Marian Kozub, Adrian Mitręga
Jan Kochanowski University in Kielce

STRATEGIC THINKING ABOUT SECURITY IN CYBERSPACE

ABSTRACT

Since its emergence, cyberspace has been developing dynamically. It has become an information and communication sphere for billions of people, and thus plays an increasingly important role in our lives, as many political, economic, social, and cultural activities now take place in virtual space. Nevertheless, with the widespread use of the Internet and people's growing dependence on information and communication technologies, threats from cyberspace have become a significant factor directly related to social stability and national security. Protection against threats that have appeared in cyberspace has become an important issue for countries and international organisations, as consequences to a cyber-attack may be equally as serious as a military attack. Therefore, the aim of this article is to present the relationship between strategic thinking and security in cyberspace.

Key words:
strategic thinking, cybersecurity, cyberspace

INTRODUCTION

In recent years, the issue of cybersecurity[1] has been raised in many debates related to national security due to the fact that cyberspace capabilities are now considered an element of power. Many countries of the modern world develop these capabilities for various purposes, e.g. to provide essential services to its citizens, gather intelligence and counterintelligence information,

[1] The concept of *cybersecurity of the Republic of Poland* was defined as: "the process of ensuring the safe functioning of the state in cyberspace as a whole, its structures, natural and legal persons, including entrepreneurs and other entities without legal personality, as well as ICT systems and information resources in global cyberspace at their disposal." *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, BBN (National Security Bureau), Warsaw 2015, p. 7.

steal business information and technology in obtaining economic benefits, or attack the digital infrastructure of the opponent(s). Such attacks are conducted with the involvement and/or support of hackers in order to inflict economic damage, but also to cause consternation among the decision makers of the attacked country. After the events of 11th September 2001, cyberspace began to be treated as a new threat, but also a challenge to global security, as al-Qaeda used it as a battlefield against the United States. In 2007, cyberspace became an "area" (space) of hostilities in the Estonian-Russian conflict, and in 2008, in the war between Russia and Georgia. The cyber-attack with the use of the Staxent virus on the Iranian nuclear program in 2010 was another significant change in the development of cyber weapons. Social networks have also played an important role in the evolution of threats to the international security environment, as evidenced by, e.g., the Arab revolutions in early 2011.[2] In view of the above, it can be assumed that security organisations around the world have had to deal with the growing problem of the potential use of cyber capabilities and possibilities by various types of hacker groups – created by states or autonomous. This has become all the more important since the complex strategic security environment, created by various types of cyber capabilities in order to, *inter alia*, disrupt digital systems, is a very serious problem for both national and international security planners. It is no wonder that already in September 2010, the then US Deputy Secretary of Defence W.J. Lynn III officially classified cyberspace as the "fifth domain of conflict" besides land, sea, air, and space.[3] It was also from that moment that most countries decided to move to designing and planning their security through the prism of their own strategic culture,[4] strategies for cyberspace security, to deal with threats, but also challenges that, even "only" in terms of ordinary cybercrime and electronic espionage, are

[2] *Cyberspace and weapons of mass proliferation between deterrence and the arms race,* https://seconf.wordpress.com/2015/05/15/, access: 03.08.2020.

[3] W. J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy* , "Foreign Affairs" 2010, pp. 97-108; *The threat from the internet: Cyberwar,* http://www.economist.com/node/16481504?story_id=16481504, access: 05.08.2021.

[4] The issue of strategic culture spread in security sciences in the second half of the 1970s, when Jack Snyder developed an analytical study on the Soviet strategic culture in terms of the use of nuclear weapons. Snyder pointed out that the decisions made by politicians in the Soviet Union differed from their US counterparts in terms of factors taken into account in the decision-making process. This situation made it difficult to predict how the Russians would behave in the face of a nuclear crisis. According to Jack Snyder, "strategic culture can be defined as the sum of thoughts, conditional emotional responses, and behavioural habits acquired by members of the national strategic community through instruction or imitation." J. L. Snyder, *The Soviet Strategic Culture: Implications for Limited Nuclear Operations*, RAND, Santa Monica 1977.

growing at an extremely rapid pace, profoundly affecting the economy and the competitiveness of a large number of countries.[5]

One should therefore bear in mind that if, during the Cold War, technology was a factor of strategic advantage in the rivalry between two superpowers, also involved in the militarisation of space and development of computer networks to serve their military strategies, in modern times the emphasis is increasingly moving towards the virtualisation of international relations, including conflicts.[6]

CYBERSPACE AS A SECURITY AREA

Cyberspace analysed in the area of security is a battlefield and geopolitical competition in the 21st century. There are few strategic analyses to point out that future wars between states will no longer be initiated by politics and armed forces, but will be focused on the massive use of cyber-attacks to preemptively sabotage the enemy's defence capabilities. It is a huge global space with virtually infinite dimensions, which is also used by organised criminal networks aimed at economic gain, by fundamentalist terrorist movements to attract new followers or spread news via the Internet, or by non-governmental spy agencies that can steal vital economic information, thus distorting fair competition.[7]

According to the American military expert F.D. Kramer, there are about 30 definitions of cyberspace.[8] The first person to use this term was W. Gibson – in his book called "Neuromancer" published in 1982, he defined cyberspace as: *"A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data."*[9] In turn, according to the Cybersecurity Doctrine of the Republic of Poland of 2015, cyberspace is defined as: *"space for processing and exchanging information, created by ICT systems (groups of*

[5] S. Mele, *I principi strategici delle politiche di cybersecurity,* https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-delle-politiche-di-cyber-security.html, access: 10.08.2021.

[6] *Doc. XXXIV n. 4,* https://www.camera.it/_dati/leg16/lavori/documentiparlamentari/indiceetesti/034/004/d020.htm, access: 12.08.2021.

[7] Ibid.

[8] *Киберпространство как стратегический инструмент социальной инженерии,* https://whatisgood.ru/theory/analytics/kiberprostranstvo-kak-strategicheskiy-instrument/, access: 15.08.2021.

[9] W. Gibson, *Neuromancer,* Ace Books, New York 1984, p. 53.

cooperating IT devices and software, enabling the processing, storage, as well as sending and receiving of data via telecommunications networks using a terminal device appropriate for a given type of telecommunications network, intended to be connected directly, or indirectly, to network termination points), along with the connections between them and the relations with users."[10] The document also specifies the term *cyberspace of the Republic of Poland* as: *"cyberspace within the territory of Poland and in places where there are representative offices of the Republic of Poland (diplomatic missions, military contingents, vessels and aircrafts outside the territory of the Republic of Poland, subject to Polish jurisdiction)".*[11] According to NATO, in turn, cyberspace *"is more than the Internet, hardware, software and information systems, it is also about people and social interactions within these networks."*[12] In the face of serious threats in cyberspace, [13] in 2016, NATO recognised cyberspace as another type of space – besides land, sea, and air – in which operational activities can be carried out in the context of various types of conflicts. In consequence, the interested parties (countries, international organisations, including NATO) systematically create and update strategic documents and legal acts that constitute the basis of their cybersecurity policies,[14] especially in view of the fact that cyber-attacks enable anonymity, while offering a much better profitability ratio compared to conventional military attacks. Moreover, it is becoming increasingly likely that a cyberattack will precede – or even replace – an attack against NATO, thus placing cyber defence at the forefront of security issues. Therefore, the issue of new

[10] *Doktryna Cyberbezpieczeństwa Rzeczypospolita Polskiej*, *op. cit.*, p. 7.

[11] Ibidem.

[12] A. Klimburg, *National Cyber Security Framework Manual*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2012, p. 8.

[13] For analytical and interpretative simplification, the threats from *cyberspace* can be divided into four main types: 1) *cybercrime*: a set of threats posed by national or international criminal organisations that use cyberspace for crimes such as: fraud, identity theft, unjustified theft of information, or intellectual creations and property; 2) *cyberterrorism*: the use of the Internet by terrorist organisations for propaganda, slander or related purposes. Particularly important is the case of cyber-propaganda or the manipulation of information posted on the Internet for the purpose of political slander and delegitimisation, social or personal discrimination. In extreme cases, the sophisticated use of the Internet, or electronic controls, by terrorist organisations to disable critical transmission reels of structures or processes related to national security; 3) *cyberespionage*: a set of activities aimed at using the potential of a network to steal industrial secrets for the purpose of unfair competition (if consumed in the civil patent market) or strategic advantage (in the case of theft of military designs or dual-use equipment); 4) *cyberwar*: a scenario relating to a real conflict between nations by the systematic destruction of critical protective barriers to the enemy's security or by disrupting or "closing" strategic communication networks and integrating these activities with strictly militant ones. Doc. XXXIV n. 4, *op. cit.*

[14] J. Cichosz, *Polityka cyberbezpieczeństwa Rzeczypospolitej Polskiej*, PhD dissertation, UJK, Kielce 2019, p. 202.

strategic thinking and action appears to be essential in order to be able to mitigate this very real threat, which is also a challenge for the future.[15]

When thinking of cyberspace, we tend to imagine an abstract information space, as opposed to the real world and its geography, because the boundaries of cyberspace are virtual and only recreated artificially. However, in the case of sovereign states, cyberspace creates new problems related to user monitoring, as well as adapting legal regulations to virtual reality. Cyberspace has created the impression of an imaginary world born during the first Internet revolution in the late 1990s, which emphasises the concept of openness to the world and crossing borders.[16] However, cyberspace is also, on the one hand, a new reality, environment, space that the armed forces recognise as a battlefield, and on the other hand – a tool by which various entities shape the human worldview.

It is a common belief that in the coming times, the importance of cyberspace certainly will increase even more; therefore, it is imperative to tackle the issues of Internet governance, accountability, and establishing a comprehensive framework to create and guarantee security in cyberspace.[17] These aspects are thus becoming a priority subject of strategic considerations by people dealing with security issues.

STRATEGIC THINKING[18]: THE ESSENCE OF THE CONCEPT

The variable dynamics, complexity, chaos, shock, i.e. the features of the modern security environment, are increasingly more often one of the basic determinants of decision-making. They force strategists and managers of organisations (institutions) to analyse the critical links between the strategy and the

[15] *Préparer le futur : la cyberdéfense et le nouveau concept stratégique,* https://www.nato.int/cps/en/natohq/news_77515.htm?selectedLocale=fr, access: 10.08.2021.

[16] K. Limonier, *Russia in Cyberspace: Issues and Representations,* “Hérodote” 2014, No. 1, pp. 140-160.

[17] S. Gurza, *Cyberbezpieczeństwo Indii: spojrzenie na podejście i gotowość,* https://www.icwa.in/show_content.php?lang=2&level=3&ls_id=6187&lid=4245, access: 14.08.2021.

[18] In general, thinking is understood as a process taking place in the minds of individual people. From the philosophical category point of view, this term can be defined as: a certain direction of perception and evaluation of the surrounding world (individual and collective); a summary of the general principles of decision making; a strong concept of problem solving in a specific area (e.g. economic thinking, philosophical thinking, military thinking, strategic thinking). J. Mika, *Strategie a strategické myšlení,* [in:] *Vojenská Strategie,* ed. V. Galatík, A. Krásný, K. Zetocha, Univerzita Obrany, Ministerstvo obrany České republiky – PIC MO, 2008, p. 39.

socio-cultural foundations of the security model in its broad sense. Hence, it is important to understand the effect and impact of the dynamics of the changes occurring – wide-scoped, various, often not forecasted – on the efficiency and effectiveness of the management[19] of security, including cybersecurity. This is all the more important as the implementation of various security programs and strategic plans was in the past treated by many politicians, strategists, and managers as a kind of internal mechanism that can automatically restore a disturbed balance.[20] That is also the case nowadays. This approach, however, along with the development, intensification and increased level of complexity, unpredictability or variability of conditions, the creation of traditional programs and strategic plans turns out to be insufficient. Their horizon has been reduced, as well as their duration and content, more and more frequently filled with "only" fragmentary declarations, gradually replacing unambiguous specific measures, often not supported by any specific undertakings or provisions – e.g. the Polski Ład program[21] (the name of which roughly translates to the Polish Order). On the other hand, programs, but most of all, plans – first strategic, and then operational, tactical – should contribute to the success of the process of

[19] J. Rokita, *Problemy zarządzania w warunkach nowej ekonomii,* [in:] *Zarządzanie strategiczne w warunkach nowej gospodarki*, ed. J. Rokita, W. Grudzewski, Wyd. Górnośląskiej Wyższej Szkoły Handlowej, Katowice 2007, p. 31.

[20] A. Mróz, *Strategiczne podejście do myślenia o przyszłości w bezpieczeństwie narodowym. Metodologia strategicznych studiów nad przyszłością w bezpieczeństwie narodowym. Studium teoretyczne*, AON, Warsaw 2016, p. 11.

[21] "Polski Ład" (the Polish Order), a program of economic and social reforms until 2030 proposed by the Government of the Republic of Poland, the aim of which is to counteract the effects of the pandemic. "*…A new decade of the century is ahead of us – a decade that may decide the future of Poland and Europe in the next few decades. Therefore, our goal is clear: to return to the path of economic growth as soon as possible, and continue building the Polish welfare state. If we want our dreams back, we must act today. It's time for another breakthrough. It's time for the Polish Order – a comprehensive strategy for overcoming the effects of the pandemic. This is our economic recovery plan. And a new hope for a good future"*… "We still want to continue building a welfare state that will not deviate from European standards. We still dream about Poland being a place where everyone are able to live and work safely and for decent money. Therefore, the response to the challenges posed by the COVID-19 crisis must be a new action strategy"... "The Polish Order is more than a recovery plan, it is a strategy of civilisation change. We created it with a view to the actual promotion of Polish families and Polish companies. ... "*we are standing at the guidepost." We are faced with the choice of which path to follow. We know well that the coming years will decide about the future of Poland, Europe and the world for decades to come. Therefore, the third decade of the 21st century must become a decade of development for Poland. Historical challenges await us, but we face them aware of our difficulties and our purpose. For the first time in modern history, we have a chance to be an actor, rather than just a passive viewer of changes that will shape the new face of the world. The Polish Order will allow us to achieve this goal." Program Polski ład,* Warsaw 2021, pp. 5, 12.

strategic management, "creating a security architecture," while being a source of information and data necessary for creative strategic thinking.[22] Thus, strategic thinking, together with action,[23] construed as unity, create a future-driven strategy, constituting a project containing *the basic directions, rules and instruments of action* (i.e. of the use of resources and skills), in response to signals coming from the internal and external environment and ensuring its future position in relation to the surroundings. They should also constitute the basis of strategic thinking and its evolution, but not determine the only possible path of development. Now, identifying the essence of a strategy as, *inter alia*, thinking and operation of an organisation that combines specific goals, resources, and tools in the domain of security, as well as the diagnosed genesis and development of strategic thought, one should attempt to answer the following question: *what basic factors (determinants) can influence the activity of strategic thinking and significantly create (shape) it?* Intuitively, one could say that a great number of these forces, various factors (determinants) can affect all aspects of this thinking, including, e.g., the level of civilisation development, political goals and entity wealth, value systems and the degree of technical and technological development, geographical conditions, etc. This implies that the security policy and strategy could be defined as *"mega-thinking and action"* (identified as one!), which consists of a number of sub-processes, and the main goal of the strategy should be to generate favourable strategic effects supporting the achievement of goals for defence and protection of national interests. These effects, in turn, should arise from the results of actions taken, i.e. from the effect of synergy[24] in

[22] In praxeological terms, thinking is nothing else than *reflection*, i.e. an internal action consisting in the thinker being transformed by themselves from *unknowing* into *knowing*, and thus, looking for a global assessment of actions that arises in a specific way from positive and negative values. T. Pszczołowski, *Mała encyklopedia prakseologii i teorii organizacji*, Ossolineum, Wroclaw 1978.

[23] What is meant by "*action*" is "*...deliberate, conscious, arbitrary human behaviour*." The elements of action are therefore nothing else than: "*...actors, material, means, methods, ends, products, etc.*" and the end(s), conditions and means are the main parts of practical activity. After all, "*...to act is to change reality in a more or less conscious way; to pursue a specific goal under given conditions by appropriate means in order to move from the existing conditions to the conditions corresponding to the assumed goal; to incorporate into reality the factors which have the effect of moving from a system subject to determination of initial conditions to a system of defined end conditions. The action to be carried out requires a threefold designation: designation of a purpose, designation of conditions belonging with reality, and designation of means adapted both to the intended purpose and to the existing reality."* T. Kotarbiński, *Traktat o dobrej robocie,* Ossolineum, Wroclaw 1982.

[24] The synergy effect is a principle that could be colloquially summarised as "2 + 2 = 5" – the synergy effect says that the joint action of all parts is much greater than the sum of the individual parts together; it is the opposite of antagonism. The synergy effect can be either positive or negative. There is a phenomenon referred to as the Apollo Syndrome, which

achieving the assumed goals, in consequence of concepts of action applied and resources (forces and means) used, as well as appropriately utilised methods. Thus, these effects should constitute a specific measure of the quality of actions taken to achieve the defined political intentions.

Optimising security involves being strategic[25], strategic thinking, as well as strategic action, which result from the need for a holistic, multi-faceted view of security, but looking far into the future[26] in order to be able to face it, predict it, but also anticipate the already known threats in advance, or take effective action in the areas of ever-emerging new challenges.[27] Success in such actions will thus require an appropriate approach, respecting the diverse situation in the world, as well as people's innate desire for security, which should be

describes negative synergy. It concerns management – in a situation where a group of intelligent and capable people achieve worse results than a group of less capable people or each member of the team individually. The synergy effect is relevant in virtually every field – social psychology, chemistry, power engineering, etc. The essence: synchronisation of e.g. the efforts of troops and resources of individual Armed Forces during combat operations to achieve their goal, in the use of their various capabilities so that as a result of the synergy effect, the effects of combined operations are greater than the simple sum of the effects of the separate operations of the Armed Forces – they perform tasks for the operation rather than, *as it was before*, for the benefit of either of them. M. Kozub, *Konflikty początku XXI wieku. Użycie sił powietrznych*, AON, Warsaw 2007, pp. 61-64.

[25] Understood as: significance, fundamentality, elementariness, constitutiveness. M. Kozub, *Bezpieczeństwo przyszłości jako efekt synergii myślenia i działania strategicznego*, [in:] *Edukacja obronna kierowniczej kadry administracji publicznej w ramach WKO – Doświadczenia i wyzwania*, ed. W. Kitler, S. Olearczyk, Z. Piątek, Ruch Wspólnot Obronnych, Warsaw 2014, p. 9.

[26] This is important specifically because security science is one of the scientific disciplines included in the area of social sciences, however, the subject of security science research are contemporary, but *mainly future security systems* in various dimensions, i.e. military and non-military, and their functioning on various organisational levels. It is research in this discipline that should serve the creation of theoretical foundations and development of international and national security systems, as well as operating systems functioning in the area of broadly interpreted security. These systems, in turn, include the activities of state, government and local government institutions, entrepreneurs and social organisations, as well as individual ones. Thus, while security sciences do not deal with history, they use its conclusions, and create a concept for shaping and creating security in the future. *Nauki o bezpieczeństwie* (Security sciences), https://pl.wikipedia.org/wiki/Nauki_o_bezpiecze%C5%84stwi, access: 12.08.2021.

[27] *Challenges* – elements of a set of forecast events, phenomena, states, processes, etc., which the entity (organisation) should (must) take into consideration when designing the future. Challenges are subjectified and objectified. They should be seen as threats, but also as opportunities. They are neither good nor bad. They are "electrically neutral." The language of challenges is the language of forecasting. Thus, a challenge will be anything that may happen in the future and that the organisation should (must) take into account when designing its own future attitudes and actions. M. Kozub, *Strategiczne środowisko bezpieczeństwa w pierwszych dekadach XXI wieku,* AON, Warsaw 2009, p. 72.

shaped, created, and not imposed. This maxim should be not only relevant, but also perceived in a special way in modern times, in the era of information, immediate communication, revolutionary and evolutionary changes, both political and technological, or the environmental and climate era in which every organisation wishing to not only maintain itself but also develop, must be recognised not only by individual leaders but also by entire societies. In general terms, this could be formulated as follows: "…*a world order without freedom (security), even if sustained by a temporary rapture, ultimately creates a counterbalance to itself, while freedom cannot be achieved or secured without the framework of an order that maintains peace."*[28] In order to achieve this, to be able to function in a safe organisation, it is necessary to specify certain skills in strategic thinking, the most important of which include:[29]

- *multidisciplinary approach*, based primarily on understanding and associating facts from various areas, i.e. political, social, economic, military, and technological – not only knowledge of these areas will be required, but also the ability to formulate problems and communicate with specialists in these fields;
- *systemic approach*, which will allow to understand the emerging and potential problems, which in turn will allow not only to favour a specific sphere as dominant from the outset, but also, over time, to make the necessary adjustments in the identified priorities;
- *multivariate thinking*, focused on the long-term perception of the complexity and variability of phenomena (processes) in creating security, which should enable the extraction of appropriate sets of data (information, factors, etc.) enabling the construction of possible directions and then possible scenarios, and therefore, to an extent, having the ability to correctly formulate and select criteria for making decisions;
- *focusing not only on anticipating the future, but also on making this knowledge more concrete in formulating the strategy*. Not only is strategic thinking cognitive (based on analysis and diagnosis), but also pragmatic – in the form of building and proposing appropriate reactions in a long-term perspective (e.g. in the form of an appropriate concept).

It should be emphasised, therefore, that in modern times there is not only no generally accepted definition of strategic thinking, but also no common agreement as to its role (meaning), and no standard list of basic competences. However, most people agree that traditional strategy-creating models are

[28] H. Kissinger, *Porządek światowy*, Wydawnictwo Czarne, Wołowiec 2016, p. 16.

[29] P. Daniluk, *Myślenie strategiczne w naukach o bezpieczeństwie*, http://www.dsw.edu.pl/fileadmin/user_upload/wydawnictwo/RBM/RBM_artykuly/20127.pdf, access: 12.08.2021.

mainly based on strategic planning, but strategy in today's competitive security environment is shifting from basic "strategic planning" to "strategic thinking."[30] General A. Beaufre wrote in 1963 that strategic thinking "*is a mental process, abstract and rational at the same time, which must be able to synthesize both psychological and material data. The strategist must have great abilities for both analysis and synthesis; collect data on the basis of which they make a diagnosis, make a synthesis in order to make a diagnosis from these data – and the diagnosis in fact comes down to choosing amongst alternative methods of operation*".[31] H. Mintzberg, in turn, defined strategic thinking as "*a distinctive managerial skill that allows the creation of new strategies based on predicting the future*."[32] The Japanese strategic thinking specialist K. Ohmae, who in his homeland is called "Mr. Strategy", believes that "*strategic thinking is the ability to think creatively and actively, which gives rise to dynamic ideas and goals. In this interpretation, strategic thinking is a fundamental skill of those who strive for success.*"[33] According to this strategist, three basic types of thinking can be identified in relation to strategic thinking, which are the following:

- *mechanical thinking*, which is based on logical thinking with an emphasis on analysis and the creation of several variants. When making decisions, it follows the recommended and proven procedures;
- *intuitive thinking*, which is based on intuition and is usually used to solve partial problems. Intuition is usually a narrow view in which the whole is assessed on the basis of a selected element, but it allows for quick and unambiguous adoption of solutions;
- *strategic thinking* is based on detailed analyses, and its result is a new solution, difficult to predict or duplicate. Strategic thinking thus brings unique solutions that may mean a significant competitive advantage.[34]

Now, strategic thinking has many dimensions, one of which is *the ability to look at the place* where the organisation is at a current time and where it could (should?) be in the future, i.e. the place where we would like it to be. The second dimension should be to look at the organisation *from a distance* so as to be able to see all its individual elements, rather than only the general view.

[30] J. Liedtka, *Łączenie myślenia strategicznego i planowania strategicznego,* "Strategia i przywództwo" 1998, No. 26 (4), pp. 30-35.

[31] A. Beaufre, *An Introduction to Strategy*, Frederick A. Prager. LCCN 65014177, 1965.

[32] H. Mintzberg, *Strategy Formulation As A Historical Process,* "International Studies of Management & Organization" 1977, Vol. 7, No. 2, pp. 28-40.

[33] *Стратегическое мышление старшеклассников (будущих руководителей) как фактор общего роста России,* https://mgpu-media.ru/issues/issue-21/psycho-pedagogical-science/strategic-thinking.html, access: 16.08.2021.

[34] *Strategický Manažment,* https://gtk.uni-miskolc.hu/files/5043/STRATEGICK%C3%9D%20MANA%C5%BDMENT.pdf, access: 18.08.2021.

Strategic thinking should therefore become a management method to connect the present with the future, the current and the future positions of the organisation, but also a method that cannot be treated separately from action. As already mentioned, strategic thinking and action always form a whole; they are inseparable. And all this should lead to the "creation" of an appropriate strategy, without which the organisation will not be able to function. While one cannot rule out a situation where that the lack of a strategy would definitely condemn an organisation to loss, not knowing its strategic goals (long-term goals, etc.) may not only make its route to success, constructed and then implemented *ad hoc*, extend, but even put it at the mercy of chance.

Assessing various sources of theoretical materials concerning these problems, it seems that this was expressed relatively clearly by Seneca, who wrote: "*…If one does not know to which port one is sailing, no wind is favourable."* Referring to this, one could assume that an organisation without a strategy is like a ship drifting on the sea. The existence of an organisation in a strategic security environment without a vision and strategy may cause chaos in its functioning and development, where its individual elements, unaware of the common pattern of operation, will follow directions that are known only to them, which are not going to always be consistent with the others' direction of activities. Perceiving strategic thinking in this way in the development and implementation of different strategies may result in the emergence of various errors, the most common of which could include, e.g.:

- overestimating the organisation's own resources and competences;
- formulating an erroneous mission and, in consequence, an erroneous vision and erroneous strategic goals;
- wrong choice of strategy, resulting in the lack of link between strategic and operational goals;
- wrong structure or management of the organisation and lack of budget to achieve its strategic goals.

However, it should be emphasized that strategic thinking and acting is not a new question. One can even get the impression that the basic domains for these concepts not only raise no doubts, but also should not be subject to any discussion. Meanwhile, merely a brief review of the contemporary literature on this topic is enough to see that it is still an open area, and that almost every issue is the subject of disputes and division.

This is important specifically because in praxeological terms, *strategic thinking* is nothing else than reflection, i.e. an internal action consisting in the thinker being transformed from unknowing into knowing, looking for a global assessment of actions that arises in a specific way from positive and negative values.[35] *Strategic action*, in turn, should be understood as: "*…deliberate, conscious, arbitrary human behaviour,* the elements of which will be, *inter alia*: *actors, material, means, methods, ends, products, etc."*[36] At this point, it should be noted that *"…the action to be carried out requires the designation of a purpose, conditions belonging with reality, and means adapted both to the intended purpose and to the existing reality."*[37] But also that "…*to act – or at least to act thoughtfully – is to change reality in a more or less conscious way; to pursue a specific goal under given conditions by appropriate means in order to move from the existing conditions to the conditions corresponding to the assumed goal; to incorporate into reality the factors which have the effect of moving from a system subject to determination of initial conditions to a system of defined end conditions".*[38] Thus, an action that is to be carried out requires the designation of *a purpose, conditions belonging with reality*, and *means* adapted both to the intended purpose and to the existing reality.

It is thus all the more important to remember that strategic thinking consists in an interdisciplinary approach to strategic processes, i.e. processes containing a large number of unknown or uncertain factors, and the creation of multivariate mental concepts describing future situations and directions of development.[39] It is also a guided process of imagination underpinned by appropriate information about the future, enabling the creation of different visions, different scenarios that may arise as a result of changes in the environment, presenting relatively reliable conditions for the company (i.e. office, but also us) to operate in, and thus uncertain and unforeseen circumstances, creating threats, opportunities and risks,[40] but also "*striving to examine the situation, research any opportunities, choose goals and rules for the use of resources, looking many years into the future; using a set of techniques and methods of analysis and synthesis enabling the implementation of aspirations and the collection of information for this; willing to constantly change the areas and methods of operation; preparing the organisation for operating in the future;*

[35] T. Pszczołowski, *Mała encyklopedia prakseologii i teorii organizacji*, Ossolineum, Wroclaw 1978, pp. 127-128.

[36] T. Kotarbiński, *Traktat o dobrej robocie*, Ossolineum, Wroclaw 1982, p. 16.

[37] Ibid., p. 18.

[38] "*…essential to strategic thinking and action is the necessity and quality of strategic culture, which is a prerequisite for the emergence of such specific strategy styles and for the possibility of creating a strategy in the first place."* Ibid., p. 20.

[39] J. Penc, *Zarządzanie dla przyszłości,* PSB, Krakow 1998.

[40] M. Kozub, *Myśleć strategicznie o bezpieczeństwie przyszłości,* AON, Warsaw 2013, p. 102.

thinking about the organisation as a whole and not the sum of individuals; creating a favourable image of the organisation in the society."[41]

Strategic thinking is the ability to look into the future and take control of the overall situation, as well as the ability to grasp the general trend and direction of development. However, the ability to think strategically is not an innate trait, but is gradually formed through long-term learning (training) and practice through mastering various methods.[42] By continuously working with strategic thinking, one is able to find the best way to achieve their end goal, and the ability to find solutions anywhere is the essence of strategic thinking.[43] J. Liedtka observed five "key attributes of strategic thinking" similar to competences, which are as follows:

- *system perspective*, meaning that one can understand the consequences of strategic actions ("Strategic thinkers have a mental model of a complete, comprehensive value creation system, they understand their role and competences associated with it");
- *intent-oriented*, meaning that the strategist is more assertive and less distracted than their competitors in the market. In order to popularise this concept by Hamel and Prahalad, Liedtka defines strategic intention as "concentration that allows individuals in an organisation to gather and use energy, focus their attention, resist distractions, and concentrate on achieving the goal for as long as required for it to be implemented;"
- *thinking about time*, meaning that you can make better decisions and accelerate the implementation of those decisions while keeping in mind the past, the present, and the future. This is in consequence to the fact that the strategy is not driven by future intentions only. What is important here is the difference between the present reality and the intentions for the future. Scenario planning is the practical application of incorporating this attribute into strategy formulation;
- *hypothesis-based*, which allows creative and critical thinking to be incorporated into strategy formulation. This competence clearly integrates scientific methods with strategic thinking;

[41] *Management strategique de PME/PMI*, Guide methodologique, Economica, Paris 1991. [in:] M. Kozub, A. Mitręga, *Podstawy strategii bezpieczeństwa. Wybrane aspekty,* UJK, Kielce 2018, p. 202.

[42] *The deep connotation of strategic thinking and the value of the times,* http://www.qstheory.cn/llwx/2019-07/09/c_1124727205.htm, access: 20.08.2021.

[43] *How to improve and acquire strategic thinking*, https://www.roberthalf.jp/ja/career-advice/career-development/strategic-thinking-skills, access: 18.08.2021.

- *intelligent opportunism*, i.e. responding to good opportunities, "The dilemma of using thoughtful strategies for effective and efficient communication of the organisation's efforts must always be balanced against the risk of missing out on alternative strategies that are better suited to the changing environment."[44]
- Strategic thinking is crucial in the process of strategic management. Without a certain level of strategic thinking, it is impossible to create strategies at any level. In the past, it was assumed that a person was born with the ability to think strategically (creatively) and that this way of thinking cannot be learned. Today it is known that, as already mentioned, strategic thinking can be learned,[45] and you think strategically when:
    - *you know where you are going*. There must be a clearly defined goal. Otherwise, the strategy will not make sense;
    - *you know your current location.* In other words, you must be able to determine what your current situation is and how far away your goal is;
    - *you know how to delineate a path.* This is the key point of a strategy. It involves determining the way to achieve your goals.
    - *you have the ability to self-evaluate and self-correct.* Strategic thinking requires flexibility to change your actions if necessary.

In brief, strategic thinking is comprehensive and systematic mental effort aimed at predicting the future and proactively constructing it based on comprehensive historical, geographic, anthropological, and scientific data, which constitute a broad knowledge base and an inspiration factor.[46] Increasingly more often, strategic thinking constitutes a kind of synthesis that requires intuition and creativity in creating the future, which is realised with the help of created programs and strategic plans;[47] in addition, it is rather long- than short-term. It includes both a wide perspective and a detailed approach, as opposed to focusing only on particular details. Strategic thinking should therefore be both analytical and creative, while non-strategic thinking is characterised by only one direction, either the former or the latter. Consequently, it can be assumed that the main principles of strategic thinking include a critical approach

[44] J. Liedtka, *Łączenie myślenia strategicznego i planowania strategicznego, op. cit.*, pp. 30-35.

[45] О.С. Анисимов, *Мышление стратега: модельные сюжеты. Выпуск 21. Стратегическое мышление и цивилизация,* http://www.metodologika.ru/node/192, access: 20.08.2021.

[46] *Strategic thinking... its characteristics and importance*, https://www.saharamedias.net/3420, access: 19.08.2021.

[47] H. Mintzberg, *The Fall and Rise of Strategic Planning,* "Harvard Business Review" 1994, p. 108.

to the procedures currently used in various organisations, but also courage in proposing changes. Furthermore, strategic thinking is a skill that facilitates achieving goals. It helps you think in a more organised way, but most of all, to bear in mind what you want to achieve in the long run.[48] What is more, strategic thinking results from two things: firstly, it deals with facts of reality and tries to improve them as much as possible, and secondly, it takes this reality and its data as a basis for planning the future and improving it through anticipation. These two issues are essential in life in general, but in particular in the area of security, including cybersecurity.[49]

People who think strategically focus on how they can use what they already have as effectively as possible, and treat their conclusions as hypotheses, because their innovations (prognostic knowledge)[50] should always be based on partially inaccurate information (non-prognostic knowledge)[51] or predictions

[48] *Strategic thinking gives purpose to life,* https://wonderfulmind.co.kr/strategic-thinking-how-to-give-your-life-purpose/, access: 19.08.2021.

[49] M. Alwani, *A culture of strategic thinking. Visions and principles,* https://www.rowadalaamal.com, access: 19.08.2021.

[50] Prognostic knowledge, determinants of the entity's security environment are derived from superior decisions that shape the final form of the set of determinants. This approach is described by task determinants (current and forecast missions, goals and tasks, as well as possible (forecast) conditions for their implementation, executive concepts adopted for implementation) and constitutive determinants (over- and non-task determinants – current and forecast system requirements and intra- and non-organisational requirements, as well as possible conditions for the functioning and development of the organisation, executive concepts). Note: the weakest links in the process of identifying prognostic knowledge include: "weakness" of knowledge about the challenges of the future, "weakness" of the methodology and practice of shaping the informational basis for the management of the organisation, including designing its shape in conditions of limited quantitative and qualitative knowledge about the past. M. Kozub, *Strategiczne środowisko bezpieczeństwa przyszłości. Kierunki ewolucji oraz możliwe teorie i prognozy dla bezpieczeństwa RP do końca trzeciej dekady XXI wieku*, AON, Warsaw 2016, p. 41.

[51] Non-prognostic knowledge, lack of knowledge, area inaccessible to cognitive exploration, but significant for reflection on the future of the entity (organisation); generator of many determinants of features and properties, as well as development missions (tasks). The starting point for identification in this approach includes, *inter alia*, awareness of the existence of an area of reality which cannot be examined today, but which is where processes, phenomena and events occur that can manifest themselves in a perceptible form at any time, disturb the functioning of the entity (organisation), with a probability many times greater than forecast phenomena. The awareness of the existence of this area allows – with the use of appropriate methods, techniques and heuristics of creative thinking - to specify a fairly extensive set of consequences – premises of the desired/necessary features and properties of the organisation – as a whole, as well as its individual structural and functional elements. Ibid., p. 41.

(forecasts).[52] Therefore, a good "strategic thinker" must be able to do two main things: think forward by following the direction in which their problem is heading, while also not losing sight of what is happening around them. They must be ready for quick changes in the direction of activities and to combine planning with effective management. The best strategic thinkers constantly verify the latest trends, but also know what their opponents, rivals and competitors are doing, and keep adapting to it. They are able to see opportunities because they are continuously on the lookout for them, and try to be in two places at the same time: in the future, but also "here and now."[53]

In the third decade of the 21st century, the world is different than the one we knew and in which we lived not so long ago. However, the reasons for this statement are both the revolutionary changes occurring in science and technology, as well as the evolution of already diagnosed threats and forecast challenges,[54] for both shaping and creating the security of the future in the world we live in. It is a world where one of the basic distinguishing features is various kinds of knowledge, but also wisdom,[55] which, unfortunately, vanishes just as rapidly as technology develops. Thus, the world, as we know it, its environment and the surroundings which we live in, become increasingly more

[52] *forecast* – a tool for thinking about the future that tries to answer the question: *what will be the shape of the future?*, and the answer to this question is formulated in an unambiguously affirmative (conclusive) sense: *it will be this and that*, thus, in the category of *events* rather than *processes*; in a forecast, e.g., when building a picture of the future based on the use of specific econometric models, it is necessary to adopt some of one's own substantive assumptions as to the shaping of real future processes; it is assumed that certain substantive assumptions provide better results in shorter and medium periods (up to 5 years) than long ones (in relation to science and technology, they are easier to predict *ex ante* in periods of up to 5 years than longer). M. Kozub, *Myśleć strategicznie o bezpieczeństwie przyszłości,* AON Warsaw 2013, pp. 98-100.

[53] M. Majewska, expert of monsterpolska.pl.

[54] *Challenges* – elements of a set of forecast events, phenomena, states, processes, etc., which the entity should take into consideration when designing (predicting, forecasting, etc.) the future. They are subjectified and objectified and should be seen as: threats, opportunities, as well as risks. They are "electrically neutral" and should be described using the language of forecasting. Thus, a challenge will be anything that may happen in the future and that the entity (organisation) should (must) take into account when designing its own attitudes and actions. M. Kozub, *Myślec strategicznie o…, op. cit.*, pp. 29-30.

[55] wisdom is "...mind brought to perfection" (Seneca); ...is "the knowledge of divine and human rights" (Cicero); ...is "knowledge that teaches us to attain happiness" (Leibnitz); and nowadays: it is "pragmatic and technical – 'instrumental' knowledge, which tells us how to repair a car, what TV set to buy, but does not say what is the meaning of life, who a person should be, how to behave when seeing someone else's suffering" (Horkheimer, German philosopher), but also "the ability to find a balance between the contradictions that make up human life, and man has both material and spiritual needs, but how to reconcile them?" T. Gadacz, *Bez mądrości zginiemy*, "Gazeta Wyborcza", 30-31.08.2014.

unpredictable and dynamic, but also full of risk and uncertainty, creating a series of barriers and dilemmas for all of us. It is, however, people-oriented. For this reason, when making a diagnosis, or preparing any forecasts of the behaviour of various strategic players in specific spaces, it would be advisable to fully identify the nature and forms of the diagnosed threats, as well as the forecast challenges for various types of security, in its various dimensions. It is all the more important in view of the fact that in the times in which we live and work, there is no single coherent theory to describe "this" predicted shape of the future security, even from the perspective of the coming few years.[56]

Therefore, when attempting to generalise the identification of the essence of "strategic thinking about the future, its security,"[57] one should bear in mind that nowadays, in the field of social sciences, in the discipline of security science, these terms are very "trendy", but are most often presented as default, and thus, not quite precise. It should also be pointed out that both the experience based on history, as well as the results of the latest research, show that the concept of "strategic thinking about security"[58] is inextricably linked with the history of mankind, and therefore with the fates of individual people, nations, states, as well as the widely understood international community, which is also constantly evolving. This means that the identification of the essence of strategic thinking should include the following elements:

- *scientific approach to the problem*, meaning, to an extent, a method of reaching conclusions that we are interested in,
- *identification of desired*, possible (probable) *changes* (trends), i.e. processes leading to the future (which is the subject of these studies),
- *recognition (indication) of the image of future security*, i.e. the vision[59] (directions of desired changes) of target security (which determines the result of the studies).

[56] A Mróz, *Strategiczne podejście do…, op. cit.*, pp. 14-15.

[57] *8 elements in strategic thinking (studies) about future security*: defining a multi-variant vision of the future; the purpose of action in each of the considered variants; the manner of achieving the adopted main goal (from the variant), referred to as "access route" or "road map"; selection of priorities ensuring the best results of achieving the adopted goal; distribution of available development means in accordance with the adopted priorities, i.e. distribution to individual goals; defining the complexes of strategic activities necessary to achieve the goal; distribution of activities over time, placing them in order by urgency – a specific "timetable"; determining the performers of individual activities and deadlines for their implementation. M. Kozub, *Myśleć strategicznie o…, op. cit.*, pp. 93-94.

[58] A. Karpiński, *Co trzeba wiedzieć o studiach nad przyszłością?*, PTE, Warsaw 2009, pp. 28-29.

[59] a vision is a dream – situations in which the organisation wants to and may find itself in the future, i.e. a certain coherent scenario of dreams about the future of the organisation and achieving the position it aims at; it is a description of the entity's role and the effects of its activities in the environment, how the entity wants to be perceived; it is a picture of the future that the participants of the organisation wish to create. Having a vision is the ability

Referring to the above elements, one may conclude that without them, it is impossible not only to speak of strategic thinking about security, including cyberspace, but also to deal with this problem, this priority goal that is so important for people.

CYBERSPACE AS AN AREA OF STRATEGIC THINKING

Thinking about state security as a process perceived in a multifaceted way has become the basic paradigm of perceiving reality. The potential of the new level of state security in cyberspace generates many threats, but also challenges, which include, e.g.: individuals, state structures, private entities that are users of modern information technologies. This, in turn, translates into the need to implement measures (undertakings) to ensure the security of users of new technologies, such as, e.g., ICT networks. The growing phenomenon of cyber threats in global cyberspace is a challenge for many countries, leading to increased expenditure on protection in virtual space.[60] According to T. Maurer of The Open Technology Institute and The New America Foundation, "cyber weapons" are constantly and rapidly changing, as a result of which there is no single winning strategy against cyber threats.[61]

Traditional conflicts and wars were based on the confrontation of states that planned to defeat the enemy in the domains of air, sea, land and, in recent years, space. Nowadays, cyberspace has quickly become the fifth domain of hostilities. In 2010, the US recognised cyberspace as an operational domain, stating that "*Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation*."[62] Also, in 2011, former CIA director L. Panetta warned that "*... the next Pearl Harbor that we confront could very well be a cyber-attack*."[63]

to see the future as an improved present; it is an idea for the future, a dream with the power to make people want to turn it into reality. M. Kozub, lecture: *Wprowadzenie do strategii. Geneza i rozwój strategii jako nauki, sztuki i praktyki,* AON, WBN.

[60] T. Szubrycht, *Analiza podobieństw operacji militarnych innych niż wojna oraz działań pozwalających zminimalizowana zagrożenia asymetryczne*, "Zeszyty Naukowe Akademii Marynarki Wojennej" 2006, No. 1 (164), Gdynia 2006, p. 141.

[61] *Cyber Crime Study 2017 Insights on the Security Investments that make a difference,* https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf, access: 20.08.2021; C. Kavanagh, T. Maurer, E. Tikk-Ringas, *Baseline Review ICT- related process and events implications for international and regional security (2011-2013)*, ICT4PEACE Foundation, Geneva, 2014.

[62] *Strategy for Operating in Cyberspace,* Department of Defense, July 2011, p. 1.

[63] N. Menon, *The Potential Impact of Cyber Capabilities on Future Strategy,* https://www.e-ir.info/2021/05/05/the-potential-impact-of-cyber-capabilities-on-future-strategy/, access: 21.08.2021.

The IISS report on cyber capabilities assessed 15 countries based on seven parameters. These 7 parameters are: strategy and doctrine; governance, command and control; core cyber-intelligence capability; cyber empowerment and dependence; cyber security and resilience; global leadership in cyberspace affairs; and offensive cyber capability. On the basis of these parameters, countries have been divided into three categories: Tier One covers countries that have "*world-leading strengths*" in all spheres. According to the report, the USA is the only country to be included in this Tier One category. Tier Two countries, with "*world-leading strengths in some of the categories*" are: Australia, Canada, China, France, Israel, Russia, and the United Kingdom. Finally, Tier Three countries are those that have "*strengths or potential strengths in some of the categories but significant weaknesses in others*," i.e. India, Indonesia, Iran, Japan, Malaysia, North Korea, and Vietnam.[64]

As previously mentioned, cyberspace is a term but also a strategic tool; thus, it is believed that anyone who controls the content of cyberspace will also shape the future. E.g., according to F. Hoffman, there is a growing concern with regard to cyberwars;[65] nevertheless, no consensus has yet been reached as to the basic principles of a strategic framework for the use of cyber capabilities that would give states an advantage in times of conflict. In consequence, it can be concluded that cyber capabilities should be combined with other political tools, such as economic sanctions, conventional military force, etc. B. Valeriano, B. Jensen, R. Manes, and F. Rare indicate three strategies of using cyber capabilities:

- the first is a strategy of Internet disruption;
- the second is cyber espionage;
- the third is related to cyber degradation, associated with severe damage and high costs.

In their opinion, it is difficult to separate cyber capabilities from other political tools, as this would require overcoming a number of obstacles, including the integration of cyber capabilities with conventional forces. The fight for control over cyberspace may therefore become the dominant form of strategic competition in the age of information. This seems particularly relevant in light of the fact that already in modern times, there is fierce competition between

[64] *Cyber Capabilities and National Power: A Net Assessment,* International Institute for Strategic Studies, 28 June 2021.

[65] Cyberwar, a kind of destructive (disorganising) cyber conflict with political goals at the state level. *Cyberwojna, Biuro Bezpieczeństwa Narodowego* (National Security Bureau), https://www.bbn.gov.pl/pl/bezpieczenstwo–narodowe/minislownik–bbn–propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow–z–dziedziny-bezpieczenstwa.html, access: 21.08.2021; *Security Threat Report Mid-year 2010,* Sophos 2010; D. Gardham, *Hackers recruited to fight „new cold war",* http://www.telegraph.co.uk/technology/news/6727100/Cold-war-enemies-Russia-and-China-launch-a-cyber-attack-every-day.html, access: 22.08.2021.

individual countries to maximise the benefits resulting from its military and economic advantage.[66]

As the issue of cybersecurity has undergone many significant changes in recent years, including from technical aspects to strategic issues related to national and international security, the cybersecurity rules system is also facing the challenge of reconstruction.[67] The system of strategic goals in cyberspace during a possible war can be divided into two levels, i.e. the government level and the military level. The overall strategic goals of the government include, *inter alia*, minimising the risk of using cyber weapons to commit hostile acts and acts of aggression that undermine national (state) sovereignty, undermine territorial integrity, and threaten international peace, security and strategic stability.

The strategic goal at the military level has become to stop, prevent, and solve the armed conflicts in cyberspace. To this end, the armed forces should:

- first, have a fully operational cyberspace security system,
- second, have combat capabilities in cyberspace in order to effectively respond to threats in cyberspace,
- third, continuously monitor any potential armed conflict in cyberspace,
- fourth, react effectively whenever a conflict in cyberspace escalates or enters a crisis.[68]

The analysis carried out by S. Mele shows that there are 13 strategic pillars that constitute the basis of strategic thinking and action in cyberspace, i.e.:

1. identification and classification of the protected critical infrastructure;
2. establishment of national and/or international treaties, laws and rules of conduct;
3. developing diplomatic relations and strengthening international partnership;
4. focusing on the protection of fundamental rights, privacy rights and/or freedom of expression;
5. concentration on cybercrime;
6. treating cyberspace as a domain of warfare;

[66] W. Hoffman, *Is Cyber Strategy Possible?,* "The Washington Quarterly" 2019, Vol. 42, No. 1, pp. 131-152.

[67] L. Chuanying, *The International Rule System of Cyberspace and the New Type of Sino-U.S. Relations between Great Powers,* http://theory.people.com.cn/n1/2016/1202/c386965-28920732.html, access: 16.08.2021.

[68] *Research on the Construction of Russian Cyberspace Warfare,* https://www.secrss.com/articles/8215, access: 20.08.2021.

7. creating appropriate political and decision-making structures to counteract this threat;
8. developing deterrence to prevent conflict in cyberspace;
9. increasing the level of security, reliability and resilience of networks and information systems;
10. enhancing the exchange of information, including between public and private entities, as well as capacities in respect of early warning and incident response;
11. increasing the public awareness of the threat and the importance of cybersecurity;
12. creating and/or increasing the number of security organisations,
13. encouraging innovation, research and development.[69]

This is quite relevant as the course of actions in asymmetric conflicts implies challenges in the form of cyberspace protection and defence, and providing civil and military sector personnel with increasing IT knowledge to work with new technologies. The cooperation of multinational teams, e.g. within the Alliance or other organisations, regarding the building of cybersecurity potential (under various political, economic conditions and management methods) is of particular importance.[70] J. Chipman, director of the International Institute for Strategic Studies, believes that the greatest challenge is the development of intellectual strategic thinking that should correspond to technological development. Just like after the invention of the atomic bomb in the 1950s new international tools and resources were developed to deal with nuclear relations, today there is a great need for thinking (political and military), e.g. on the Internet, to also develop in this way. Furthermore, he believes that in the coming years we will witness the armed forces being re-armed so as to equip them with the appropriate capabilities that will be effective in digital war.[71]

It should be emphasised, however, that when addressing the issue of strategic changes – and thus, in the most general sense, of strategic thinking – many authors put forth a hypothesis about the inability of today's elites to make this type of changes. Those authors argue that, in order to prepare and implement changes in strategic thinking, new and different people are needed in the organisation, "...*a change of guard in management*" is necessary,[72] meaning that change in strategic thinking is needed. "...*We need a system where an evolutionary shift of guard will be made in the traditional structures of power,*

[69] S. Mele, *I principi strategici delle politiche di cybersecurity, op. cit.*

[70] R. Zwilling, *Boxer: The GTK Multirole Armoured Wheeled Vehicle in Modern German Army Service*, Verlag Jochen Vollert - Tankograd Publishing, Erlangen 2012, pp. 2-4.

[71] *Davos 3: Krigen i cyberspace,* https://www.mm.dk/artikel/davos-3-krigen-i-cyberspace, access: 23.08.2021.

[72] M. Crozier, *Kryzys inteligencji. Szkic o niezdolności elit do zmian*, Poltext, Warsaw 2002.

career and leadership."[73] One of the main distinguishing features of people in new management should therefore be the awareness that change is not (cannot) be a threat! It may, admittedly, give rise to threats, but above all, it is an opportunity!

Bringing the above reflection into the area of strategic change can be done by formulating a sequence of derivative theses – statements that determine the general way of thinking about, perceiving and solving the problem:

- a change of civilisation or world order forces radical changes in people and changes in our organisations (their essence, meaning, value, purpose, and shape);
- a different meaning of human life and activity, as well as different organisations lead to a different management, and a different management means a different view of its functions (including planning), their essence, rank, content, principles, methods, techniques, and tools,
- different functions, methods, techniques, and tools are the need for different knowledge, skills, personal characteristics ("different people") and different structures, processes and mechanisms,
- different performers, different structures and processes under different conditions are different products and criteria for their evaluation.

Thus, the description of change in strategic thinking in cybersecurity, showing its essence, character and nature, should come down to looking for permanent development trends in "abstracted" planes, which in the future may have a significant impact on the development of the world, individual civilisations, the structure of the international order, or directions of world politics. These tendencies can now be identified in three spheres (dimensions): technological, organisational and structural, and in the sphere of values.[74] However, the overlapping and interconnecting changes occurring in these spheres demonstrate the regularity of permanent development trends, which strongly affect societies, organisations and individuals.[75] And since the above dimensions are to create the security of the future world, one can assume that strategic thinking also should not remain indifferent to the process of creating cybersecurity of all entities and objects, including the formulation of security strategies for countries and organisations creating a strategic security environment. The increase

[73] U. Muller, *Zmiana warty w zarządzaniu,* Placet, Warsaw 2000.

[74] This methodology was drawn from the publication "Funky Business: Talent Makes Capital Dance" by two Swedish analysts J. Ridderstrale and K. Nordstrom, who, with technological, institutional (structural) changes and transformations in the value system, tried to sketch the general character of the world. J. Ridderstrale, K. Nordstrom, *Funky biznes. Taniec talentu z kapitałem,* WIG Press, Warsaw 2001.

[75] M. Kozub (ed.), *Dydaktyka strategicznego i operacyjnego planowania sił zbrojnych*. Studium teoretyczne, AON, Warsaw 2008.

in the novelty and intensity of these changes may, as a result, also lead to an increasingly frequent loss of management continuity and the emergence of the phenomenon of *strategic surprise*, caused e.g. by an increasing number of events, often more significant for our existence (functioning) and development abilities, which we not only do not take into account, but also do not include in the information base of our design and implementation activities. Such situations may mean that in such a complex, but also increasingly more interdependent and asymmetric security environment, as claimed by analysts specialising in strategic management, these changes, also in cybersecurity, should be expected and searched for in the "periphery." That is because it is these places that pose and will pose – not only today, but also in the future – challenges for strong, deeply rooted, but simultaneously ponderous structures, from small dynamic organisations, full of creativity and innovation in action and able to bear greater risks.

SUMMARY

Over the past two decades, there has been a reorientation of strategic thinking: war is no longer defined solely in terms of pure military confrontation, but is also fought using non-military tools, including cyber tools. Cyberspace itself has become a highest-level strategic concept, used in military doctrines and international negotiations.[76] The 21st century is anticipated to be a period of proliferation in the use of electronic weapons,[77] and cyberspace itself – to become a field of competition, alongside land, sea, air, and space, making the continuous evolution of cybersecurity strategies inevitable. Furthermore, digitisation is constantly evolving, and new cyber threats and challenges continue to arise. In the context of this progress, cybersecurity must be an integral and indivisible part of the process and system of national and international security. States need to be aware of their current level of cybersecurity capabilities and, simultaneously, identify areas where this cybersecurity needs to be strengthened. One might say that cybersecurity is a continuous "armaments race" between countries, but also between the security environment and hostile hackers. Cybersecurity is a complex challenge that encompasses many different management, policy, operational, technical and legal aspects,[78], therefore "*it is imperative that modern cybersecurity strategies change from prevention to response. This means not only ensuring appropriate cybersecurity policies*

[76] A. Desforges, *Les représentations du cyberespace : un outil géopolitique,* "Hérodote" 2014/1-2 (n° 152-153), pp. 67-81.

[77] *Cyberspace and weapons of mass proliferation between deterrence and the arms race, op. cit.*

[78] M. Lehto, *Strategic leadership in cyber security, case Finland,* "Information Security Journal: A Global Perspective" 2021, Volume 30, Issue 3, pp. 139-148.

and procedures, but also managing detection and response so as to ensure that states are prepared for the worst."[79] In addition, states should attach great importance to building the capabilities of a strategic early warning system in cyberspace,[80] the more so as the most developed countries are also the most vulnerable due to the increase in interconnections of computer networks necessary for the nation's lives. Considered to be the "nervous system" of states, networks have become a serious problem for them.[81]

Considering the above, the fight and prevention against cyber-attacks related to cyber conflicts or cybercrime requires strengthening the resilience of infrastructure, the development of adapted human, organisational, legal and technological capacities, and the mobilisation of all entities in society. It should also be added that cybersecurity is not solely a matter of the state or government strategy. No white paper or military doctrine can compensate for the lack of individual and collective responsibility of civil society and the lack of effective partnerships between the private and public sectors.[82]

REFERENCES

[1] Alwani M., *A culture of strategic thinking. Visions and principles,* https://www.rowadalaamal.com, access: 19.08.2021.

[2] Beaufre A., *An Introduction to Strategy,* Frederick A. Prager. LCCN 65014177, 1965.

[3] Chuanying L., *The International Rule System of Cyberspace and the New Type of Sino-U.S. Relations between Great Powers,* http://theory.people.com.cn/n1/2016/1202/c386965-28920732.html, access: 16.08.2021.

[4] Cichosz J., *Polityka cyberbezpieczeństwa Rzeczypospolitej Polskiej,* PhD dissertation, UJK, Kielce 2019, p. 202.

[5] *Creating and rolling out an effective cyber security strategy,* https://www.information-age.com/creating-rolling-out-effective-cyber-security-strategy-123494607/, access: 25.08.2021.

[6] Crozier M., *Kryzys inteligencji. Szkic o niezdolności elit do zmian,* Poltext, Warsaw 2002.

[79] *Creating and rolling out an effective cyber security strategy,* https://www.information-age.com/creating-rolling-out-effective-cyber-security-strategy-123494607/, access: 25.08.2021.

[80] *Thoughts on the Construction of Strategic Early Warning System in Cyberspace,* https://new.qq.com/omn/20210603/20210603A00ZA100.html, access: 25.08.2021.

[81] A. Desforges, *Les représentations du cyberespace : un outil géopolitique, op. cit.*

[82] S. Ghernaouti-Hélie, *Menaces, conflits dans le cyberespace et cyberpouvoir*, "Sécurité et stratégie" 2011/3 (7), pp. 61-67.

[7] *Cyber Capabilities and National Power: A Net Assessment,* International Institute for Strategic Studies, 28 June 2021.

[8] *Cyber Crime Study 2017 Insights on the Security Investments that make a difference,* https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf, access: 20.08.2021.

[9] *Cyberspace and weapons of mass proliferation between deterrence and the arms race,* https://seconf.wordpress.com/2015/05/15/, access: 03.08.2020.

[10] *Cyberwojna,* Biuro Bezpieczeństwa Narodowego (National Security Bureau), https://www.bbn.gov.pl/pl/bezpieczenstwo–narodowe/minislownik–bbn–propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow–z–dziedziny-bezpieczenstwa.html, access: 21.08.2021.

[11] Daniluk P., *Myślenie strategiczne w naukach o bezpieczeństwie,* http://www.dsw.edu.pl/fileadmin/user_upload/wydawnictwo/RBM/RBM_artykuly/20127.pdf, access: 12.08.2021.

[12] *Davos 3: Krigen i cyberspace,* https://www.mm.dk/artikel/davos-3-krigen-i-cyberspace, access: 23.08.2021.

[13] Desforges A., *Les représentations du cyberespace : un outil géopolitique*, "Hérodote" 2014/1-2 (n° 152-153).

[14] *Doc. XXXIV n. 4,* https://www.camera.it/_dati/leg16/lavori/documentiparlamentari/indiceetesti/034/004/d020.htm, access: 12.08.2021.

[15] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej,* BBN (National Security Bureau), Warsaw 2015.

[16] Gadacz T., *Bez mądrości zginiemy,* "Gazeta Wyborcza", 30-31.08.2014.

[17] Gardham D., *Hackers recruited to fight „new cold war",* http://www.telegraph.co.uk/technology/news/6727100/Cold-war-enemies-Russia-and-China-launch-a-cyber-attack-every-day.html, access: 22.08.2021.

[18] Ghernaouti-Hélie S., *Menaces, conflits dans le cyberespace et cyberpouvoir,* "Sécurité et stratégie" 2011/3 (7).

[19] Gibson W., *Neuromancer,* Ace Books, New York 1984.

[20] Gurza S., *Cyberbezpieczeństwo Indii: spojrzenie na podejście i gotowość,* https://www.icwa.in/show_content.php?lang=2&level=3&ls_id=6187&lid=4245, access: 14.08.2021.

[21] Hoffman W., *Is Cyber Strategy Possible?,* "The Washington Quarterly" 2019, Vol. 42, No. 1.

[22] *How to improve and acquire strategic thinking,* https://www.roberthalf.jp/ja/career-advice/career-development/strategic-thinking-skills, access: 18.08.2021.

[23] Karpiński A., *Co trzeba wiedzieć o studiach nad przyszłością?,* PTE, Warsaw 2009.

[24] Kavanagh C., Maurer T., Tikk-Ringas E., *Baseline Review ICT- related process and events implications for international and regional security (2011-2013),* ICT4PEACE Foundation, Geneva, 2014.

[25] Kissinger H., *Porządek światowy,* Wydawnictwo Czarne, Wołowiec 2016.

[26] Klimburg A., *National Cyber Security Framework Manual,* NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2012.

[27] Kotarbiński T., *Traktat o dobrej robocie,* Ossolineum, Wroclaw 1982.

[28] Kozub M. (ed.), *Dydaktyka strategicznego i operacyjnego planowania sił zbrojnych. Studium teoretyczne*, AON, Warsaw 2008.

[29] Kozub M., *Bezpieczeństwo przyszłości jako efekt synergii myślenia i działania strategicznego,* [in:] *Edukacja obronna kierowniczej kadry administracji publicznej w ramach WKO – Doświadczenia i wyzwania*, ed. W. Kitler, S. Olearczyk, Z. Piątek, Ruch Wspólnot Obronnych, Warsaw 2014.

[30] Kozub M., *Konflikty początku XXI wieku. Użycie sił powietrznych,* AON, Warsaw 2007.

[31] Kozub M., Mitręga A., *Podstawy strategii bezpieczeństwa. Wybrane aspekty,* UJK, Kielce 2018.

[32] Kozub M., *Myśleć strategicznie o bezpieczeństwie przyszłości,* AON Warsaw 2013.

[33] Kozub M., *Strategiczne środowisko bezpieczeństwa przyszłości. Kierunki ewolucji oraz możliwe teorie i prognozy dla bezpieczeństwa RP do końca trzeciej dekady XXI wieku,* AON, Warsaw 2016.

[34] Kozub M., *Strategiczne środowisko bezpieczeństwa w pierwszych dekadach XXI wieku,* AON, Warsaw 2009, p. 72.

[35] Lehto M., *Strategic leadership in cyber security, case Finland,* "Information Security Journal: A Global Perspective" 2021, Volume 30, Issue 3.

[36] Liedtka J., *Łączenie myślenia strategicznego i planowania strategicznego*, "Strategia i przywództwo" 1998, No. 26 (4).

[37] Limonier K., *Russia in Cyberspace: Issues and Representations,* "Hérodote" 2014, No. 1.

[38] Lynn III W. J., *Defending a New Domain: The Pentagon's Cyberstrategy,* "Foreign Affairs" 2010.

[39] *Management strategique de PME/PMI*, Guide methodologique, Economica, Paris 1991.

[40] Mele S., *I principi strategici delle politiche di cybersecurity,* https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-delle-politiche-di-cyber-security.html, access: 10.08.2021.

[41] Menon N., *The Potential Impact of Cyber Capabilities on Future Strategy,* https://www.e-ir.info/2021/05/05/the-potential-impact-of-cyber-capabilities-on-future-strategy/, access: 21.08.2021.

[42] Mika J., *Strategie a strategické myšlení,* [in:] *Vojenská Strategie,* ed. V. Galatík, A. Krásný, K. Zetocha, Univerzita Obrany, Ministerstvo obrany České republiky – PIC MO, 2008.

[43] Mintzberg H., *Strategy Formulation As A Historical Process,* "International Studies of Management & Organization" 1977, Vol. 7, No. 2.

[44] Mintzberg H., *The Fall and Rise of Strategic Planning,* "Harvard Business Review" 1994.

[45] Mróz A., *Strategiczne podejście do myślenia o przyszłości w bezpieczeństwie narodowym. Metodologia strategicznych studiów nad przyszłością w bezpieczeństwie narodowym. Studium teoretyczne*, AON, Warsaw 2016.

[46] Muller U., *Zmiana warty w zarządzaniu,* Placet, Warsaw 2000.

[47] *Nauki o bezpieczeństwie* (Security sciences), https://pl.wikipedia.org/wiki/Nauki_o_bezpiecze%C5%84stwi, access: 12.08.2021.

[48] Penc J., *Zarządzanie dla przyszłości,* PSB, Krakow 1998.

[49] *Préparer le futur : la cyberdéfense et le nouveau concept stratégique,* https://www.nato.int/cps/en/natohq/news_77515.htm?selectedLocale=fr, access: 10.08.2021.

[50] *Program Polski Ład,* Warsaw 2021.

[51] Pszczołowski T., *Mała encyklopedia prakseologii i teorii organizacji*, Ossolineum, Wroclaw 1978.

[52] *Research on the Construction of Russian Cyberspace Warfare,* https://www.secrss.com/articles/8215, access: 20.08.2021.

[53] Ridderstrale J., Nordstrom K., *Funky biznes. Taniec talentu z kapitałem,* WIG Press, Warsaw 2001.

[54] Rokita J., *Problemy zarządzania w warunkach nowej ekonomii,* [in:] *Zarządzanie strategiczne w warunkach nowej gospodarki,* ed. J. Rokita, W. Grudzewski, Wyd. Górnośląskiej Wyższej Szkoły Handlowej, Katowice 2007.

[55] *Security Threat Report Mid-year 2010*, Sophos 2010.

[56] Snyder J. L., *The Soviet Strategic Culture : Implications for Limited Nuclear Operations*, RAND, Santa Monica 1977.

[57] *Strategic thinking gives purpose to life,* https://wonderfulmind.co.kr/strategic-thinking-how-to-give-your-life-purpose/, access: 19.08.2021.

[58] *Strategic thinking... its characteristics and importance,* https://www.saharamedias.net/3420, access: 19.08.2021.

[59] *Strategický Manažment,* https://gtk.uni-miskolc.hu/files/5043/STRATEGICK%C3%9D%20MANA%C5%BDMENT.pdf, access: 18.08.2021.

[60] *Strategy for Operating in Cyberspace,* Department of Defense, July 2011.

[61] Szubrycht T., *Analiza podobieństw operacji militarnych innych niż wojna oraz działań pozwalających zminimalizowana zagrożenia asymetryczne,* "Zeszyty Naukowe Akademii Marynarki Wojennej" 2006, No. 1 (164).

[62] *The deep connotation of strategic thinking and the value of the times,* http://www.qstheory.cn/llwx/2019-07/09/c_1124727205.htm, access: 20.08.2021.

[63] *The threat from the internet: Cyberwar,* http://www.economist.com /node/16481504?story_id=16481504, access: 05.08.2021.

[64] *Thoughts on the Construction of Strategic Early Warning System in Cyberspace,* https://new.qq.com/omn/20210603/20210603A00ZA100.html, access: 25.08.2021.

[65] Zwilling R., *Boxer: The GTK Multirole Armoured Wheeled Vehicle in Modern German Army Service,* Verlag Jochen Vollert - Tankograd Publishing, Erlangen 2012.

[66] Анисимов О. С., *Мышление стратега: модельные сюжеты. Выпуск 21. Стратегическое мышление и цивилизация,* http://www.metodologika.ru/node/192, access: 20.08.2021.

[67] *Киберпространство как стратегический инструмент социальной инженерии,* https://whatisgood.ru/theory/analytics/kiberprostranstvo-kak-strategicheskiy-instrument/, access: 15.08.2021.

[68] *Стратегическое мышление старшеклассников (будущих руководителей) как фактор общего роста России,* https://mgpu-media.ru/issues/issue-21/psycho-pedagogical-science/strategic-thinking.html, access: 16.08.2021.