technologies, people create their wellbeing and where, by means of the same modern technologies, military conflicts of a new type are occurring. The Western civilisation conception of a military conflict, based on the Clausewitz model where leaders set political goals and control soldiers; soldiers fight directly and become lawful targets of violence; and civilians do not participate in the conflict, but support their leaders by paying taxes and backing their political goals, is falling apart. A conflict of the information age is, in a sense, a "pre-Westphalian" conflict where crimes against civilians and the internal order of the state were the norm.

The question arises of how the state may ensure the security of its citizens. The great powers try to find an answer in the strategies and programs of information operations. A great amount of attention is given to the public information of the state during a conflict, as well as to information security. In the latter sphere, Lithuania has already made its first steps; however, Lithuania needs to learn the principles of public information not only during conflict, but also during peacetime.

Introduction

Military conflicts are inseparable elements of the development of the international system and its change. As a consequence of interstate wars, the dependence of territories used to change, new norms of international relations would take root whereby the *status quo* favoured by the winners was ensured. New international organisations, as well as international regimes, would come into being. However, such a relationship has always been reciprocal: the processes taking place in the international system used to influence the nature of a conflict, its potential participants, as well as measures used in the conflict.

One of the most essential global processes, which started long before the Cold War ended, is the information revolution. It has had an effect on every person, on everyday activities, on public and private institutions, and, what is most important, on every state and its role in the international system. It has been stated that following the industrial revolution, or the nuclear age, which was the motivating power of the past century, the age of information has begun. A global information space is being formed in international relations where the means of communication and information

* *Nerijus Maliukevičius* - Ph.D. candidate, Institute of International Relations and Political Science of the University of Vilnius. Address: Vokiečių 10, LT-01130 Vilnius, tel. +370-5-2514130, e-mail: n.maliukevicius@vilsat.net

technologies eliminate the boundaries of time and space. Hence, the international system is changing, a new security environment is forming, and at the same time the nature of military conflicts is also undergoing a change.

At the end of the 20th century, the costs of collection, dissemination and effective use of information had been reduced. This happened due to the rapid development of information technologies. Therefore, it is not surprising that currently many states, including Lithuania, develop programs of "the information society", "a knowledge-based society", "e–government", etc., because they associate their wellbeing with an effective use of information.

However, "knowledge is the key to destruction as well as production"[1]. The information revolution has exerted an impact on conflict, which may occur at different levels. Information wars going on between the oligarchs and politicians are often discussed in Russia, however, at the same time, such states as the USA, Canada, Russia or China develop programs or strategies of information operations with which they associate the state security or participation in future military conflicts.

The present article is aimed at shedding light on the impact that the information revolution had on the nature of military conflicts, on how these conflicts are understood by the USA and NATO, and on the means they will seek to ensure their security in such conflicts. Also, it is sought to look at what Lithuania could learn from these centres of military power.

The conception of information operations[2] generalises a new viewpoint of military conflict, which will be considered in this article in more detail. Lithuania has become a member of NATO. During the conflicts in Afghanistan and Iraq, Lithuania provided the USA and other NATO allies with the possibility to make use of its airspace and airports, if need be. Moreover, Lithuania sent an officer to the command post of the US military forces (CENTCOM), and some soldiers of the Special Forces, medical officers, and logistics specialists to participate in real military operations. Despite that, there is an impression that understanding is lacking among the experts on Lithuanian political sciences and war studies of what information warfare/information operations are, and in what way they influence the adoption of political and military decisions. The assumption is that information operations or defence against them is the prerogative of the great and wealthy powers. This assumption, however, is wrong, and this is proved by the example of Austria, which will be discussed in this article.

Hence, the objective of this article is not an attempt to prove that Lithuania should create a strategy, which is analogous to the USA strategy of information operations and allocate large financial resources to do that. This is not practical since Lithuania has become a member of NATO, it has gained the experience and standards of analogous operations from that defensive Alliance. On the contrary, the aim of the present paper is to reveal what the USA and NATO have achieved in this

---

[1] Baylis J., Smith S. eds., *The Globalization of World Politics*, Oxford: Oxford University Press, 1997, p. 554.

[2] Sometimes the term "information warfare" is used, however "information operations" is used in official US and NATO documents.

sphere and what Lithuania should take on in the sphere of state administration and policy. In the sphere of ensuring security of information technologies, Lithuania has taken the first steps – the State Strategy for Security of Information Technologies and the plan of measures of its implementation have already been approved. Meanwhile the current state policy of public information is uncoordinated – at the time of a military conflict our state would run onto considerable difficulties. Therefore, it is necessary to broaden experience in this sphere by learning from NATO.

1. Information Revolution and the International System

Many authors who try to generalise the picture of the international system after the Cold War, make a reservation, that a decade is too short a time period to determine if one or another state of this system has already settled into shape. It is common practice to present several scenarios: for example, the scenarios of Huntington; Fukujama; victory of the capitalist system; Pax Americana and the like. As long as chaos reigns in the international system, the right thing to do, in the opinion of Ian Clark, would be to characterise that period of international relations as "the beginning of a new historic era in which fragmentation is a dominant factor in international relations"[3]. The author draws this conclusion for two reasons: first, the period of systematic contrariety between the capitalist and communist poles came to an end with the end of the Cold War; second, this systematic contrariety neutralised or subjugated all other ethnic, national and religious aspirations for the benefit of one of the two poles. After the downfall of the bipolar system, all these forces became uncontrollable. Therefore, Ian Clark maintains that currently the basic task of experts on international relations is to establish the new axis of the conflict, and, contrary to the time of the Cold War, there might be many of them[4]. Within such a context it is of particular importance to elucidate what the role a modern state plays in ensuring the security of its citizens.

A number of authors emphasize that the importance of the sovereignty of the state in international relations is declining, that is, the assumption is made that the state is losing its monopoly of power. To a significant extent, this was caused by the information revolution – the state has lost its monopoly on information. This process was initiated by the Thatcher-Reagan telecommunications revolution.[5] A global process of deregulation[6] of the telecommunications sector had begun and as a consequence, the importance of corporations in the telecommunications sector in the international arena increased. John Baylis and Steve Smith maintain that the information revolution had several consequences for the participants in the international system[7].

---

[3] Clark I., *Globalization and Fragmentation: International Relations in The Twentieth Century*, Oxford: Oxford University Press, 1997, p. 172.
[4] *Ibid*, p. 174.
[5] Baylis J., Smith S., eds., p. 542 (note 1).
[6] In 1981, the British Law on Telecommunications was adopted, in 1984, the AT&T monopoly of US telecommunications was broken up.
[7] Baylis J., Smith S., eds., Op. cit, p. 549 (note 1).

First, a larger amount of information is accessible to the states and other participants in international relations, however, this has a positive effect only if this information is effectively processed and used, otherwise, the problem of information overload arises. Second, global channels of information allow decentralised management, which is used by transnational corporations, international organisations, even terrorist groups, whereas governance of the state is based on the mechanism of centralised decision making, therefore the states encounter serious difficulties in this sphere. Third, the monopoly of information control no longer exists, therefore the role of the mass media, that of world television companies in particular, increases. Fourth, the information revolution manifests itself in global transparency, that is, the problems, which earlier were considered to be the internal matter of states, become global problems which deepen the erosion of state sovereignty. M.E. Olsen and M.N. Marger draw the conclusion that the mass media, which is a main moulder and disseminator of information, has become one of the major power institutions in the international system due to the information revolution[8].

One should take into consideration, however, the fact that the information revolution provides the states with certain possibilities. In a global world, the state may consolidate its power not only by means of military or economic potential but also by means of communication based on the dissemination of culture. H.H. Frederick calls the states which carry out such a policy and make use of their power in this way, hegemonies.[9] While this is a very simplified use of the concept, in this case it perfectly defines US policy following the Cold War.

2. Information Revolution and Conflict

Hence, a state, seeking to ensure the security of its citizens, must change by adapting itself to the environment of global information. All modern armed forces invest big money in the sector of communications and information technologies. Military technology and strategy undergo changes. US military experts compare different strategies by presenting the following chart:

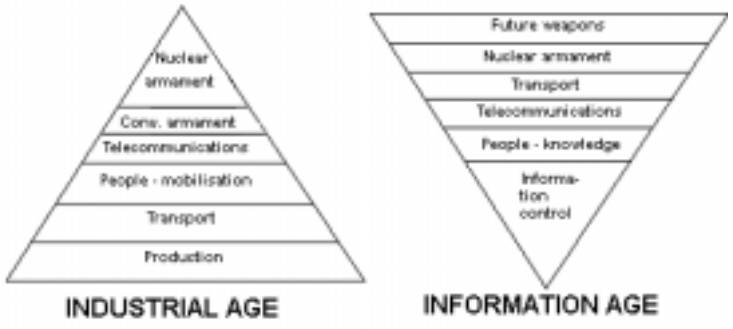

Chart 1. Pyramid of military strategies of the industrial age and information age[10]

[8] Olsen M. E., Marger M. N., eds., *Power in Modern Societies*, Westview Press, 1993, p. 238.
[9] Frederick H. H. *Global Communication and International Relations*, Belmont: Wadsworth Publishing Company, 1992, p. 205.

Control of information and an effective application of measures ensuring it plays a decisive role in the course of military conflicts that take place in the global information space.

The paradigmatic change currently taking place may be compared with the change that took place following the Treaty of Westphalia. Prior to the Thirty Year War there was no clear differentiation between a military campaign and mass banditism. Richard Mansbach and Edward Rhodes state that by means of the Treaty of Westphalia the leaders of the European states decided to restrict war and this determined the nature of future military conflicts[11]. Since then a distinction has been made between "legitimate" fighting carried out by professional soldiers against other soldiers (seeking to achieve political goals set by the heads of specific states) and "illegitimate" fighting – crimes against civilians and the internal order of a state. Hence, "a war was carried out by a specific group of individuals (professional soldiers), which is accountable to a specific authority (a sovereign state) basing itself on clearly defined rules, which limited the use of violence"[12]. Violence had become another political measure, which could be used by the monarchs of the European states when other measures failed to achieve desired goals. Such a conception of controlled violence formed the basis of the war theory of the Prussian officer Clausewitz. This strategist's statement about war as policy carried out by other means, and the conception of the war triangle developed by him, has formed Western civilisation's concept of a military conflict. At present, however, this conception is rapidly changing and it is likely to return to the pre-Westphalian conception of a military conflict, with crimes against civilians and the internal order of a state becoming the norm.

Preconditions for change appeared much earlier. According to Clausewitz's theory, the war triangle consists of: 1.) the heads of state who set political goals and control soldiers; 2.) soldiers who directly fight and are direct targets of violence; and 3.) the civilians who do not participate in a conflict but support the heads by paying taxes and backing political goals set by them, to the interrelated corners of the triangle. Clausewitz formulated the conception of a limited or controlled war. However, World Wars I and II, in the opinion of Richard Mansbach and Edward Rhodes, demonstrated how changes in military technology, the possibility to mobilise the entire economy of the state for military purposes, as well as how wide-spread nationalism, may destroy this theoretical

[10] "Report of the Defense Science Board Task Force on Information Warfare – Defense". *Defense Science Board*, 1996; "Report of the Defence Science Board Task Force on Information Warefare – Defence". – Defense Science Board, http://cryptome.org/iwdmain.htm, 1996. 06 09 2003

[11] Mansbach R., Rhodes E., eds., *Global Politics in a Changing World*, Boston: Houghton Mifflin, 2003, – p. 35.

[12] *Ibid*, p. 35.

triangle[13] . The world wars were total wars, where no difference was made between the soldiers and the civilians, and the heads of states could hardly control the processes of the conflict. During the Cold War, military technology was further developed; the USA and the Soviet Union created nuclear weapons. Looking at the period of the Cold War through the prism of Clausewitz's theories, one may suggest that a war between the superpowers became impossible because it would not be a rational policy carried out by other means. Nevertheless, limited military conflicts did take place during that period, e.g. Vietnam, Afghanistan. After the Cold War, military technology went on developing at an incredible pace; however, Lawrence Freedman and Efraim Karsh attribute the military conflict in the Persian Gulf to the type of limited wars[14] to which the conception of Clausewitz's war triangle is applied: the US authorities had a clear political goal – to drive the Iraq Forces away from Kuwait. Having achieved the first goal, the Bush Administration did not set another goal – to overthrow Sadam Hussein; precise blows delivered by the coalition may serve to illustrate the clear separation of soldiers from the civilians as emphasised by Clausewitz. Besides, not only the US public, but also the international community backed the actions of the coalition and became the third pillar.

However, this conflict already took place in a new environment, which experts from the USA, Canada and NATO call the global information space:

Chart 2. The place of military conflict in the global information space[15]

[13] *Ibid*.
[14] *Ibid*, p. 49.

The global information space is institutions, organisations and systems that are beyond the boundaries of a military conflict, but may still exert influence on the conflict itself. Earlier, this space was controlled exclusively by the states; however, in the age of information, any subject's intentions and actions may be significant to international relations. R.Garigue and T.Romet maintain that "all processes take place in the global information space, and it directly influences these processes"[16] . The mass media is the most influential player in this space and "may influence strategic trends and volumes of military operations"[17] at the time of military conflicts. However, non-governmental organisations, trans-national organisations, international organisations, individuals, other countries and their armed forces may not be less significant, provided they are able to efficiently control information in the global information space. Such international mass media corporations such as CNN and BBC, dominated that space in the past decade. However, at present Al-Jazeera and Al-Arabia television channels propagating Islamic culture and values lay claims to these positions. J. Chirac's initiative to establish the French analogue of CNN testifies to that important role that television plays in the global information space: "this is a legal aspiration of our country, and I would like it to be implemented; France must actively participate in a fight of filmed material, which is going on between the world televisions"[18] .

The importance of terrorism and radical religious or similar organisations have increased in this global environment. Their actions during a military conflict destroy the Clausewitz model that has prevailed thus far. John Keegan states that post-modern conflicts will be a characteristic of the age of information and the state must be prepared to solve them: "the conception of a post-modern war is destroying the understanding that wars are fought between the sovereign states when, with the help of violence, it is sought to consolidate the political will of one state against another state"[19] . A new conception of conflict reflects a trend in fragmentation of state sovereignty and political power. A war is no longer exceptionally a policy of the states carried out by other means; this may be the "policy" of terrorists. The possibility of controlling a conflict, which has been the responsibility of the states participating in a conflict, is clearly on the decline. A post-modern conflict no longer complies with other statements of the military triangle of Clausewitz either; a clear difference between soldiers and civilians no longer exists. Their role during a conflict is also changing. With terrorist organisations or radical religious groups getting involved in

[15] Garigue R., Romet T., "Information Warfare and the Canadian Forces", *National Defense, May 1996.* http://www.iwar.org.uk/iwar/resources/canada/iw_&_cf.pdf 06 09 2003
[16] *Ibid.*
[17] *Ibid.*
[18] Jacques Chirac proposes that a twenty-four-hour channel broadcasting the world news should be established http://www.delfi.lt/archive/index.php?id=1784033, 06 09 2003
[19] Mansbach R., Rhodes E. (Note 9) – p. 59.

international military conflicts, the executors of violence become impersonal "international terrorists". Furthermore, they choose civilians as "lawful" military targets. The role of these groups during a conflict also changes. First, political goals of the parties taking part in a conflict are no longer as clear or they are impossible to control. For example, if the aim of international terrorists is to fight against the USA and all of Western civilisation, how and when is their goal achieved? Second, during a conflict, Clausewitz assigned the civilians the role of providing material and ideological support to their state; at the time of earlier conflicts it was relatively simple to mobilise societies for pursuing the political goals of the state, however, the information revolution manifests itself by global transparency. Therefore, the essential problem is how to ensure internal and international support for political and military goals. Here it is useful to give the example of Lithuania during the war in Iraq. Lithuanian television viewers could watch military actions not only on international broadcasts of CNN or BBC, but also on AL-Jazeera, which was re-broadcast on local TV[20] .

3. The Role of the State in Ensuring the Security of its Citizens in the Information Age

Thus, within this new context of international relations and security, states review their preparedness for the participation in military conflicts of a new type and analyse measures whereby security of their citizens could be ensured. Andriu Latham supposes that "currently a revolution is going on in the military affairs when an industrial total war (World Wars I and II) is replaced by a war, which has plenty of names: 'information warfare', 'precision warfare', 'cyberwar'[21] ". Several factors determine such a paradigmatic change: improving military technology, especially, all that is related to the information revolution; the mass of armed forces, the number of which is decreasing due to new technologies[22] ; and the new security environment with its new threats being formed after the Cold War. However, the tradition of the USA, which is considered to be the leader of this revolution, to include new conceptions into strategic documents – doctrine – is of no less importance. Therefore, it does not only include theoretical considerations about future conflicts but also practical preparation of the Armed Forces to participate in them.

Andriu Latham maintains that the history of a war is marked by revolutionary changes: dramatic improvements in cannon/powder; the Napoleonic wars; the industrial total war, etc. Some authors count up to ten revolutionary stages of this type, others, like Toffler, speak about three revolutionary waves of wars: prior to the in-

---

[20] TV3 will broadcast material of "Al-Jazeera" channel http://www.delfi.lt/archive/index.php?id=2085167 06 09 2003

[21] Latham A. "Re–imagining Warfare: The "Revolution in Military Affairs"" in Snyder C.A. ed., *Contemporary Security and Strategy*, New York: Routledge, 1997, p. – 210. http://www.delfi.lt/archive/index.php?id=1869108 06 09 2003.

[22] Plans for the reform of the Lithuanian Armed Forces also provide for reducing the military reserve from 20 thousand to 7 thousand soldiers. The number of volunteers should also be reduced and the Lithuanian Armed Forces will be reorganised for collective defense

dustrial, industrial and information ones[23]. Dupuy, basing himself on the ratio of the change in speed to technology, states that there exist four periods, whereas Russian general and theoretician Slipchenko thinks that weapons of "the sixth generation"[24] were used in the Persian Gulf. However, it is more important to make clear why current changes in military matters are regarded as revolutionary ones rather than to elucidate which periodisation is the most accurate. Martin Show states that military conflicts of the past century were "total" for two reasons: first, during a conflict the states focused their main attention on total destruction; second, these conflicts distinguished themselves by total mobilisation of the society and state economy for military purposes[25]. When one looks at the conflicts in the Persian Gulf, Kosovo, Afghanistan and Iraq, the precision, rather than total nature of destruction, is striking. Another important aspect is that internal and international support of military actions is one of the essential guarantors of success in a conflict and achieving it requires great efforts – much greater then during total war. Andriu Latham thinks[26] that changes going on in military matters should be regarded as revolutionary ones for three reasons. First, the information revolution has altered the way information is collected, stored, conveyed and presented, that is, the speed of this process is approaching the zero limit. This allows one to speak about a virtual battlefield, and this, naturally, changes the decision-making process from that of hierarchical to a more decentralised one. Second, a mass destruction is replaced by a precision destruction, which leads to the reduction of the mass Armed Forces, that is, the need for professional, specialised armed forces arises. Third, the evolution of the threat discourse, that is, after the contrariety between the USA and the Soviet Union has disappeared, the new, already mentioned axes of the conflict come into existence.

The Institute of Strategic Studies under the Operations and Planning Department of the USA Armed Forces in its investigation "Military conflict in the 21st century: the information revolution and a post-modern war", states that currently the Armed Forces must be especially self-critical and at the same time must evaluate changes going on in global business: "today a successful and effective business organisation takes a global attitude towards business, has decentralised management, a network of strategic partnership all over the world and is flexible in taking the most important decisions"[27]. Corresponding changes should take place in the military sphere too. As has already been mentioned, the major factor in the age of information is effective control of information; therefore, the US Defense Department is convinced that the US Armed Forces must strive for information dominance in future military conflicts[28]. This principle is laid down in the Joint Doctrine for Information

[23] Toffler A. *War and anti–war: Survival at the Dawn of the Twenty–first Century*, 1993, 301 p.
[24] Bosch J.M.J., "Information Operations: Some Operational Reflections" in Bosch J.M.J., Luiijf H.A.M., Mollema A.R. eds. *Information Operations*, NLARMS, 1999, – p. 80.
[25] Latham A. Op. cit., p. 216 (note 19).
[26] Latham A. Op.cit., p. 220 (note 19).
[27] Metz S. *Armed Conflict in the 21st Century: the Information Revolution and Post–modern Warfare*, Strategic Studies Institute, 2000, p. vii.
[28] *Ibid*., p. x.

Operations. According to J.M.J. Bossch, "information operations do not only have an impact on the military sphere but also on the national, international and global political and economic strata and influence the states, unions and the international society"[29] and they may be used at different stages of the spectrum of a conflict:

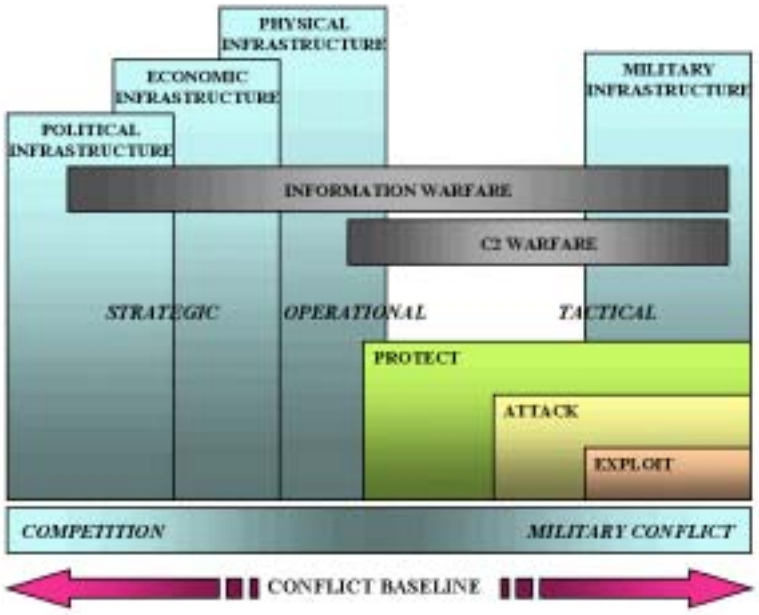

Chart 3. Spectrum of Conflict and Information Operations[30]

[29] Bosch J.M.J., Op. cit., p. 79 (note 21).
[30] Information Warfare Architecture http://www.herolibrary.org/iwarch.htm 06 09 2003

4. The US attitude towards Information Operations

The conception of information operations appeared for the first time in official USA documents in December, 1992, when the Defense Department approved Directive 36.00.1, where information operations are defined as: "military actions directed towards the global information space whereby it is sought to influence information or decision-making possibilities of an adversary"[31] . This definition evolved and its final version is presented in the Joint Doctrine for Information Operations approved on 9 October 1998: "information operations involve actions taken to affect adversary information and information systems while defending one's own information and information systems"[32] . It should be noted that in the military doctrine approved in the year 2000, Russia also regards information operations in the same way as does the USA: "information operations are information (information technical and information psychological) attacks directed against Russia or its allies"[33] , and in the same year, after the Doctrine for Information Security of Russia had been approved, Russia sought to protect itself from potential information attacks.

The US Joint Doctrine for Information Operations underlines that the use of information operations during a conflict is "an essential condition in seeking to achieve the objectives set"[34] . The Doctrine specifies that the measures mentioned must be applied at strategic, operational and tactical levels, irrespective of the intensity of a conflict; in military operations in times of peace, in crisis and in war[35] . This document covers offensive and defensive operations, their definitions, and the organisation of their use and management. Moreover, part of the document is devoted to the methodology of planning information operations and principles of co-ordination. Much attention is also paid to military training, exercising and simulation. The US Joint Doctrine for Information Operations should be regarded as the most exhaustive and essential military document devoted to this new sphere of future military conflicts:

---

[31] Bosch J.M.J. Op. cit. p. 91 (note 21)

[32] Joint Doctrine for Information Operations, 1998, www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf , 06 09 2003

[33] Военная доктрина Российской Федерации. – Совет Безопасности Российской Федерации. – 2000.04.21 http://www.scrf.gov.ru/Documents/Decree/2000/706-1.html 06 09 2003

[34] Joint Doctrine for Information Operations, p. vii (note 28).

[35] *Ibid*., p. II–7.

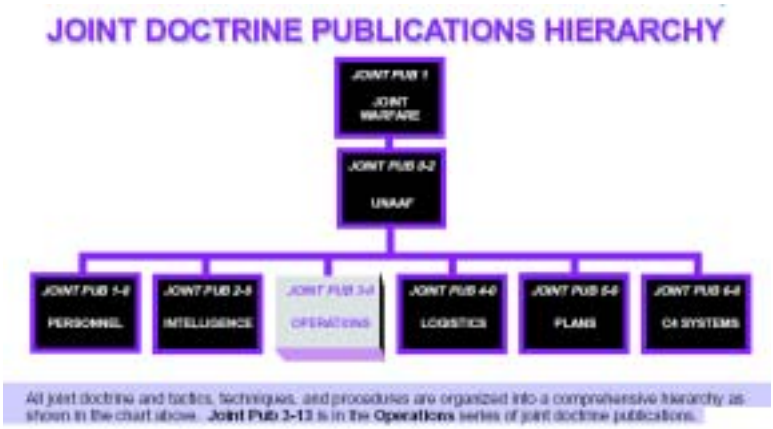

Chart 4. Place of the doctrine of information operations in the hierarchy of the USA joint doctrines[36]

Offensive information operations in the Doctrine, that is, "actions taken to affect adversary information and information systems", include the following: operational security, military deception, psychological operations, electronic war, physical attacks/destruction, special information operations[37]. Defensive information operations, that is, "actions aimed at defending one's own information and information systems", include the following: assurance of information, operational security, physical security, counter-deception, counter-propaganda, counter-espionage, an electronic war and special information operations.

In the Doctrine, the Chairman of the Joint Authority, who is "the main adviser to the Defense Secretary on the issues of information operations, is assigned the function of information operations management. He approves the plans of these operations, ensures continual practical exercises of information operations and the training of the military personnel"[38]. Military commanders "are responsible for direct planning and execution of information operations, as well as practical training"[39]. During a military conflict, the "cell" of information operations is entrusted with planning and simulation of information operations. It should be emphasised that the Doctrine contains future plans which reorganise the existing command and control "cell" into the "cell" of information operations[40]. Hence, in the future, US information operations will become the basis of the military strategy. They will combine the functions of command and control.

At the strategic level, the Doctrine provides for "the actions to be taken whereby an attempt will be made to make an effect on all the elements of the adversary's power (military, political, economic and information), at the same time protecting one's own elements of power, as well as those of the allies"[41]. At the operational level,

---

[36] *Ibid.,* p. GL–11.
[37] Doctrine does not provide the content of such operations.
[38] Joint Doctrine for Information Operations, p. I-6 (note 28).
[39] *Ibid.,* p. I–6.
[40] *Ibid.,* p. ix.
[41] *Ibid*., p. I–2.

information operations are used to achieve the objectives of the military campaign, and at the tactical level they are used to implement more concrete tactical goals[42]. The principles by which information operations must be carried out are laid down in the Doctrine: first, the basic target of these operations is the decision-making process of the adversary; second, the objectives of information operations must be clear and co-ordinated with national interests and general military goals; third, offensive measures must be selected according to the capabilities of the adversary and the possibilities of its response; fourth, it must be established in advance whether information operations are central, auxiliary or only partial offensive military measures; fifth, these operations must be fully integrated into all US military actions[43]. Attention should be given to the fact that the Doctrine specifies that at the strategic level, information operations must be based on the public information campaign and close co-operation with civil institutions and organisations. This is an essential aspect – the doctrine states that the success of information operations is determined by the co-operation of public information actions in the military and civil sphere. In the USA, the State Department, which centralised these functions after abolishing the USA Information Agency, is responsible for public information. This should become an example to Lithuania where the public information activities of separate governmental institutions or even ministries are, to put it mildly, uncoordinated. During a military conflict, such a lack of co-ordination could be destructive.

Targets of information operations may be very different: the authorities (civil, military, social cultural, etc.), the civil infrastructure (telecommunications, transport, energy, finances, production, etc.), the military infrastructure (communications, reconnaissance, logistics, etc.), military systems (aircraft, vessels, artillery, target armament, anti-aircraft defense, etc). Technology assures effective functioning of all these structures; therefore, it becomes the principal target. At the same time, however, one should remember that technology is not a means of carrying out certain actions, therefore the intelligence of humans will always remain the real target, and, to be more precise, the decision-making mechanism[44].

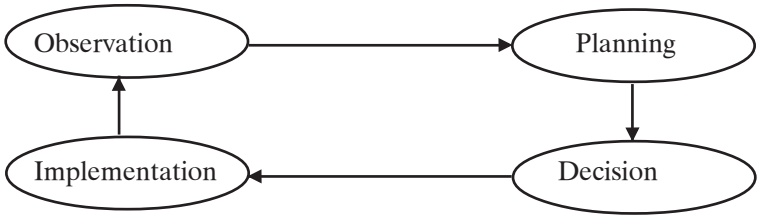

Chart 5. Decision-making cycle[45]

[42] *Ibid.,* p. I–3.
[43] *Ibid.,* p. II–1.
[44] Col John Boyd, USAF (Ret), coined the term and developed the concept of the "OODA Loop" (Observation, Orientation, Decision, Action)
[45] US Information Operations Field Manual FM 100–6. – Headquarters Department of the Army, Washington, DC, 27 August 1996. http://www.atsc-army.org/cgi-bin/atdl.dll/query/download/FM/100-6/fm100-6.zip, 06 09 2003

Taking into consideration the fact that special attention is devoted in the Doctrine to defense from information operations, operational security measures must determine the most vulnerable information or information systems and create mechanisms for their protection; measures of an electronic war must contribute to this defensive function; education and practical exercise must develop an understanding of information security for military and civilian personnel because the majority of information leaks are a consequence of the human factor; reconnaissance and counter-espionage must analyse and determine threats; counter-deception must mislead the adversary and divert its offensive attempts; counter-propaganda must expose the psychological operations of the adversary. Defense should comprise of four stages: the protection of an information environment; the determination of the source of the attack; the restoration of the functions and the response to the attack. The information environment in the Doctrine is a national information infrastructure consisting of private, governmental and military sectors. The Deputy Head of the National Security Department of the Civil Service Academy of Russia A.V. Vozzenikov, underlines that "a single national information infrastructure will be used as an effective resource, however, because of that it will become a potential target"[46] . Therefore, its protection is the primary objective. Besides, protection is also relatively cheaper, as compared with the costs of the other three stages of defense (determination of the source of the attack, the restoration of the functions, the response). Therefore, it is in this sphere that Lithuania must take advantage of other's experience, paying special attention to the achievements of smaller states, such as Austria, which will be discussed later.

5. NATO attitude towards Information Operations

The USA has always been a leader both in NATO military operations and in the maters of military strategy. Therefore it is not surprising that the NATO attitude towards information operations is nearly identical to that laid down in the US Joint Doctrine for International Operations. On January 22, 1999, the North Atlantic Council approved the strategy for NATO information operations. That document differed from the US Doctrine in that it focused special attention on the actions at the strategic level. This is reflected in the presented definition of information operations: "they are actions whereby, seeking to achieve political and military goals, decision makers are being influenced by effecting information and the information processes, management and control possibilities of the adversary, at the same time protecting their own"[47] . This definition, contrary to that of the USA, is not adapted to the exceptional military sphere. It deals with the effect on the decision makers without attributing them to either political, business or any other leaders, that is, NATO information operations are oriented towards the strategic level where it seeks to

[46] Колесникова Е. Что век грядущий нам готовит? http://www.nosorog.com/public/safety/prognoz.html, 06 09 2003

[47] Gardeta J., "Information Operations, the NATO Perspective" in Bosch J.M.J., Luiijf H.A.M., Mollema A.R., eds., *Information Operations*, NLARMS, 1999, p. 105.

assure support of its own actions during a conflict and at the same time to break down the willpower of the adversary. Jose Gardeta states that "at the strategic level by means of information operations it is sought to break down all the elements of the power of the adversary (political economic, military, information)"[48] . Therefore, public information and harmonisation of military and civil information actions in the NATO concept of information operations takes a much more significant place than that found in US Doctrine.

Like the USA, NATO accentuates information and information processes in the definition, however, it additionally singles out command and control. The concept of command and control in warfare is as old as military conflicts themselves. Eliminating the military command of the adversary has always been regarded as one of the main ways of achieving victory. The army, having lost its leadership, would not only be demoralised, but, what is most important, it would be unable to effectively organise and co-ordinate its actions. However, in the age of information, physical destruction is not necessary. It is enough to detach the command of the adversary from necessary information or to distort it, thus depriving it of the possibility to control.

NATO tactical publication ATP-3.2 presents the attitude of this organisation towards offensive information operations, though their definition accentuates the importance of defence from these operations. Offensive information operations are classified as follows: physical attacks against the command, control and communications; an electronic war; operational security; military deception and psychological operations. These measures are analogous to those laid down in the US Doctrine; however, they exclude special information operations for which the National Security Agency is responsible for in the USA. However, as has already been mentioned, a much greater attention in the NATO strategy is paid to public information and measures of civil and military co-operation than in the US Doctrine. This demonstrates NATO's focus on the strategic level rather than the operational or tactical levels of information operations. The function of public information is to ensure support of actions during times of conflict. In the above-mentioned Tactical Publication, public information is divided into military and political segments. The NATO authorities, which seek "to fully and objectively, to the extent the operational security allows, to present and explain to the public the achievements of the Alliance"[49] and thus ensure internal and international support of its actions, are responsible for the military segment of public information. The political segment of public information must be ensured by co-ordinated actions of all members of the Alliance. It is more directed towards assurance of international support. However, it is these actions that are most difficult to be implemented effectively due to a large number of states and because of the fact that responsibility for them rests with different institutions and organisations (military, political, non-governmental, etc.).

---

[48] *Ibid* – p. 106.

[49] ATP–3.2 Allied Tactical Publication "Information operations, Psichological Operations and Public Information" p. 3.

Organisation and planning of NATO information operations is also similar to that of the USA. There exists an analogous "cell" of information operations, a working group on NATO Information Operations[50] headed by the Director of the Operational Division of the International Military Personnel. This working group includes specialists with expertise in wartime command and control, psychological operations and other functions.

Though during the conflict NATO particularly accentuates actions at the strategic level, operational and tactical levels also have great significance. Jose Gardeta maintains that "at the operational level information operations supplement the basic measures of the military campaign and are directed towards the command, control, communications and logistics of the adversary, whereas at the tactical level they help achieve specific tactical tasks".[51]

The Allied Tactical Publication, like the US Doctrine, lays down principles on the basis of which information operations must be carried out[52]: first, leadership of the Commander, who is fully responsible for information operations; second, coordination of all actions and integration into joint military measures; third, accurate reconnaissance information, which must form the basis for information operations; fourth, all actions must be directed towards the adversary's "centre of gravity", that is, towards its most vulnerable points; fifth, information operations must rest on the principle of centralised planing and decentralised execution; sixth, the list of potential targets must be devised in detail; seventh, preparation for information operations must begin long before a military conflict itself starts, this is particularly applicable to defense from information attacks; eighth, in carrying out these measures flexibility and the ability to adapt to changing situations must dominate; ninth, the efficiency of measures applied must be constantly assessed.

Jose Gardeta summarised the attitude of NATO towards information operations by maintaining that "they may affect the core of the state, its infrastructure, the basic functions of its existence"[53]. Therefore, information operations fulfil a peculiar function of discouragement and "should be used in the time of peace seeking to prevent a crisis"[54]. However, this is a very complicated task due to the very nature of NATO. This organisation is a union of states, which often fails to find a common language on much simpler issues than information operations. NATO has no such unified willpower to use offensive or defensive information operations, which the USA has. Primarily, this is because information operations are a relatively new concept in the military strategy of NATO. Furthermore, it is copied from the US Joint Doctrine for Information Operations and it is not clear whether it fully complies with the defensive needs of the Alliance. Perhaps, most importantly, the Alliance consists of many states, which have a different viewpoint of the possibilities of using various means of information. Legal consequences are differently understood in the states;

---

[50] Gardeta J. (note 40) – p. 113.
[51] *Ibid*., p. 108.
[52] ATP–3.2 Allied Tactical Publication "Information operations, Psichological Operations and Public Information", p. 3–2
[53] Gardeta J. (note 40), p. 105.
[54] *Ibid* ., p. 105.

therefore, limitations differ on psychological operations, electronic war, computer hacking, etc. Furthermore, the success of information operations depends to a great extent on reconnaissance information, and the amount of such information available to NATO is equal to the amount of information provided by the states.

6. Military Conflict in the Information Age – What Lithuania Should Learn?

Lithuania lacks the options that are available to the USA and NATO to independently develop programs and strategies for information operations. However, this is not necessary because after Lithuania joined the North Atlantic Alliance, the country is having to transpose military standards of this defensive organisation and to adapt itself to its strategies and programs, including information operations. At present, two factors are essential. First, with Lithuania's NATO membership, one should take into consideration the fact that the Alliance concentrates its main attention on strategic information operations where public information plays the most significant role. Second, a discussion about the changing nature of a military conflict must be encouraged between military experts and experts on Lithuanian political sciences because the global information space has no boundaries, therefore the conflicts that take place within it are potentially threatening to Lithuania too. One should also raise the question of how it is possible to ensure the security of the citizens of the state, as well as the international security, in such a changing security environment. Therefore it is of particular importance to take care of information security in Lithuania.

6.1. Co-ordinated Public Information Strategy – a Key to Success

The Program for NATO information operations considers public information as one of the most essential components of different stages of a conflict or crisis, thru which it is possible to avoid a crisis, to discourage the adversary from taking certain actions, and in the event the conflict has occurred, to prove to internal and international public opinion the validity of one's actions. The Allied Tactical Publication defines public information as follows: "information, which is disseminated or published seeking to provide full information to the public thus ensuring its understanding and support"[55] . Public information in the US Joint Doctrine for Information Operations, as in the NATO Program, is divided into information intended for external and internal audiences. However, the NATO document distinguishes relatives and family members of soldiers as a separate audience and states that "priority will always be given to this audience"[56] . This is a very important aspect in such cases as the first Russian military campaign in Chechnya, where the local mass media devoted special attention to how victims and their family members suffered during that campaign.

[55] ATP–3.2 Allied Tactical Publication "Information operations, Psichological Operations and Public Information", p. 3–25
[56] *Ibid.,* p. 3–30

External public information is directed towards the mass media and, according to the NATO Document, should rest on the following principles: trust is the basis of everything – one must never lie to the mass media; each aspect of a military operation may have consequences of publicity; restricting information is becoming practically impossible, therefore it should be applied only for the sake of security; priority must not be given to one means of the mass media at the expense of others – information must be accessible to all under equal conditions; one must always try to provide information; not all news is good news, however, even bad news has its positive aspects (heroism of soldiers, provisions to help the wounded, etc.); the mass media is the main provider of information, therefore it forms a significant part of information operations; the public information campaign must be carried out throughout all stages of a conflict; media interest is not continual – sometimes it must be encouraged; NATO Forces cannot be separated from public information; journalists must be accredited by NATO[57] . Attention should be drawn to the fact that public information covers the entire spectrum of a conflict, from simple competition to military confrontation. NATO's program specifies that the Public Information officer, using a continual and uninterrupted link with the military authorities, is responsible for public information during a conflict.

This document, when discussing public information, accentuates once again the significance of the global information space. The essential conclusion is that information control and censorship have become practically impossible in the modern world and may do harm to political and military objectives. This has happened due to technological changes, the consequence of which is the separation and independence of military and private means of communication. In earlier military conflicts, in Vietnam for example, the mass media was also given an important role. However, at that time an attempt was made to control information provided to the journalists because their activity depended on whether the army provided them with the means of communication to enable their reporting or not. The appearance of portable computers, video telephones and other facilities made journalists independent of military technology. Therefore, to effectively carry out a public information campaign, NATO had to draw certain conclusions: first, the essential method of communicating with the mass media became "openness to the media and independent journalism"[58]; second, the thing that stopped to be surprising following the experiences of the military conflict in Iraq was the embedding of journalists into military units, seeking to develop certain emotional attachment to the soldiers and support for the tasks being carried out by them; third, announcements of the media may not be censored, irrespective of whether they are conveyed through private or official NATO communication channels; fourth, information security must be assured at the level of its source rather than at the level of the provider of information, the journalist. Hence, such words as "control" and "censorship", which were extremely important earlier, have disappeared from the strategy of public information.

[57] *Ibid.*
[58] *Ibid.*

Internal communications are a very important function in every organisation. It maintains the morale and resolve of the army's soldiers. The NATO means of internal public information involve internal newspapers, magazines, bulletins, radio, television, etc. Moreover, a safe, fast postal service and means for electronic mail are ensured to maintain contact between soldiers and their family members.

Another important aspect of public information is training and practical exercises for all representatives of NATO Forces, for both ordinary soldiers and officers. The Tactical Publication specifies that NATO personnel must participate in the courses "The Mass Media Today", "The Mass Media and the Human Rights", "How to Answer to the Journalists' Questions", "Security at the Level of the Source", and the managers of the personnel and officers must take part in the courses "Planning of a Meetings with Journalists", "How to Impart the News", "Principles of the Interview", and "Briefings"[59]

6.2. Information security and Lithuania's preparedness

Irrespective of Lithuania's membership in NATO, it is necessary for our country to ensure security of the national information infrastructure. Our Eastern neighbour could serve as an example: on September 9, 2000, the Doctrine for Information Security of the Russian Federation was approved, which is "the continuation of the National Security Conception in the sphere of information <...>, it forms the state policy in the sphere of information security, <...>, provides recommendations on how to improve the legal basis, <...>, encourages the creation of target information security programs"[60].

However, it would be more appropriate for Lithuania to base its information security program on that of another small European state – Austria. A.A.J. Forstner-Billau states that three interrelated layers form the national information infrastructure: private, federal (or governmental) and military information infrastructures. Seeking to achieve effective security, it is necessary to protect all of these infrastructures. The military infrastructure is always protected best because it is based on the implementation of uniform standards, requirements and training. Many countries try to adapt a similar policy to governmental information infrastructures. But, insecurity within the private infrastructure causes the greatest number of problems. "The national information infrastructure, which is the backbone of the modern society, is impermissibly violated by the criminals, terrorists or actions committed by the adversely-disposed countries"[61]. The US Joint Doctrine for Information Operations revealed the fact that the great powers invest large financial resources into this sphere, whereas smaller states may be classified into three groups: such states as Austria, which understand this problem and try to resolve it; the states which do not even understand this problem; and the states like Lithuania, which also fail to understand

[59] *Ibid.,* p. 3–31

[60] Доктрина информационной безопасности Российской Федерации. http://www.scrf.gov.ru/Documents/Decree/2000/09-09.html 06 09 2003

[61] Forstner–Billau A.A.J., Information Operations: Ideas for a Strategic Approach in a Small Country / Bosch J.M.J., Luiijf H.A.M., Mollema A.R. eds. Information Operations, NLARMS, 1999, – p. 231.

this problem, however, paradoxically as it might be, they solve this problem in part by copying the experience of foreign states.

These issues started to cause concern in Lithuania when, in preparing for European Union membership, it sought to transpose the measures of the "e–Europe" program, "to increase the security of the transactions being made through information technologies beginning with technological decisions and ending with the legal means"[62]. Furthermore, on November 23, 2001, based on the initiative of the European Union, 30 European states signed the convention in Hungary designed to suppress the increasing threat of electronic crimes, "On the basis of the Treaty, the undersigned states undertook to establish national permanently functioning centres providing mutual assistance on all the issues relating to computer crimes, beginning with computer hacking and embezzlements and ending with grave crimes posing a threat to life"[63]. In Lithuania, however, attention is focused exclusively on the state information structure.

The US Doctrine for Information Operations considers a military information infrastructure to be the best protected. However, because it is practically inseparable from the governmental and private information infrastructures, it is also vulnerable. The best characterisation of the vulnerability problem of the private infrastructure is given by A.A.J. Forstner-Billau: "in the past information technologies were implemented in business as single systems, which practically had nothing to do with other systems at all, and therefore not only technologies themselves differed but they also were incompatible – now it is sought consistently and continuously to resolve this problem"[64] and information technology companies earn big money for doing just that. Currently, developing businesses of the Eastern European states are introducing much more advanced technologies which must comply with general standards, including safety standards, because business logic demands doing so. A.A.J. Forstner-Billau thinks, however, that the process of protecting the private information infrastructure may be sped up: "it is necessary to draw high-quality information security products to the market, which are expensive and often unaffordable to a single business, therefore business of a small state should be attractive to investments of large corporations, and a part thereof would be allocated to information security"[65]

The problems, which governmental information infrastructures of small states encounter, are analogous to those faced by the private sector. Public administration information systems were created without being controlled – there were information systems of separate ministries and agencies which were not co-ordinated with one another. Resolving the problem of information security in the public administration sector has an essential advantage – there exists the possibility to entrust a specific institution and responsible officials with resolution of that problem. An agency has been established in the Federal Office of Austria to solve the issues of information technologies compatibility[66].

---

[62] IT security: security of state institutions http://www.ivpk.lt/main-aktual.php?cat=61&n=8 06 09 2003

[63] *Ibid.*

[64] Forstner–Billau A.A.J. Op cit., p. 231 (note 54).

[65] *Ibid.,* p. 233.

[66] *Ibid.,* p. 234.

In the year 2001, the Government of the Republic of Lithuania, in creating favourable conditions for the safe development of the information society and electronic government, authorised the Ministry of the Interior to co-ordinate information technologies security actions in the state sector. The Ministry devised the State Strategy for Security of Information Technologies and planned measures for its implementation by the year 2005. Both of these documents establish the principles of ensuring security measures requiring implementation, which include the development of the legal basis, preparation of recommendations and methodologies, training of specialists, strengthening security of the most important state information systems and education of the society[67]. According to the Director of the Information Policy Department of the Ministry of the Interior, Aurimas Matulis, "the Strategy underlines that security should be ensured in a complex way by introducing programme, technical, physical security and, of course, administration measures"[68]. Attention should be directed to the fact that the strategy emphasises the principle of information significance, which is one of the most essential ones in the USA and NATO concepts of information security. According to Aurimas Matulis, "security measures should comply with the value of the resources sought to be protected and possible consequences of their violation – it is not every system that needs maximum protection, therefore the security measures to be implemented are selected taking into account their importance and future security costs"[69]. Moreover, the Strategy provides other principles too: observation of the environment; the principle of interdependence of the information technology security systems and the information systems; and the principle of training users and specialists of information technologies[70]. The last principle is also accentuated in the US Joint Doctrine for Information Operations. It is of particular importance, since, according to Aurimas Matulis, "to a great extent – about 70 per cent – security of information technologies depend on the human factor and organisational processes, and only about 30 per cent – on technological facilities"[71].

To implement the above-mentioned Strategy, it is planned to allocate 3,2 million Lithuanian Litas (930,000 Euro) in the years 2002-2004. Furthermore, seeking to implement the security management principles at state institutions, the Government approved the General Requirements for Data Protection[72]. They establish that state institutions shall have to prepare and, upon co-ordination with the Ministry of

---

[67] Resolution No. 1623 of the Government of the Republic of Lithuania of 22 December 2001 On the Approval of the State Strategy for Information Technologies Safety and the Plan for its Implementation

[68] It is sought to ensure safety of information technologies it Lithuania http://www.vrm.lt/nuorodos/rvs/sp030108.htm 06 09 2003

[69] *Ibid.*

[70] Resolution No. 1623 of the Government of the Republic of Lithuania of 22 December 2001 On the Approval of the State Strategy for Information Technologies Safety and the Plan for its Implementation

[71] It is sought to ensure safety of information technologies it Lithuania http://www.vrm.lt/nuorodos/rvs/sp030108.htm 06 09 2003

[72] Resolution No. 2015 of the Government of the Republic of Lithuania of 31 December 2002 On data Protection in the State and Municipal Information Systems

the Interior, approve the security policy and ensure compliance with it in its activity. The requirements were co-ordinated with the Lithuanian Association of Municipalities; therefore, it has been recommended that local governments follow them[73].

Furthermore, according to Director Aurimas Matulis, "with Lithuania successfully integrating into NATO and the European Union, it is necessary to properly prepare for working together in the electronic space, to ensure the safe exchange of information between organisations of our country and international organisations, as well as between foreign countries"[74]. Therefore, the State Security Department, the Ministry of National Defence and the Ministry of the Interior jointly form the security system which will guarantee the safe processing, storing and transmission of electronic state secrets via computer networks. The work done by Lithuanian specialists in this sphere received positive evaluations from NATO and US experts.[75]

Conclusions

In the age of information, post-modern military conflicts will occur when states and other international relations actors seek to consolidate their policy in the global information space by force. These conflicts, however, will not resemble the Clausewitz model where leaders set political goals and control soldiers; soldiers fight directly and are lawful targets of violence; and the civilians do not participate in the conflict but support their leaders by paying taxes and backing their political goals. A conflict in the information age is a "pre-Westphalian" conflict where crimes against the civilians and the internal order of the state were the norm. But the means for achieving a victory will be the most modern ones.

The state must look for new means of ensuring the security of its citizens. The USA and other great powers suppose that information dominance on the global information space may ensure success in future conflicts, and this may be achieved by means of information operations. The means of public information, as well as coordination of information actions between military and civilian spheres are of paramount importance during these operations. NATO has devised such a strategy, therefore Lithuania, as a member of the alliance, should use this experience.

In the age of information, states associate their wellbeing with the programs of "the information society", "the knowledge-based society", "the electronic government", etc. However, information may serve not only as a means of production, but also forms the basis for destruction. Therefore, every state must devote particular attention to information security. Lithuania has already made the first steps in this sphere: the State Strategy for Security of Information Technologies and the plan of measures for its implementation until the year 2005 have already been devised. Nevertheless, there is much to be learned from the experience of Austria, a fellow member of NATO.

---

[73] It is sought to ensure safety of information technologies it Lithuania http://www.vrm.lt/nuorodos/rvs/sp030108.htm 06 09 2003

[74] *Ibid.*

[75] *Ibid.*