# NATO IN THE NEW STRATEGIC ENVIRONMENT: CYBER ATTACKS NOW COVERED BY ARTICLE 5 OF THE NORTH ATLANTIC TREATY


## Grzegorz Kostrzewa-Zorbas

Institute of Organisation and Management, Faculty of Cybernetics,
Military University of Technology, Warsaw, Poland



**Abstract.** The greatest change ever in the defence policy and military strategy of the North Atlantic Treaty Organisation occurred in 2014 in response to a series of major cyber attacks against NATO member states and partner states - Estonia in 2007, the United States and Georgia in 2008, and others in later years - and to a general transformation of the security environment in which cyberwar and other threats to cybersecurity gain rapidly in importance. At the 2014 Wales Summit, NATO recognised that cyber defence is part of its central task of collective defence and that Article 5 of the North Atlantic Treaty - "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all . . ." - can be invoked in the case of cyber attacks. This statement is the first and only expansion of the meaning of Article 5 and the first and only addition of a new type of warfare to the policy and strategy of NATO. After the change, the Alliance must face new challenges not less urgent and difficult than the old ones of kinetic warfare or weapons of mass destruction. This article addresses the broadest strategic context of the change. An analysis is made in the light of the global strategic thought and of the development of warfare through history. By entering the new strategic space of cyber warfare, NATO proves itself to be among the world's most modern and advanced powers while, at the same time, it returns to the ancient - and lasting - tenet of strategy: information is not inferior to force. This way the Alliance moves away from Carl von Clausewitz and closer to Sun Zi. The recognition of cyberspace as a strategic space also corresponds to another influential idea in the heritage of strategy: the concept of the "great common" the control of which is the key to the power over the world and over war and peace worldwide. Alfred Thayer Mahan considered the global ocean to be the "great common" crossed by vital trade routes and by navies competing for superiority. Now cyberspace is as open, vital and fragile as the maritime space was in Mahan's vision. Cyberwar also creates a promise and a temptation of a decisive strike - the first and last strike in a war - circumventing all military defences and paralysing the enemy country. It is a new version - less lethal or not, dependent on the tactics of cyber attacks in a cyber offensive - of the idea of strategic bombing and of the entire concept of air power, especially by its visionary Giulio Douhet, and then of nuclear strategy. Finally, the article provides two practical recommendations regarding the policy and structure of the North Atlantic Alliance in unfolding new era. Now NATO needs a speedy follow-on to the breakthrough decision of the Wales Summit. Cyber defence should be fully integrated into the next Strategic Concept which is expected in or around 2020 but could be worked out sooner because of the accelerating transition of the security environment. NATO should also consider establishing a global Cyber Command to maintain the initiative and to assure the credibility of the enlarged meaning of Article 5 of the North Atlantic Treaty. This credibility will be immediately, continuously and comprehensively tested by many players of the global game.

**Keywords:** NATO, North Atlantic Treaty, cyberdefence, cyberdefense, cybersecurity, cybernetics, information technology, cyberwar, cyber war, cyber warfare, information war, information warfare, cyberattack, cyber attack, cryptology, strategy, strategic concept, Poland, United States, USA, Estonia, Georgia, Sun Zi, Sun Tsu, Clausewitz, Mahan, Douhet, strategic bombardment, nuclear strategy

## 1. Introduction

The greatest change ever in the defence policy and military strategy of the North Atlantic Treaty Organisation occurred in 2014 in response to a series of major cyber attacks against NATO member states and partner states – Estonia in 2007, the United States and Georgia in 2008, and others in later years – and to a general transformation of the security environment in which cyberwar and other threats to cybersecurity gain rapidly in importance. At the 2014 Wales Summit, NATO recognised that cyber defence is part of its central task of collective defence and that Article 5 of the North Atlantic Treaty – "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all ..." – can be invoked in the case of cyber attacks. This statement is the first and only expansion of the meaning of Article 5 and the first and only addition of a new type of warfare to the policy and strategy of NATO. After the change, the Alliance must face new challenges not less urgent and difficult than the old ones of kinetic warfare or weapons of mass destruction.

This article addresses the broadest strategic context of the change. An analysis is made in the light of the global strategic thought and of the development of warfare through history. By entering the new strategic space of cyber warfare, NATO proves itself to be among the world's most modern and advanced powers while, at the same time, it returns to the ancient – and lasting – tenet of strategy: information is not inferior to force. This way the Alliance moves away from Carl von Clausewitz and closer to Sun Zi.

The recognition of cyberspace as a strategic space also corresponds to another influential idea in the heritage of strategy: the concept of the "great common" the control of which is the key to the power over the world and over war and peace worldwide. Alfred Thayer Mahan considered the global ocean to be the "great common" crossed by vital trade routes and by navies competing for superiority. Now cyberspace is as open, vital and fragile as the maritime space was in Mahan's vision.

Cyberwar also creates a promise and a temptation of a decisive strike – the first and last strike in a war – circumventing all military defences

and paralysing the enemy country. It is a new version – less lethal or not, dependent on the tactics of cyber attacks in a cyber offensive – of the idea of strategic bombing and of the entire concept of air power, especially by its visionary Giulio Douhet, and then of nuclear strategy.

Finally, the article provides two practical recommendations regarding the policy and structure of the North Atlantic Alliance in the unfolding new era. Now NATO needs a speedy follow-on to the breakthrough decision of the Wales Summit. Cyber defence should be fully integrated into the next Strategic Concept which is expected in or around 2020 but could be worked out sooner because of the accelerating transition of the security environment. NATO should also consider establishing a global Cyber Command to maintain the initiative and to assure the credibility of the enlarged meaning of Article 5 of the North Atlantic Treaty. This credibility will be immediately, continuously and comprehensively tested by many players of the global game.

## 2. A turning point in the history of NATO

NATO entered a new strategic era on 4–5 September 2014, when the North Atlantic Council, convened on the top level of Heads of State and Government at the Welsh seaport city of Newport in the United Kingdom, issued the *Wales Summit Declaration*. The breakthrough decision on cyber attacks and collective defence is stated and justified in paragraph 72 that also defines the international legal framework and outlines an Enhanced Cyber Defence Policy, whereas paragraph 73 lists several related concrete activities and actions of the Alliance, many of which began before the breakthrough and will be continued or enhanced after it:

> "72. As the Alliance looks to the future, cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging. To face this evolving challenge, we have endorsed an Enhanced Cyber Defence Policy, contributing to the fulfillment of the Alliance's core tasks. The policy reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence. It recalls that the fundamental cyber defence responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks. Our policy also recognises that international law, including international humanitarian law and the UN Charter,

applies in cyberspace. **Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis**.

73. We are committed to developing further our national cyber defence capabilities, and we will enhance the cyber security of national networks upon which NATO depends for its core tasks, in order to help make the Alliance resilient and fully protected. **Close bilateral and multinational cooperation plays a key role in enhancing the cyber defence capabilities of the Alliance. We will continue to integrate cyber defence into NATO operations and operational and contingency planning, and enhance information sharing and situational awareness among Allies. Strong partnerships play a key role in addressing cyber threats and risks. We will therefore continue to engage actively on cyber issues with relevant partner nations on a case-by-case basis and with other international organisations, including the EU, as agreed, and will intensify our cooperation with industry through a NATO Industry Cyber Partnership**. Technological innovations and expertise from the private sector are crucial to enable NATO and Allies to achieve the Enhanced Cyber Defence Policy's objectives. We will improve the level of NATO's cyber defence education, training, and exercise activities. We will develop the NATO cyber range capability, building, as a first step, on the Estonian cyber range capability, while taking into consideration the capabilities and requirements of the NATO CIS School [Communications and Information Systems School] and other NATO training and education bodies."[1]

The *Enhanced Cyber Defence Policy*, endorsed and outlined in paragraph 72 of the Wales Summit Declaration above, had already been approved

[1] Wales Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales, 4–5 September 2014 (emphasis added).
http://www.nato.int/cps/en/natohq/official_texts_112964.htm
Last accessed 21 December 2014.

by the defence ministers of the Alliance's member countries in Brussels on 3–4 June 2014. Its full content remains not public. Only three years earlier, in 2011, the original version – called *Defending the Networks: The NATO Policy on Cyber Defence* – had been prepared and announced on the order of NATO's 2010 Lisbon Summit[2].

Never before 2014 the North Atlantic Alliance devoted so much attention and energy to cyber defence. Its importance was recognised and appreciated at the Wales Summit even under the pressure of the gravest international security crisis in Europe since the Cold War: the Russian military aggression against Ukraine, the related threats to other NATO partners and to the Alliance itself, and the breakdown of many post-Cold War security standards and mechanisms. An effective short-term and long-term response to this dangerous crisis was – and is – rightly the first priority of the Alliance. Cyber defence, however, achieved a high position next to the top.

## 3. Back to the future: from Clausewitz to Sun Zi

The Western military philosophy and strategy developed through history far from the most influential strategic thinker in the world – Sun Zi (Sun Tsu in an older and still popular transcription) of ancient China. His treatise *The Art of War* is the most universally read and studied work on strategy. (All quotations from Sun Zi below are based on the classic and most popular English translation by Samuel B. Griffith [31].) By recognising and appreciating the major role of cyberspace in warfare and security, NATO becomes more modern and advanced, but also – paradoxically – closer to the ancient and classic global heritage of strategy. It was Sun Zi who underscored, at the very beginning of the recorded strategic thought, the centrality of information and intellect – not physical force:

> "Generally in war **the best policy is to take a state intact; to ruin it is inferior to this.** ...
>
> For to win one hundred victories in one hundred battles is not the acme of skill. **To subdue the enemy without fighting is the acme of skill.**

[2] North Atlantic Treaty Organisation, Defending the Networks: The NATO Policy on Cyber Defence, [Brussels:] 2011.
http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf
Last accessed 21 December 2014.

> Thus, what is **of supreme importance in war is to attack the enemy strategy.**" [31]

Sun Zi's recommendation "to attack the enemy strategy" has a very broad meaning. It includes knowing the strengths and weaknesses of the enemy, learning all the significant information the enemy possesses, and – even more ambitiously – taking over the control of the enemy's mind, especially the collective or institutional mind, like the authorities of a state or a coalition, or the command of a national or multinational military force. This is one of the maximum objectives, in offence or offensive defence, not only of intelligence activities – and, to a limited extent, of psychological operations – but also of cyber attacks and cyber campaigns, and of cryptology.

NATO's current shift contradicts some of the fundamental assumptions of the Western civilisation's most influential strategist and philosopher of war: Carl von Clausewitz of the 19th century Prussia. His treatise *On War* is regarded as the West's equivalent of Sun Zi's The Art of War. (All quotations from Clausewitz below are based on the scholarly English translation by Michael Howard and Peter Paret, based on a true version of the original, not distorted by ideologues of German militarism [3].) The "common heritage and civilisation of their peoples" – the safeguarding of which the NATO member states pledged in the Preamble to the North Atlantic Treaty – is evolving and adopting new ways to survive.

Clausewitz assumed, among others, the superiority of physical force over information and intellect, and the superiority of defence over attack – another dogma widely rejected in the world, especially today's world. He made the thesis on the centrality of physical force in warfare a part of the very definition of war:

> "**War is** . . . **an act of force** to compel our enemy to do our will.
> . . .
>
> **Combat is the only effective force in war; its aim is to destroy the enemy's forces as a means to a further end.** That holds good even if no actual fighting occurs, because the outcome rests on the assumption that if it came to fighting, the enemy would be destroyed. It follows that the destruction of the enemy's force underlies all military actions; all plans are ultimately based on it . . . **The decision by arms is for all major and minor operations in war what cash payment is in commerce. Regardless how complex the relationship between the two parties, regardless how rarely settlements actually occur, they can never be entirely absent.**" [3]

New means – cyber means – can achieve exactly the aim defined by Clausewitz above. Today – as the *Wales Summit Declaration* states or implies – "force" can be cyber power, "combat" can take place in the cyber space, and "arms" can be cyber weapons. Due to the rise of cyberwar – together with other global conditions – the Western civilisation is now learning from the strategic thought of the Far East. Cyberwar contributes this way to the convergence and globalisation of warfare and security.

## 4. The fifth strategic space – the decisive space?

Four strategic spaces emerged prior to cyberspace. In each of them, warfare takes place and wars can be decided. The first strategic space was the land, the second was the sea – which gained a central position during the era of global empires – and two more were added in the 20th century: the airspace and the outer space. Now in the 21st century, NATO contributes to the addition of the cyberspace. The current change in the Alliance's policy and strategy will probably resolve the present worldwide dispute whether cyberspace – or information space – plays an autonomous strategic role. Even more spaces compete, or will likely compete in the near future, for a similar recognition. After cyberspace proper, the next debate will probably be about the mind space: an extension of cyberspace into the human minds, with electronic, photonic and other artificial devices integrated with the brain and the nervous system of humans. Then may come the biospace: biological and especially genetic space, controlled and engineered by advanced biotechnology. All these spaces – actual or potential – are also called "the domains of warfare," cyberspace becoming the fifth actual domain. Always an important question arises if a single space or domain is decisive – if a strategic advantage in it guarantees a strategic advantage everywhere, and therefore a war victory.

A wider change in the strategic thinking of the nations of the West and of the whole world preceded NATO's shift and accelerates following it. Cyberwar had prominently appeared in general national security strategies and national defence (military) strategies – besides specialised national cyber security strategies – of many NATO members and partners, and other nations, in the early 21st century, expanding exponentially after around 2010. (An exponential growth is clearly visible in a selection of official strategic documents provided in the "Sources" section below.) This cyberwar tsunami resembles the rise of the air power idea and practice in 1914–1918 – during the First World War.

The then rising air forces and air strategists quickly made a bold promise that air power alone can and will win major wars, by the means of strategic bombing. The boldest and purest visions were developed by the Italian strategist Giulio Douhet in *The Command of the Air of 1921* [10]. Before the era of nuclear weapons, he already envisioned an equivalent to the nuclear first strike – a single strike deciding the result of a whole war. Douhet proposed the employment of a combination of conventional and chemical weapons. Not the destructive force of explosives and toxins, however, but the uniqueness of the new strategic space justified the promise. The appeal of the new dimension, freedom and independence unique to airspace resembled the appeal of cyberspace today:

> "**The airplane has complete freedom of action and direction**; it can fly to and from any point of the compass in the shortest time .... Nothing man can do on the surface of the earth can interfere with a plane in flight, moving freely in the third dimension. **All the influences that have conditioned and characterized warfare from the beginning are powerless to affect aerial action**. By virtue of this new weapon, the repercussions of war are no longer limited by the farthest artillery range of surface guns, but can be directly felt for hundreds and hundreds of miles over all the lands and seas of nations at war. No longer can areas exist in which life can be lived in safety and tranquillity, nor can the battlefield any longer be limited to actual combatants.
>
> ... both the army and navy may well possess aerial means to aid and integrate their respective military and naval operations; but that does not preclude the possibility, the practicability, even the necessity, of having **an air force capable of accomplishing war missions solely with its own means**, to the complete exclusion of both army and navy.
>
> ... the decision in this kind of war must depend upon smashing the material and moral resources of a people caught up in a frightful cataclysm which haunts them everywhere without cease until the final collapse of all social organization. Mercifully, **the decision will be quick** ... since the decisive blows will be directed at civilians, that element of the countries at war least able to sustain them.
>
> A complete breakdown of the social structure cannot but take place in a country subject to . . . merciless pounding from the air

> ... to put an end to horror and suffering, the people themselves, driven by the instinct of self-preservation, would rise up and demand **an end to the war – this before their army and navy had time to mobilize** at all!" [10]

Douhet did not call for aggressive wars but advocated offensive defence similar to the later concept of nuclear retaliation. The promise of decisiveness of airspace was tested before and during the Second World War with mixed and uncertain results. Cyber campaigns – for offence or defence, to break peace or to restore peace – can now also be based on a newer and more complex air power concept that replaced strategic bombing: the concept of air campaign, best formulated by John A. Warden of the United States Air Force in *The Air Campaign: Planning for Combat*, first published in 1988 and revised in 1998 in the light of new experiences [34].

Another promise of decisiveness appeared at the end of the Second World War and during the Cold War with the conquest of outer space, the invention of nuclear weapons and the building of missiles flying through outer space and supported by outer space-based intelligence, reconnaissance, communications and other assets [11]. Indeed, the Cold War did not turn into a global hot war, but the cause and effect relationship is uncertain. The cyberwar concepts of retaliation and deterrence, however, correspond more to nuclear than conventional military strategy. According to many nuclear strategists and theorists of international relations, nuclear weapons are "equalisers" of states in warfare and therefore politics. The international game becomes more democratic with nuclear proliferation [29]. Small states and non-state players – like terrorist organisations – can advance to the rank of major players due to the possession of even minor nuclear arsenals.

All these ideas spread from the classic nuclear thought to the developing cyber thought. The pro-Western Israel and the anti-Western North Korea may serve as perfect examples of small states that became big players in both nuclear and cyber warfare. Estonia – a very small state in an extremely difficult local geostrategic environment – strives to be a cyber fortress for the West. Private groups armed with cyber weapons may fight like equals with a superpower nation of the United States and with the strongest alliance on Earth – the North Atlantic Alliance. Or they may take revenge on China and Russia for aggressive military actions or for human rights abuses.

Maritime superiority is the decisive step to the power over the world according to the American strategist Alfred Thayer Mahan in *The Influence of Sea Power Upon History*, first published in 1890 [19]. Mahan's

explanation of the key role of the global ocean in the life of humankind can be directly applied to cyberspace with an analogous conclusion on world hegemony. Today the open Internet and other large components of the global cyberspace constitute a new "great common" or "wide common" like the original one:

> "**The first and most obvious light in which the sea presents itself from the political and social point of view is that of a great highway; or better, perhaps, of a wide common, over which men may pass in all directions**, but on which some well-worn paths show that controlling reasons have led them to choose certain lines of travel rather than others. These lines of travel are called **trade routes**; and the reasons which have determined them are to be sought in the history of the world.
>
> . . . it is the possession of that overbearing power on the sea which drives the enemy's flag from it, or allows it to appear only as a fugitive; and which, by controlling the great common, closes the highways by which commerce moves to and from the enemy's shores. This overbearing power can only be exercised by great navies . . ." [19]

Countries and civilisations, and the economic, political and military life of the world, are becoming even more concentrated around cyberspace – and more dependent on it – than around the global ocean. NATO can, thanks to its strong maritime foundation – beside the nuclear one – easily understand and appreciate cyberspace as an additional strategic priority for the 21st century. No other entity is both willing and able to keep the new great common open.

## 5. The first ever addition of a new type of warfare to NATO's strategy

Nuclear weapons and nuclear warfare were present in the strategy of NATO from its very beginning. Immediately after the signing of the North Atlantic Treaty on 4 April 1949 and its entry into force on 24 August 1949, the Alliance developed *The Strategic Concept for the Defense of the North Atlantic Area* – secret at that time, declassified only after the Cold War [21]. On 29 August 1949, the Soviet Union conducted its first nuclear weapon test, revealed to the world by the United States on 23 September 1949. The first *Strategic Concept* was drafted

by the Alliance's military authorities in the fall of 1949 and finally approved by the North Atlantic Council on 6 January 1950. NATO planned to use all available means in all then existing strategic spaces or domains:

> "IV MILITARY MEASURES
> TO IMPLEMENT DEFENSE CONCEPT
>
> Basic Undertakings
>
> 7. Over-all defense plans must provide in advance of war emergency, specifically for the following basic undertakings in furtherance of the common objective to defend the North Atlantic area. The successful conduct of these undertakings should be assured by close coordination of military action as set forth in over-all plans.
>
> **(a) Insure the ability to carry out strategic bombing promptly by all means possible with all types of weapons, without exception**. This is primarily a U.S. responsibility assisted as practicable by other nations.
>
> (b) Arrest and counter as soon as practicable the enemy offensives against North Atlantic Treaty powers by all means available, including **air, naval, land and psychological** operations. . . "[3].

The expression "all types of weapons, without exception" meant first of all "the atomic bomb" as stated in drafts since October 1949. Diplomats then agreed to change the explicit wording with no change of the intended meaning[4].

[3] The Strategic Concept for the Defense of the North Atlantic Area, approved by the North Atlantic Defense Committee on 1 December 1949, [approved by the North Atlantic Council on 6 January 1950,] in NATO Strategy Documents 1949-1969, Edited by Dr. Gregory W. Pedlow, Chief, Historical Office, Supreme Headquarters Allied Powers Europe, in Collaboration with NATO International Staff Central Archives, [Brussels: North Atlantic Treaty Organisation, 1997], pp. 5–6 (emphasis added).
http://www.nato.int/docu/stratdoc/eng/a491201a.pdf
Last accessed 21 December 2014.

[4] Gregory W. Pedlow, "The Evolution of NATO Strategy 1949-1969," in NATO Strategy Documents 1949-1969, Edited by Dr. Gregory W. Pedlow, Chief, Historical Office, Supreme Headquarters Allied Powers Europe, in Collaboration with NATO International Staff Central Archives, [Brussels: North Atlantic Treaty Organisation, 1997], pp. XI-XIII.
http://www.nato.int/docu/stratdoc/eng/intro.pdf
Last accessed 21 December 2014.

Therefore, the current inclusion of cyber attacks and cyber defence into the extent of collective defence is the first ever addition of a new type of warfare to the responsibility and strategy of NATO, dominated earlier by kinetic warfare and nuclear, chemical and biological weapons of mass destruction. Preoccupied with weapons based on chemical, thermal, nuclear, electromagnetic and kinetic energy, and on radioactive, chemical and biological agents, the Alliance tended to underestimate the information dimension of warfare. Now the balance is restored. One of the reasons for this breakthrough was the force multiplier capability of information. Another – the interaction of cyberspace with physical reality. A cyber weapon can release kinetic and other energy from the military arsenal and other resources of an attacked state or alliance. Cyberspace is autonomous but interconnected with all the other strategic spaces.

## 6. Cyberwar is an integral part of warfare in general

There are two different major components to the breakthrough of the Wales Summit. First, the openly stated recognition that cyber attacks can be armed attacks. Second, the implied recognition that cyberwar is not a detached kind and field of warfare but an integral part of warfare in general. Cyberwar remains distinct and autonomous like naval warfare or air warfare. Strong connections and interactions exist, however, between cyberspace and the sea, airspace, outer space and land.

Whoever launches cyber attacks on NATO or its member countries, cannot count on an exclusively cyber nature of the Alliance's reaction. A combat response can come through any strategic space, with any kind of weapons under the condition of proportionality. Cyberspace ceased to be a sanctuary for cyber warriors. All warriors are now equal under the law and in operational plans.

## 7. Recommendation 1: Next Strategic Concept sooner than around 2020

NATO needs to quickly and fully integrate cyber warfare, cyber defence and cyber weapons into its *Strategic Concept*. There is a regular cycle of revisions approximately every ten years, but Wales Summit breakthrough justifies an exception. The work could and should be completed in about two or three years from now.

Because of the ethical and legal novelty and complexity of the matter, NATO should also clearly define the necessary political, humanitarian and

international law guidelines and limitations of cyber defence. This can be accomplished, in part, with the use of the already published half-official *Tallinn Manual on the International Law Applicable to Cyber Warfare* [32].

## 8. Recommendation 2: NATO Cyber Command

Cyber defence requires the establishment of a NATO Cyber Command with a global reach and on the highest reasonable level: directly under Allied Command Operations. All the structural innovations outlined in paragraph 73 of the *Wales Summit Declaration* may not prove sufficient in the coming years. The existing Cyber Defence Committee – known as the Defence Policy and Planning Committee (Cyber Defence) before April 2014 – and the NATO Cooperative Cyber Defence Centre of Excellence established in Tallinn, Estonia have responsibilities different from a command. So will have a NATO military cyber training centre planned also in Tallinn.

"In a chosen country of Central Europe, NATO should create a new – corresponding to new challenges – headquarters with tasks covering the whole of Europe or the world. It should be a battle command directly subordinated to the Allied Command Operations, ACO, in Mons, Belgium. The most justified choice would be a European missile and air defense command or **a global cyberwar command**" – I suggested before the Wales Summit [15]. Not another research, planning or training institution, but a combat command is indeed necessary to fully implement the *Wales Summit Declaration*. Among the Central European member countries, Poland has the greatest potential to host and support a NATO Cyber Command. A major asset within this potential is the Military University of Technology in Warsaw – the largest military research and teaching university in the European part of NATO and in the entire European Union.

Within NATO, the United States was the first member country to create a combat cyber command. Established in 2009 and fully operational since 2010, the United States Cyber Command (USCYBERCOM), located at Fort George G. Meade in Maryland near Annapolis and Washington, DC, is a Subordinate Unified Command under the United States Strategic Command (USSTRATCOM), a top-level Functional Combatant Command. The Netherlands was the first European member nation that followed – in the year of the Wales Summit. Outside of the Alliance, two states – Israel and Russia – are preparing their cyber commands, while India is considering a similar plan.

## 9. Conclusions

Today the North Atlantic Alliance needs a visible credibility of its defence policy and military strategy expanded into cyber defence at the Wales Summit of 2014. The *Wales Summit Declaration* includes the first and only expansion of the meaning of Article 5 of the North Atlantic Treaty and the first and only addition of a new type of warfare to the policy and strategy of the Alliance in its 65 years of history. Credibility can be assured by maintaining the initiative, especially by follow-on conceptual and organisational moves: integrating cyber defence into the NATO *Strategic Concept* and by establishing a NATO Cyber Command. Initiative is a universal strategic principle, although Clausewitz never appreciated it:

> "Tactical initiative can rarely be expanded into a major victory, but a strategic one has often brought the whole war to an end at a stroke. On the other hand, the use of this device assumes *major, decisive and exceptional* mistakes on the enemy's part" [3].

The perfectly stable and predictable world of Clausewitz no longer exists, if it ever existed. Losing the initiative in cyber warfare would be a *major, decisive and exceptional* mistake on NATO's part. Sun Zi sounds much more convincing on both the unpredictable and the speed in warfare:

> "Generally, in battle, use the normal force to engage; use the extraordinary to win...
>
> Speed is the essence of war" [31].

Speed is, in particular, the essence of cyberwar. Speed is also the essence of cyber defence and cyber security, and of the cyber peace the North Atlantic Alliance decided to guarantee.

## 10. Sources

### 10.1 Current Documents

[Australia.] Australian Government. Cyber Security Strategy. [Canberra:] 2009.
http ://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20 − %20for%20website.pdf

[Australia.] Australian Government, Department of Defence. Defence White Paper 2013. [Canberra:] 2013.

http : //www.nationalsecurity.gov.au/Mediaandpublications/Publications /Pages/dafault.aspx#_dwp

[Australia.] Australian Government, Department of the Prime Minister and Cabinet. Strong and Secure: A Strategy for Australia's National Security. [Canberra:] 2013.
http : //apo.org.au/files/Resource/dpmc_nationalsecuritystrategy _jan2013.pdf

[Canada.] [Ministry of] National Defence. Canada First Defence Strategy. [Ottawa:] 2008.
http : //www.forces.gc.ca/assets/FORCES_Internet/docs/en/about /CFDS − SDCD − eng.pdf

[Canada.] Government of Canada. Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada. [Ottawa:] 2010.
http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy /index-eng.aspx

[Estonia.] Ministry of Economic Affairs and Communication. Cyber Security Strategy 2014-2017. [Tallinn:] 2014.
https : //www.mkm.ee/sites/default/files/cyber_security_strategy_2014 −2017_public_version.pdf

[Estonia.] Estonian Ministry of Defence. National Defence Strategy [of] Estonia. [Tallinn:] 2011.
http : //www.kaitseministeerium.ee/files/kmin/img/files/KM_riigikaitse _strateegia_eng%282%29.pdf

[Estonia.] Parliament of Estonia. National Security Concept of Estonia. [Tallinn:] 12 May 2010.
http : //www.kaitseministeerium.ee/files/kmin/img/files/National _Security_Concept_of_Estonia.pdf

[European Union.] European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, 7 February 2013.
http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan -protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[European Union.] European Commission. Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the

Union. Brussels, 7 February 2013.
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN

[France.] Republic of France. Minister of Defence. Defence and National Security 2013: Twelve Key Points. White Paper. [Paris: 2013.]
www.defense.gouv.fr/content/download/207914/2305785/file/LB-fiche%2012pts-UK.pdf

[France.] Republic of France. Prime Minister; French Network and Information Security Agency. Information Systems Defence and Security: France's Strategy. Paris: February 2011.
http : //www.ssi.gouv.fr/IMG/pdf/2011 − 02 − 15_Information_system_defence_and_security_ − _France_s_strategy.pdf

[Germany.] Cyber Security Strategy for Germany. Berlin: Federal Ministry of the Interior, February 2011.
https : //www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob = publicationFile

[Germany.] German Ministry of Defence. Defence Policy Guidelines: Safeguarding National Interests – Assuming International Responsibility – Shaping Security Together. Berlin, 27 May 2011.
www.bmvg.de/resource/resource/MzEzNTM4MmUzMzMyMmUzMTM1MzMyZTM2MzIzMDMwMzAzMDMwMzAzMDY3NmY2ODMyNjEzMTc2NjgyMDIwMjAyMDIw/110527%20VPR%20engl.pdf

[Japan.] Information Security Policy Council. Cybersecurity Strategy: Towards a World-leading, Resilient and Vigorous Cyberspace. [Tokyo:] 10 June 2013.
http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf

[Japan.] Ministry of Defense. Defense of Japan 2014. [Tokyo:] 2014.
http : //www.mod.go.jp/e/publ/w_paper/2014.html

[Japan.] Government of Japan. National Security Strategy. [Tokyo:] 17 December 2013.
http://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-e.pdf

[Netherlands] Ministry of Defence. The Defence Cyber Strategy. [The Hague: 27 June 2012.]
https : //ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf

[Netherlands] [Government of the Netherlands.] International Security Strategy: A Secure Netherlands in a Secure World. [The Hague: 21 June 2013.]
http://www.government.nl/news/2013/06/21/a-secure-netherlands-in-a-secure-world.html

[Netherlands] National Coordinator for Security and Counterterrorism. National Cyber Security Strategy 2: From Awareness to Capability. [The Hague: 2013.]
https://english.nctv.nl/Images/national-cyber-security-strategy-2_tcm92-520278.pdf

[Netherlands] Ministry of Defence. Netherlands Defence Doctrine. [The Hague: 20 November 2013.]
www.defensie.nl/binaries/defence/documents/publications/2013/11/20/defence-doctrine-en/defensie-doctrine_en.pdf

[North Atlantic Treaty Organisation.] Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon [19–20 November 2010].
http : //www.nato.int/cps/en/natolive/official_texts_68580.htm

[North Atlantic Treaty Organisation.] Wales Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales, 4–5 September 2014.
http : //www.nato.int/cps/en/natohq/official_texts_112964.htm

[Poland.] Republic of Poland. Ministry of Administration and Digitisation and Internal Security Agency. Cyberspace Protection Policy of the Republic of Poland. Warsaw, 25 June 2013.
www.cert.gov.pl/download/3/162/PolitykaOchronyCyberprzestrzeniRP148x210wersjaang.pdf

[Poland.] Ministry of National Defence. Defence Strategy of the Republic of Poland. Sector Strategy of the National Security Strategy of the Republic of Poland. Warsaw: 2009.
http://en.mon.gov.pl/z/pliki/dokumenty/rozne/2014/02/strategia_obronnosci_eng.pdf

[Poland.] President of the Republic of Poland. National Security Strategy of The Republic of Poland. Warsaw: 5 November 2014.
http://www.bbn.gov.pl/ftp/dok/NSS_RP.pdf

[United Kingdom of Great Britain and Northern Ireland.] HM Government. A Strong Britain in an Age of Uncertainty: The National Security Strategy. London: October 2010.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

[United Kingdom of Great Britain and Northern Ireland.] The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World. London: Cabinet Office, November 2011.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

[United States of America.] Department of Defense. Department of Defense Strategy for Operating in Cyberspace. [Washington, DC: The Pentagon, July 2011.]
http://www.defense.gov/news/d20110714cyber.pdf

[United States of America.] President of the United States. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Washington, DC: The White House, May 2011.
http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[United States of America.] President of the United States. National Security Strategy. Washington, DC: The White House, May 2010.
http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

[United States of America.] Department of Defense. Quadrennial Defense Review 2014. [Washington, DC: The Pentagon, 2014.]
http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf

[United States of America.] Department of Defense. Sustaining U.S. Global Leadership: Priorities for 21st Century Defense. [Washington, DC: The Pentagon, January 2012.]
http://www.defense.gov/news/Defense_Strategic_Guidance.pdf

## References

[1] R. Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", *Journal of Conflict and Security Law*, (Oxford, UK: Oxford University Press), Vol. 17, Issue 2 (Summer 2012).

[2] S.J. Cimbala, *Nuclear Weapons in the Information Age*, New York: Continuum International Publishing Group, 2012.
[3] C. von Clausewitz, *On War*, Edited and Translated by Michael Howard and Peter Paret, Princeton, NJ: Princeton University Press, 1984.
[4] E. A. Cohen, "Technology and Warfare", In *Strategy in the Contemporary World: An Introduction to Strategic Studies*, Edited by John Baylis, James J. Wirtz, and C.S. Gray, 4th Edition, Oxford, UK: Oxford University Press, 2013.
[5] *Cyberpower and National Security*, Edited by F.D. Kramer, S.H. Starr, and L.K. Wentz, Washington, DC: National Defense University Press; Potomac Books, 2009.
[6] *Cyberwar, Netwar and the Revolution in Military Affairs* Edited by E. Halpin, P. Trevorrow, D. Webb, and S. Wright, Houndmills, Basingstoke, Hampshire, UK: Palgrave Macmillan, 2006.
[7] *Cyberwar and Information Warfare* Edited by Daniel Ventre, London: ISTE, 2011.
[8] C.C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*, Athens, GA: University of Georgia Press, 2011.
[9] H.H. Dinniss, *Cyber Warfare and the Laws of War*, New York: Cambridge University Press, 2012.
[10] G. Douhet, *The Command of the Air*, Translated by D. Ferrari, Washington, DC: Office of Air Force History, 1983.
[11] L. Freedman, *The Evolution of Nuclear Strategy*, 3rd Edition, Houndmills, Basingstoke, Hampshire, UK: Palgrave Macmillan, 2003.
[12] W.T. Hagestad, *21st century Chinese Cyberwarfare: An Examination of the Chinese Cyberthreat from Fundamentals of Communist Policy Regarding Information Warfare through the Broad Range of Military, Civilian and Commercially Supported Cyberattack Threat Vectors*, Ely, Cambridgeshire, UK: IT Governance Publishing, 2012.
[13] L.J. Janczewski and A.M. Colarik (Editors), *Cyber Warfare and Cyber Terrorism*, Hershey, PA: IGI Global, 2007.
[14] L. Kello. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", *International Security*, Vol. 38, No. 2 (Fall 2013).
[15] G. Kostrzewa-Zorbas, "A Plan for NATO: Central Europe Indistinguishable from Western Europe", *Aspen Review Central Europe* (Prague, Czech Republic), No. 2/2014.
[16] A. Kott, C. Wang, and R.F. Erbacher (Editors), *Cyber Defense and Situational Awareness*, New York, NY: Springer Science+Business Media, 2014.

[17] M.C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, New York: Cambridge University Press, 2007.
[18] M.C. Libicki, *Cyberdeterrence and Cyberwar* Santa Monica, CA: RAND Corporation, 2009.
[19] A.T. Mahan, *The Influence of Sea Power Upon History, 1660–1783*, New York: Dover Publications, 1987.
[20] *National Cyber Security Framework Manual* Edited by A. Klimburg, Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012.
[21] *NATO Strategy Documents 1949–1969*. Edited by Dr. G.W. Pedlow, Chief, Historical Office, Supreme Headquarters Allied Powers Europe, in Collaboration with NATO International Staff Central Archives. [Brussels: North Atlantic Treaty Organisation, 1997.]
[22] M.E. O'Connell, "Cyber Security without Cyber War", *Journal of Conflict and Security Law* (Oxford, UK: Oxford University Press), Vol. 17, Issue 2 (Summer 2012).
[23] W.A. Owens, K.W. Dam, and H.S. Lin (Editors), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, National Research Council of the National Academies, Washington, DC: National Academies Press, 2009.
[24] C. Paul, I.R. Porche, and E. Axelband, *The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces*, Santa Monica, CA: RAND Corporation, 2014.
[25] D.S. Reveron (Editor), *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, Washington, DC: Georgetown University Press, 2012.
[26] J. Rivera, "A Theory of Cyberwarfare", *Georgetown Security Studies Review*, Vol. 2, No. 2 (June 2014).
[27] N. Robinson, A. Walczak, S.-C. Brune, A. Esterle, P. Rodriguez, it Stocktaking Study of Military Cyber Defence Capabilities in the European Union (milCyberCAP): Unclassified Summary Santa Monica, CA: RAND Corporation, 2013.
[28] M. Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford, UK: Oxford University Press, 2014.
[29] S.D. Sagan and K.N. Waltz *The Spread of Nuclear Weapons: An Enduring Debate*, 3rd Edition, New York: W.W. Norton, 2013.
[30] J.B. Sheldon, "The Rise of Cyberpower", In *Strategy in the Contemporary World: An Introduction to Strategic Studies*, Edited by J. Baylis, J.J. Wirtz, and C.S. Gray, 4th Edition, Oxford, UK: Oxford University Press, 2013.

[31] Sun Tsu [Sun Zi], *The Art of War*, Translated and with an Introduction by S.B. Griffith. London: Oxford University Press, 1963.
[32] *Tallinn Manual on the International Law Applicable to Cyber Warfare Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* General Editor M.N. Schmitt, Cambridge, UK: Cambridge University Press, 2013.
[33] N. Tsagourias, "Cyber Attacks, Self-defence and the Problem of Attribution", *Journal of Conflict and Security Law* (Oxford, UK: Oxford University Press), Vol. 17, Issue 2 (Summer 2012).
[34] J.A. Warden, *The Air Campaign: Planning for Combat*, Revised Edition. San Jose, CA: to Excel, 1998.

## NATO W NOWYM ŚRODOWISKU STRATEGICZNYM: CYBERATAKI PODLEGAJĄ JUŻ ARTYKUŁOWI 5 TRAKTATU PÓŁNOCNOATLANTYCKIEGO

**Streszczenie.** Największa zmiana w dziejach polityki obronnej i strategii wojskowej Sojuszu Północnoatlantyckiego nastąpiła w 2014 roku w odpowiedzi na serię cyberataków przeciw państwom członkowskim i partnerskim NATO – Estonii w 2007 roku, Stanom Zjednoczonym i Gruzji w 2008 roku, i innym w latach późniejszych – oraz na ogólną transformację środowiska bezpieczeństwa, w którym wojna cybernetyczna i inne zagrożenia dla cyberbezpieczeństwa szybko zyskują na znaczeniu. Na szczycie w Walii w 2014 roku NATO uznało, że cyberobrona jest częścią zbiorowej obrony jako centralnego zadania sojuszu i że artykuł 5 Traktatu Północnoatlantyckiego – „Strony zgadzają się, że zbrojna napaść na jedną lub więcej z nich w Europie lub Ameryce Północnej, będzie uznana za napaść przeciwko nim wszystkim ..." – może być przywołany w przypadku cyberataków. To oświadczenie jest pierwszym i jedynym rozszerzeniem znaczenia artykułu 5 oraz pierwszym i jedynym dodaniem nowego rodzaju wojny do polityki i strategii NATO. Po tej zmianie sojusz musi stawic czoła nowym wyzwaniom, pilnym i trudnym nie mniej od starych wyzwań wojny kinetycznej lub broni masowego rażenia. Artykuł dotyczy najszerszego strategicznego kontekstu zmiany. Analiza jest prowadzona w świetle globalnej myśli strategicznej i rozwoju wojny poprzez dzieje. Wchodząc w nową przestrzeń strategiczną cyberowjny, NATO wykazuje, że należy do najbardziej nowoczesnych i zaawansowanych potęg świata, a jednocześnie wraca do starożytnej – i trwałej – zasady strategii: informacja nie jest podrzędna wobec siły. Tak sojusz odchodzi od Carla von Clausewitza i zbliża się do Sun Zi. Uznanie cyberprzestrzeni za przestrzeń strategiczną nawiązuje również do innej wpływowej idei dziedzictwa strategii: do koncepcji „wielkiego terenu publicznego" ("the great common"), władza nad którym daje klucz do władzy nad światem, i nad wojną i pokojem w świecie. Alfred Thayer Mahan uważał ocean światowy za „wielki teren publiczny", przecinany przez żywotne szlaki handlowe i floty konkurujące o wyższość. Dziś cyberprzestrzeń jest tak otwarta, żywotna i łatwa do podboju, jak przestrzeń morska była w wizji Mahana. Wojna cybernetyczna także rodzi obietnicę i pokusę rozstrzygającego uderzenia – pierwszego i zarazem ostatniego na wojnie – które pozwala obejść wszystkie elementy obrony przeciwnika i sparaliżować wrogi kraj. To nowa wersja – mniej lub równie śmiercionośna, zależnie od taktyki cyberataków podczas ofensywy cybernetycznej – idei bombardowania strategicznego i całej koncepcji siły powietrznej według jej wizjonera Giulio Douhet, a potem według strategii

nuklearnej. Na koniec artykuł podaje dwie praktyczne rekomendacje co do polityki i struktury Sojuszu Północnoatlantyckiego na rozwijającą się nową erę. Potrzebny jest teraz szybki ciąg dalszy przełomowej decyzji Szczytu w Walii. Cyberobrona powinna zostać w pełni włączona – jako integralna część – do następnej Koncepcji Strategicznej NATO. Nowa Koncepcja Strategiczna jest spodziewana w roku 2020 lub zbliżonym, ale może być opracowana wcześniej z powodu przyśpieszającej przemiany środowiska bezpieczeństwa. NATO powinno również rozważyć ustanowienie globalnego Dowództwa Cybernetycznego dla utrzymania inicjatywy i dla zapewnienia wiarygodności artykułu 5 Traktatu Północnoatlantyckiego w rozszerzonym znaczeniu. Ta wiarygodność będzie natychmiast, ciągle i wszechstronnie testowana przez wielu graczy globalnej gry.

**Słowa kluczowe:** NATO, Traktat Północnoatlantycki, cyberobrona, cyberbezpieczeństwo, cybernetyka, informatyka, cyberwojna, wojna cybernetyczna, wojna informacyjna, cyberatak, atak cybernetyczny, kryptologia, strategia, koncepcja strategiczna, Polska, Stany Zjednoczone, USA, Estonia, Gruzja, Sun Zi, Sun Tsu, Clausewitz, Mahan, Douhet, bombardowanie strategiczne, strategia nuklearna, strategia jądrowa