HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 4. szám

FEKETE CSANÁD[1]

The Strategic Aspects of Information Warfare

Az információs hadviselés stratégiai kérdései

Abstract

Events of recent years made the issue of information warfare the central of attention, which, with the emergence of modern information societies, became a fundamental security threat to the states. Today, the information environment became a global arena where states and non-state actors continuously fight with each other in order to further their strategic interests. In this paper, I will try to paint a comprehensive picture of these conflicts, the nature of their complex information operations and their impact on the public sector.

Keywords: information warfare, future of armed conflicts, 21st century warfare

Absztrakt

Az elmúlt évek eseményei az érdeklődés középpontjába állították az információs hadviselés kérdéskörét, amely korunk információs társadalmainak kialakulását követően az államok alapvető biztonsági fenyegetésévé lépet elő. Az információs környezet napjainkra egy olyan globális küzdőtérré változott, ahol az államok és államszint alatti szereplők folyamatos harcot vívnak egymással, stratégiai érdekeik előmozdítása céljából. Cikkemben ennek figyelembevételével igyekszem átfogó képet nyújtani a konfliktusok információs tartományáról, az ott folyó komplex műveletek természetéről és azok állami szektorra gyakorolt hatásairól.

Kulcsszavak: információs hadviselés, jövő fegyveres konfliktusai, 21. századi hadviselés

[1] Nemzeti Közszolgálati Egyetem, Nemzetközi és Európai Tanulmányok Kar, Nemzetközi Biztonsági Tanulmányok Tanszék, tanársegéd, National University of Public Service, Faculty of International and European Studies, Department of International Security Studies, assistant lecturer. E-mail: fekete-csanad@uni-nke.hu ORCID: 0000-0002-9873-4736

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 4. szám

A SHORT REVIEW OF THE SECURITY ENVIRONMENT OF THE 21ST CENTURY

The rapid technological development and social transformation of the last two decades had a significant impact on warfare. The emergence of new types of security and military threats in the 21st century caused the most significant changes, which made a great impact on the military transformation processes, resulted changes in the structure and equipment of the armed forces. In today's complex security environment, terrorism, the proliferation of weapons of mass destruction (WMD), cyber- and hybrid warfare are the main threats facing the Euro-Atlantic area. Despite the fact that certain tendencies can be identified, it is very difficult to draw precise conclusions about the near and far future. Regarding this issue, Zoltán Szenes, the former chief of staff of the Hungarian Defense Forces had the following to say:

"The past one and a half decades have been characterized by unpredictability in terms of security… The armed conflicts of the one-polar-world did not remain within the traditional framework of conventional warfare between rival states." [2]

The above quotation shows that Western armed forces preparing to fight traditional interstate wars during the Cold War had to face completely new problems and challenges in the post-Soviet era. In a progressively changing world of accelerating globalization and technological development, space and time condenses, conflicts often cross geographic borders, and their consequences also affect distant parts of the world.

With the emergence of new types of challenges, more and more attention is being paid to intra-state conflicts, in which increasingly strong non-state actors are expanding their activities to several countries, thus threatening the stability of entire regions. This process was noticed by many civilian researchers and military experts, developing theories on the new forms of warfare.[3] From their examination, it can be identified that the characteristics of recent armed conflicts has undergone changes that require a different approach. The new types of asymmetric conflicts in the world in most cases go beyond the borders of the given country, the radical terrorist organizations involved, such as Al-Qaeda or the Islamic State directly threaten the societies and lifestyles of developed western democracies. Through the activities of international terrorist organizations and criminal groups, the distinction between peace and war has blurred and no longer so clear today. This trend proven by the recent bloody terrorist attacks across the globe.[4]

---

[2]SZENES Zoltán: Katonai kihívások a 21. század elején, Budapest, Hadtudomány, XV.évf. 4. sz. 2005

[3] Among others, see:
HAMMES Thomas X.: War evolves into the fourth generation, Contemporary Security Policy, 26.évf. 2. sz. 2005
HOFFMAN Frank G.: Conflict in the 21st century, Arlington, VA, Potomac Institute for Policy Studies, 2007

[4] Despite the many conflicts in the world, most analyses suggest that in the near future there is still little chance of the eruption of a major inter-state war, and the use of armed forces is likely to continue in smaller local conflicts under asymmetric conditions. For a comprehensive statistical survey of the

At the same time, however, a more significant process has taken place around the world that had an affect on all sectors of security. Because of the revolutionary development and widespread use of information and communications technologies (hereinafter referred to as: ICT) and the phenomenon of globalization accelerating in part because of these, the technological, economic and social sectors have undergone radical changes that have brought humanity to the dawn of a new information era. The recent technological advances and the information space[5] created by the horizontal spread of ICT became one of the main fields of struggle between states and non-state actors, the outcome of which can affect the function of the government and the operation of the economy, and as a worst-case scenario can even undermine the social stability of the affected states. In the next part of my paper, I will deal with the emergence of the information age and its impact on warfare, which I hope will help to better understand the attacks carried out with information tools and highlight the potential threats they pose.

1. THE TRANSFORMATION OF WARFARE IN THE INFORMATION AGE

The information revolution has fundamentally changed the nature of conflicts, to illustrate we should look back to the last years of the Cold War. In order to understand the major changes in recent past, we need to look at the nature of war more closely. The most important and most quoted author of this topic is Carl von Clausewitz of Prussian origin, who in his 1832 book titled "*On War*" created the most comprehensive and in many respects even presently valid definition of war. According to Clausewitz's famous theorem, war is nothing more than: "an act of *violence* to *compel* our *opponent* to fulfil our *will.*"[6]Clausewitz understood violence as the use of physical force, – the instrument of which is the armed force –, which is a tool in the hands of politics to reach its set objectives.

With regard to the tools available in war, he states that in the end there is only one form of it, combat: "*all that takes place in war takes place through armed forces.*"[7]In this sense, obtaining war objectives can only be achieved through the use of armed forces, physical violence, and battle. In Clausewitz's view, the outcome of war is essentially determined by battles and the combat within, which are the basis of the actual war effort and everything else is subordinated to them.[8]

---

frequency of major inter-state wars, see: Aaron Clauset: The Enduring Threat of a Large Interstate War

[5] Under information space, I mean the multidimensional spectrum of the global information environment that includes the interconnected ICT infrastructures and systems and the virtual space made up by the services they provide – the *cyberspace* – as well as the *cognitive space* made up of people's "mind" and cognitive processes. In this sense, the information space is a set of information systems, processes, resources and infrastructures where states and non-state actors are fighting each other with non-kinetic, information and cognitive attack techniques and methods.

[6]CLAUSEWITZ Carl Von: A háborúról, Budapest, Zrínyi Kiadó, 2013

[7] Ibid, p. 64.

[8] Ibid, p. 230.

The destruction of the opposing armed forces is thus a means of achieving the goal of the battle – victory –, according to which, the basis of the war effort is the destruction of the enemy. The ultimate goal of the war effort is to make the enemy unable to defend by means of disarming or defeating their armed forces, breaking their will and taking possession of their territory.[9]War is therefore a conflict between the interests of states, resolved in violent form and with blood, and this is what differentiates war from other conflicts.

Based on the above quotations we can make several observations: states aim to achieve their objectives primarily by means of violence, the main tool in Clausewitz's era was the armed forces, so the states forced their will on to others by means of arms and the usage of physical force. In this sense, however, war itself is a tool in the hands of politics, which is used to protect its interests and to enforce its will. If we accept this statement and take into account the changes and technological development of the last century, we can see that certain observations by Clausewitz – with the exception of the fundamentals – are now in need of major revision. Because today, states are able to enforce their will with countless other – violent – means besides military force, although the armed forces and war remain a major part of the toolset for enforcing their interests – the "*final argument*" for resolving conflicts. In previous centuries – and even in the mid-twentieth century – military force was the main enforcing tool of states, so research concerning security and strategy focused mainly on the military dimension. Today, however, new – more precisely renewed – tools have emerged and become part of the state toolset, with which the will of the opposing side can be broken, and the set objectives can even be achieved without physical combat. In this regard, it is worth distinguishing between two concepts, direct warfare which aims to destroy the enemy and indirect warfare which aims to exhausting the enemy.[10]The former is based on the direct engagement of forces, while the latter is based on drawing the struggle out and the avoidance of a decisive battle. One wants to defeat the other side in combat while the other wants to exhaust the enemy as much as possible and break the enemy will to fight. From this point of view, military forces are means for a state's direct warfare, while diplomatic, information or economic tools are its means of indirect warfare.

The view of physically destroying enemy forces based on direct military tools began to shift in the second half of the Cold War – primarily in the West – with the rapid development in the field of information technologies. As a result, a new military-technical revolution was born with a focus on high-precision weapon systems, space-based intelligence, surveillance, and reconnaissance systems, automated command and control, communication and information systems. The mass usage of these tools and the first debut of the operational planning concept reflecting the new approach was during the Gulf War in 1991. All this was a forerunner of a whole new era, demonstrating the profound changes in warfare.[11]

[9] Ibid, p. 40-41.
[10] Ibid, p. 31.
[11] Through advanced information technology systems and sensors, network-based warfare is being realised in the 21st century, in which the military command and control system as well as weapon

These processes initially mostly affected the air force, and the most important innovations were implemented in the fields of military operations planning and the target acquisition. In the introduction of the new approach, John Warden, colonel of the United States Air Force, gained undeniable merit by creating a new model in his 1995 paper, which identifies the Enemy as a System. Warden depicted the strategic subsystems of society with five concentric circles, in which the political leadership has its place in the inner core, followed by, inside outwards, the subsystems that are essential for running the economy, the infrastructure, the population and finally the armed forces in the outermost ring.

According to the author, when selecting the targets, one should strive to acquire them as close as possible to a strategically important center, so the air strikes will allow swift obtainment of the desired end state and the resolution of given conflict.[12]

According to Warden, the main tool for achieving the objectives is through coordinated, mass and simultaneous strikes[13] at the strategic Center of Gravity (COG)[14] of the opposing side subsystems, by which the command and control system located in the center can be paralyzed, which will interfere with the proper functioning of each subsystem, triggering the phenomenon of Strategic Paralysis. During the execution of the operations, the principle of inside outwards and not outside inwards should prevail. The attack of the central subsystems is intended to break the resistance of the enemy. Additionally, it is important new aspect that during the operation planning process one must first identify the desired end state, then the essential strategic centers of gravity, the paralyzation of which will require the identification of additional targets.[15]

---

systems operating on the battlefield are organized into interconnected real-time network-grids. All this significantly reduces reaction time and increases operational efficiency, which means that the set objectives can be achieved by the deployment of less force. SZABÓ József: Kis magyar hadelmélet illetve mire készítsük fel a honvédtiszteket a XXI. században, Hadtudományi Szemle, V.évf. 3-4. sz. 2012.

[12] For more information see: WARDEN John: Air Theory for the Twenty-First Century, Airpower Journal, 1995.

[13] These strikes are carried out by the Air Force – and, to a lesser extent, by the Navy – with the mass usage of high-precision weapon systems and unmanned aerial vehicles.

[14] The strategic center of gravity (COG) is a well-defined center of enemy subsystems, the paralyzation of which causes a degree of disruption in other subsystems that paralyzes the entire society of the opposing side. For more information, see: KRAJNC Zoltán, GÖNCZI Gabriella: Korunk meghatározó légierő teoretikusa: John A. III. Warden, Hadmérnök, V.évf. 1. sz. 2010. p. 355.

[15] With the further development of Warden's enemy as a system and five rings model, the so-called Effect Based Operations (EBO) concept was created. The bottom line of this is that, in order to achieve the desired end state, instead of the direct effects – the destruction of a given target –, the emphasis is placed on secondary and tertiary – indirect – effects, which are synchronized with the desired end state. Effect based operations do not have a unified definition, it can be best interpreted as an approach and planning methodology. For more information, see: KRAJNC Zoltán, GÖNCZI Gabriella: A légi hadjáratok (műveletek) stratégiai szintű tervezésének és az üzleti (vállalati) stratégiaalkotásnak a konvergenciája (egy. PhD-témaválasztás indoklása)., Szolnok, Repüléstudományi Konferencia, 2009. p. 10.

At the time of the model's creation, strategic paralysis could only be achieved via kinetic means – long-range and deep strike capabalities employed by the air and naval forces –, as a comprehensive information infrastructure has not yet been built up during this period that would ensure the functioning of the various subsystems and the flow of information between them.[16]

However, the change of strategic importance in recent years was precisely that the strategic paralysis of the target country can be achieved by non-kinetic means too. For this, however, two basic conditions needed to be fulfilled: first it was necessary to create a complex information infrastructure that constitutes the backbone of information societies, which ensures the operation of the various subsystems and the flow of information between them, in the meantime, the principles and methods of engagement in the new information environment had to be worked out. Due to the rapid technological development of the past two decades the vital information infrastructures became the strategic centers of gravity of information societies, so by attacking these – with minimal physical damage – strategic paralysis and the breaking of the enemy's will can be achieved. In the rest of the paper, I will first discuss the role of information infrastructures, and then present the concept of so-called strategic information warfare.

2. INFRASTRUCTURES OF INFORMATION SOCIETIES

The backbone of our modern societies is made up of infrastructures[17] that include all the institutions, facilities, equipment, services and experts required for the undisrupted operation of state, social and economic functions. All the explanations and definitions[18] developed over the years interpret infrastructure as a complex system, which, as a coherent network, contributes to a country's security and the survival of society.

When ranking infrastructures, it is worth considering national security aspects as well, on the basis of which the concept of critical and vulnerable infrastructures[19] (hereinafter referred to as: CI) gained recognition is recent years, which are indispensable for the func-

[16] With the emergence of these, the vital information infrastructures became the strategic centers of gravity of information societies, so by attacking these – with minimal physical damage – strategic paralysis and the breaking of the enemy's will can be achieved.

[17] These include telecommunications, transport, trade, education, health care and various public utilities.

[18] For more information on the different definitions of infrastructures, see: HAIG Zsolt. et al.: A kritikus információs infrastruktúrák meghatározásának módszertana, Budapest, ENO Avisory Kft, 2009.p. 23-24.

[19] Critical infrastructure, in general terms, is *"all infrastructures (the sum of operating personnel, processes, systems, services, facilities, and tools) whose destruction, loss of services or availability has a significant negative impact on the existence, conditions of existence and operation of a given user circle. Within this general concept of critical infrastructure, depending on the user circle concerned, we need to distinguish between specific concepts such as national critical infrastructure, European critical infrastructure, [national] defense/military critical infrastructure, federal critical infrastructure, or organizational critical infrastructure."* Source: Ibid, p. 36.

tioning of society. On one hand, CIs enable the production and transportation of essential goods, and the access to vital services, on the other hand, ensure the communication link between the various infrastructural elements of economy and society, and finally, they contribute to the public security and external protection of the country.[20] In the event of a disruption in the normal operation of the ICs, invaluable damage can be caused to the economic performance, political and social stability, and defense capabilities of the given state. Therefore, it is a key task for governments to identify and designate the CIs they wish to protect, which presents many difficulties – as no definitive definition has been established so far, and their identification falls under the exclusive competence of the states.

Despite the difficulties, ensuring the continuous and undisrupted operation of the CIs has become a priority of strategic importance for states in recent years. As part of this, significant advances have been made on both domestic[21] and international level in the identification and protection of vital systems.[22]

With the emergence of information societies and the development of information systems that permeates all aspects of life, the possible division of infrastructures has also changed, according to this, nowadays *general* and *information* infrastructures – that are in many respects overlapping and in close connection – can be distinguished.[23] Besides physical components, information infrastructures can be divided into other important components, from the users' point of view, including: *the information*, generated in electronic information systems of government agencies and other organizations, *softwares* and *applications* that enable access to different services, *network standards* and *transmission codes* that enable communication between information tools, and the human sphere operating

[20] For more information, see: HAIG Zsolt. et al.: Kritikus infrastruktúrák és kritikus információs infrastruktúrák, Budapest, Nemzeti Közszolgálati Egyetem, 2012. p. 46.
[21] The list of vital systems and facilities of Hungary are detailed in Act CLXVI of 2012. For more information, see: 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről,
[22] In recent years, a number of recommendations and guidance have been created, the NIS directive of 2016 on unified security regulation of network and information systems, which stipulates essential requirements for the European Union and its Member States regarding information security and the identification and protection of critical infrastructures. This directive is the first to set out a framework for community-level cooperation and institution system, furthermore, it assigns specific tasks to Member States in the field of information security, setting a minimum level of capability to be achieved. For more information, see: Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről,l
[23] Information infrastructures "*include such fixed or mobile facilities, devices, systems, networks and the services they provide, which enable the acquisition, production, storage, transportation and use of information necessary for the operation of the information society. Information infrastructure consists of physical structures, equipment and the staff capable of professionally operating them, which is a consciously designed, organized and constructed artificial environment for the processing, transmission or use of information."* For more information, see: *HAIG Zsolt: Az információs hadviselés kialakulása, katonai értelmezése, Hadtudomány, 21.évf. 1-2. sz. 2011.* p. 73.

and developing the whole system.[24] The sum of these constitutes the information infrastructure, the state and development of which fundamentally determines the efficiency and future prospects of our modern information societies.

This complex and robust system requires that information infrastructures be further classified according to purpose and application:

- According to their purpose, we can distinguish between *functional* and *supporting* information infrastructures,[25]
- And according to their application, we can distinguish between information infrastructures operating on *global* and *national* levels, and within the latter, there are special purpose closed networks such as *defense information infrastructures*.[26]

From this we can conclude that national information infrastructures operate as an interconnected system of several elements, which are linked to the global information environment,[27] thus, as part of it, contribute to the global information exchange. In addition

[24]HAIG Zsolt. et al.: Kritikus infrastruktúrák és kritikus információs infrastruktúrák, Budapest, Nemzeti Közszolgálati Egyetem, 2012. p. 38

[25] The function of functional information infrastructures is to ensure the proper operation of the information services and functions necessary for society. Functional information infrastructures carry out the acquisition, production, organization, processing, transmission and use of information. The elements of this system include:

- the *open* – subscriber – and *closed* system – public service, public utilities and public supply – telecommunication networks,
- the broadcasting and information networks,
- the air traffic, flight control and navigation systems,
- the networks that are part of the operational management systems of state-level governmental, administrative, police, military and disaster management bodies.
- the reconnaissance, surveillance and anti-jamming systems of remote sensing, remote monitoring and control systems,
- the information technology tools and nodes of the network connected and communicating information technology system.

The supporting information infrastructure contains the research, development and supply information infrastructures, the task of which is to create and provide the supportive background for functional information infrastructure, and the intellectual and material bases. Supporting information infrastructure includes:

- the elements of electricity and other energy supply systems, including power plants, transmission networks, transformer stations and load distributors,
- the electronic and information technology research and development institutions, including universities, colleges and other institutions,
- the electronics and information technology companies,
- the warehouses and wholesale companies that store and sell electronic and information technology tools.

For more information, see: HAIG Zsolt, VÁRHEGYI István: Hadviselés az információs hadszíntéren, Budapest, Zrínyi Kiadó, 2005. p. 74-76.

[26] Ibid., p. 77.

[27] The global information infrastructure is the sum of wire and wireless telecommunication systems, computer and infocommunication networks, as well as remote sensing, remote control and navigation systems that ensures global information exchange. The most important parts of this network are ground-level, underground and underwater optical fiber cables operating as transmitting tools for digital

to systems used by civilians, there are national information infrastructures aimed at security, which are connected to the allied information network in a broader sense.

Finally, in terms of national security – similarly to the classification of general purpose infrastructures – information infrastructures can be divided into additional categories, thus it is necessary to briefly mention the concept of the so-called critical information infrastructures (hereinafter referred to as: CII).[28] The delimitation of CI and CII is hampered by the fact that with the emergence of information societies, infocommunication technologies also play an important role in the operation of general purpose infrastructures, which are involved in the controlling and governing[29] of various system elements, in the exchange of information between them, creating cooperation between infrastructures. With the loss of these critical information systems, such disturbances would be created in the operation of general purpose infrastructures, which would cause the services provided by them to crash and become unavailable – resulting in substantial material and social damages. Accordingly, we can distinguish between national critical information infrastructures that are indispensable for the functioning of society – including the computer network controlling the country's energy supply system, infocommunication systems for health care, transport and food supply systems, or the mobile telecommunication network, etc.[30] –, and key information infrastructures for economic operators.

The dynamic development of ICT has made continuously increasing computing performance possible, and due to the network connection of the various tools, the efficiency of the production, processing, storage and transmission of necessary information has increased considerably. As a result, vital – previously independently operating – infrastructures for the state have been highly integrated and automated, which has enabled production processes to be optimized and personalized services can be provided to citizens.

Infrastructures using infocommunication technologies have now become the central nervous systems of 21st century information societies, allowing a continuous and undis-

signals, as well as mobile telecommunications and satellite wireless signaling systems. For more information, see: Ibid., p. 78.

[28] Critical information infrastructures *are network-like, physical or virtual systems, tools, and methodologies of society, which are essential for the operation of individually vital system elements or other identified vital system elements that are a result of the continuous provision of information and the necessity for operational continuity of information technology conditions*. Source: 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról,

[29] Industrial Controll Systems (ICS) are unavoidable for the operation of various infrastructures and industrial facilities, which are increasingly network connected, enabling the automation and efficient operation of different processes. One of the most important groups of ICS systems are the Supervisory Control and Data Acquisition (SCADA) systems, which are special computer-based systems that perform the system management and supervision of equipment of various infrastructures and industrial facilities. For more information, see:
GYURÁK Gábor: Kritikus infrastruktúrák védelme hálózati behatolás jelző rendszerekkel,Hadmérnök, X. Évfolyam 2. szám,, Hadmérnök, X.évf. 2. sz.

[30] For more information, see: HAIG Zsolt. et al.: Kritikus infrastruktúrák és kritikus információs infrastruktúrák, Budapest, Nemzeti Közszolgálati Egyetem, 2012. p. 48-49.

rupted flow of information, operating basic state functions, and ensuring access to vital services. As a result, information flow accelerated dramatically in information societies, contributing to economic development and allowing faster, more efficient operation of state, military, technological and social sectors. But despite of its many benefits[31], this process also resulted in a high degree of dependence on information technologies and digitalisation, which has exposed human beings of the 21st century to a never before seen degree – and in the meantime, posed a new and deadly vulnerability and threat to modern states.

It is imperative for the vital systems and facilities[32] – power supply, telecommunications, health care, legal system, banking system, public security, defense, etc. – of the countries to ensure the undisrupted and continuous operation of information systems and infrastructures, in the event of a failure, loss or permanent shutdown of which, the whole state may even collapse.[33]

This means that a coordinated series of attacks launched with information tools can temporarily paralyze or permanently shutdown critical infrastructures of a given country, which can render basic state, economic, social functions and services inoperable. Attacks may occur in all – physical, cyber, electromagnetic and cognitive – domains[34] of the information environment, therefore, defense must include the physical, logical[35] and administrative protection of infrastructures and information systems. In addition, it is necessary to ensure control over the information processes in the cognitive dimension, in order to neutralize attempts by the attacker to manipulation and influence.[36] Taking this into account, the protection of the CI and the CII must be closely coordinated, cooperation between the various sectors must be established, thus ensuring the conditions of proper and undisrupted operation necessary for the internal and external security of the state, the economy and society.

[31] Just think of the convenience provided by a wide range of web services – online administrative services, banking, shopping, contact and communication, information gathering, distance learning and telework, etc.

[32] The list is detailed in Act CLXVI of 2012 on the identification, designation and protection of vital systems and facilities in Hungary. For more information, see: 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről,

[33] In their paper titled *Digitális Mohács*, Csaba Krasznay and László Kovács have outlined a similar scenario in which they presented the possible consequences of a comprehensive cyberattack against Hungary. For more information, see: KOVÁCS László, KRASZNAY Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint, Nemzet és Biztonság1. sz. 2017.

[34] For relationships between the various domains of information environment, see: Figure 1

[35] Protection created by information technology tools and procedures (programs, protocols) in the electronic information system, the major components of which are identification and authentication, access control system and system of accountability. Source: MUHA Lajos (szerk.): Az informatikai biztonság kézikönyve - Informatikai biztonsági tanácsadó A-tól Z-ig, Verlag Dashöfer Szakkiadó, 2000-2005.

[36]FEKETE Csanád: Információ és hadviselésháború a kognitív hadszíntéren II., Szakmai Szemle4. sz. 2016. p. 48-52.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 4. szám

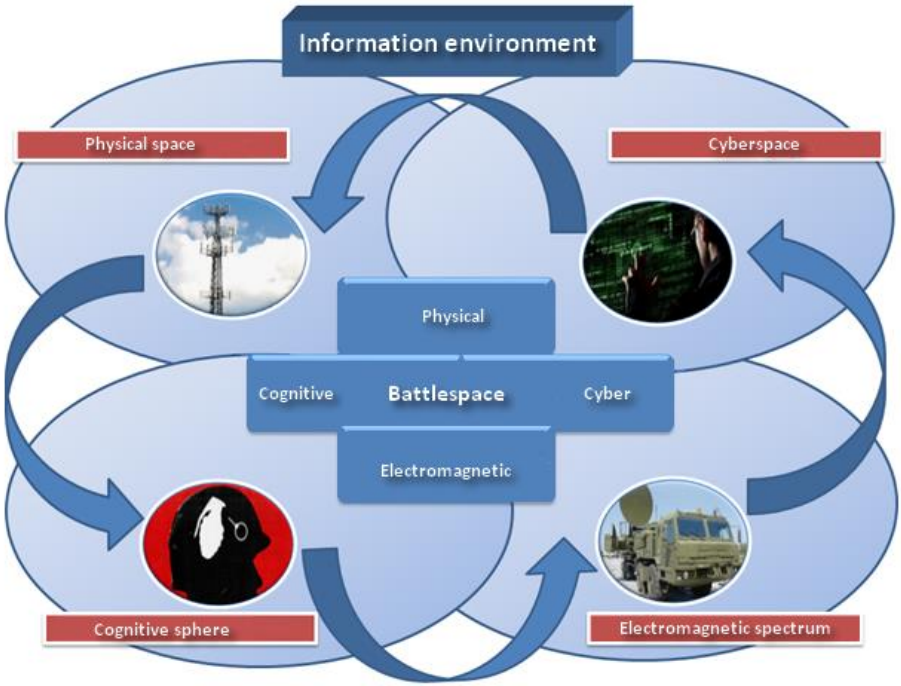

Figure 1: Relationships between the various domains of information environment (created by the author)

3. THE EMERGENCE OF STRATEGIC INFORMATION WARFARE

Infrastructures have always played a prominent role in conflicts, however, in the previous centuries they were considered geographically well-defendable, not easily accessible targets for the enemy, as they could only be attacked physically by kinetic means. Today, with the advancement of technology, and the wide spread and network connection of ICT devices, the door has been opened to attack various infrastructures with information tools, which has had a significant impact on the nature of conflicts and created the concept of information warfare.

The first definition of information warfare was created in 1976 by Thomas P. Rona, a Hungarian-born science advisor to the United States Department of Defense. In Rona's definition, he describes the coordinated usage of information tools and methods in periods of peace and war, which can proceed on strategic, operational and tactical levels as well,

helping to achieve the set objectives.[37]In the post-Cold War years, the major researchers investigating the subject have come to the conclusion from the rapid development of information technologies and the resulting political, social, economic and scientific trends that they will bring about revolutionary changes in warfare, as demonstrated by the example of the Gulf War.[38]

According to some authors, the struggle in the information space will increasingly play a strategic role in the future, thus the side that is able to acquire and maintain information superiority in a given conflict will gain an unbeatable advantage and can easily force its will upon the opposing side. Some experts[39] have gone even further and emphasized the strategic importance of the information space, as a result of which members of the RAND research institute created the concept of strategic information warfare.

During RAND Corporation's exercise in 1995 involving national security and civilian experts, they have examined several possible scenarios, in which they have executed a coordinated information attack against the United States and its allies. Based on the experiences of the exercise, they have published a paper[40] titled *"Strategic Information Warfare: A New Face of War"*, in which they have drawn attention to the threats posed by information warfare. In the paper, 7 important factors and problems were identified, which in their view characterize strategic information warfare:

1. low costs;
2. blurred borderlines – external and internal perpetrators, state actors;
3. increasing role of perception management;
4. new challenges of strategic intelligence;
5. problems of predicting and assessing attacks;
6. difficulties of creating and maintaining coalitions;
7. vulnerability of the United States homeland.[41]

Strategic information warfare, according to the authors, will become an important tool for states and non-state actors in the future, complementing advanced conventional forces possessing information tools, as well as – nuclear, biological and chemical – weapons of mass destruction.[42]

---

[37] For more information, see: HAIG Zsolt: Az információs hadviselés kialakulása, katonai értelmezése, Hadtudomány, 21.évf. 1-2. sz. 2011. p. 12

[38] The Gulf War, according to many, was a transition between traditional attrition-style industrial warfare and warfare of the information era. ARQUILLA John: The Advent of Netwar, Rand Corporation, 1996. p. 104.

[39] Among other Western authors, John Arquilla and David F. Ronfeldt dealt a lot with the topic, publishing such influential books as "*The Advanet of Netwar"* in 1996, or the "*Swarming and the Future of Conflits"* in 2000. For more information, see: ARQUILLA John, RONFELDT David F.: Swarming and the Future of Conflits., Rand Corporation, 2000; ARQUILLA John: The Advent of Netwar, Rand Corporation, 1996

[40]MOLANDER Roger C., RIDDILE Andrew, WILSON Peter A.: Strategic Information Warfare - A New Face of War, Rand Corporation, 1996.

[41] Ibid, p. 15.

[42] Ibid, p. 1-3.

Upon its publication, the concept raised rather new and groundbreaking ideas, however, the events of recent years, in my opinion, confirmed the validity of the assertions of the research. In fact, the study predicted the reality of today ahead of its time, in which various state and non-state actors, from little resources, can effectively attack information systems that permeate all aspects of life. On account of this, they can even paralyze critical infrastructures of developed countries, which is a completely new and deadly threat to the security of modern states. All this blurs the line between the state of peace and war and is a permanent threat to information societies.

Strategic information warfare	
Objectives	Weakening the strategic position of the other side, overthrowing the political system, creating a social and political crisis, paralyzing the decision-making system, triggering strategic paralysis
Targets	Decision-makers, population, information systems and critical infrastructures
Tools	Information weapons,[43] automated software applications,[44] classic tools of intelligence
Participants	Non-state actors, state-sponsored hacker groups, dedicated cyber task forces of armed forces, secret services, other state and non-state organizations, etc.
Methods	Influence operations, cyberspace operations
Operating environment	Different dimensions of the information environment: cyberspace, electromagnetic spectrum, physical medium, cognitive medium

[43] Including cyberweapons and other technical solutions such as distributed denial-of-service attacks (DDoS), or sophisticated malwares, or troll armies.
[44] In the future, the use of machine learning-based solutions will be of utmost importance. For these possibilities, see: ANDERSON Berit, HORVATH Brett: The Rise of the Weaponized AI Propaganda Machine There's a new automated propaganda machine driving global politics. How it works and what it will mean for the future of democracy., Scout, 2017.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 4. szám

4. THE APPEARANCE OF STATES IN THE ARENA OF CYBERSPACE

In the previous chapter, I tried to briefly review the major vulnerabilities of information societies and the development of the concept of information warfare. The events of recent years have also shown that the emergence of information space has fundamentally transformed the nature of power struggles between states – and non-state actors –, creating a new and effective toolset that allows the achievement of political objectives and victory without kinetic means and the eruption of war. In my opinion, the information domain has gained strategic importance by today, which is no longer only used to support military operations in conflicts, but also greatly influences power relations between states. Many authors believe that in the information age, the classic perception of wars and the usage of violence should be revised, since today, we can *"compel our opponent to fulfill our will"*, even without the deployment of kinetic attacks, thus fulfilling the perpetual clausewitzian definition of the purpose of war.[45]So compared to the age of the Prussian military officer, in the era of information societies, the toolset for achieving political objectives changed – expanded – dramatically, thus today, we are witnessing a gradual transformation of the strategies – which were predicated on the use of physical violence – prevalent in the XIX. and XX. century. Previously, in pursuit of political objectives, war was used as a tool to break the will of the enemy, the achievement of which made it possible to occupy or gain possession of the territory of another state.

War was the ultimate test of will, the result of which influenced the outcome of controversial issues that were the casus belli, the enforcement of power interests, and ultimately the change in power relations between international actors. As we saw in the previous chapter, the information battlespace was initially established as a new domain of military operations, and information warfare was limited to times of war.

However, as early as the 90s, individuals and various hacker groups have appeared in the information space, who, typically for financial gain and fame, broke into computer network systems, stole information from companies and organizations, and spread malicious softwares. However, in the early 2000s, states increasingly recognized the potential – and vulnerabilities – of interconnected networks, thus increasingly organized, state-funded groups have emerged, who, for political reasons – and state interest –, have launched more and more coordinated attacks against the infrastructures of other states. In addition, state sponsored cyberspace espionage became considerable, as a result of which, a continuous struggle began in order to hack information systems and to extract the information stored therein.[46] The information confrontation taking place in cyberspace is therefore a

[45]CLAUSEWITZ Carl Von: A háborúról, Budapest, Zrínyi Kiadó, 2013. p. 39.

[46] The intensity of this is well illustrated by a 2008 report made for the United States Congress, according to which, since 2002, US authorities involved in cyber security have detected a number of Chinese origin break-ins into the computer systems of institutions and large corporations contracted by the United States military and government. These series of attacks later became known as Titan Rain, during which 10-20 terabytes of data were downloaded by Chinese hackers. According to some sour-

result of a gradual evolution, which became interconnected with the emergence and development of information societies.

As a result, the information space has become an enormous virtual arena that goes beyond geographic borders, where states and non-state actors engage in a continuous struggle, the objective of which is to enforce economic and political interests, gain strategic advantages, improve power positions and weaken rivals. For the emergence of this battlespace, the activation of state actors was absolutely necessary, whose resources have enabled the development of such cyberwarfare capabilities that can paralyze even an entire state. To illustrate this, I have created a potential scenario in which I present the possible phases of an attack carried out by information tools on an arbitrary state.

5. A POTENTIAL SCENARIO FOR A CYBERWAR

The scenario outlined here is a summary of the experiences of the literature[47] I have examined and the case examples described above. In my scenario, there is a developing conflict of interest between two neighboring countries, which gradually escalates into an actual armed conflict. In connection to this, it is important to note that geographic distances no longer constitute an obstacle in the information age, as a coordinated attack can be launched via information tools against vital systems of a state anywhere in the world, as a result of which, the given society can be destabilized and the desired political objectives can be obtained without the use of kinetic means. Of course, even information tools have their own limitations, but all in all, it can be stated that with their usage, the resistance of the opposing side can be significantly weakened, thus kinetic operations can be minimized. Considering these, a possible conflict may develop as follows:

First step – information confrontation in peacetime (reconnaissance and demoralization)

Main objective: During an information confrontation in peacetime, the consolidation of strategic positions and continuous preparations for conflicts are taking place.

---

ces, intensive intelligence activities in cyberspace are conducted by unit 61398 of the Chinese People's Liberation Army. All this shows that states like China have recently set up special purpose units to penetrate the information systems of foreign states and economic operators, in order to gain political and economic advantages by obtaining information stored therein. For more information, see:
KOVÁCS László: Információs hadviselés kínai módra, Budapest, Nemzet és Biztonság, II.évf. 2. sz. 2009. p. 36.;
GOLD Daniel: Unit 61398: Chinese Cyber-Espionage and the Advanced Persistent Threat, Infosec Institute, 2013.

[47] During the writing of this chapter, I have strongly built on the study published by László Kovács and Csaba Krasznay, Digital Mohács. For more information, see: KOVÁCS László, KRASZNAY Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint, Nemzet és Biztonság1. sz. 2017.

Cyberspace

- Targeted Phising attacks[48] launches against major corporations, public sector employees and critical infrastructure management employees, which are usually combined with social engineering techniques[49];
- With specialized software, they detect the vulnerabilities of computer systems operating critical information infrastructures and map out weaknesses;
- The placement of various malwares begins, which embed in hidden mode on the computer networks (APT attacks[50]) and leak information to the C&C servers of the attackers. During the reconnaissance, information is gathered on the operational plans of the opposing side, on the resources at its disposal, on the level of preparedness, military equipment and dislocation of its defence and law enforcement agencies.

Cognitive space

- The gaining of media positions begins, changing the perceptions of the population, undermining the credibility of the government, and spreading alternative narratives on events;
- State-sponsored trolls begin their centrally controlled manipulation and unsettling of conversations on online forums and articles comment feeds. They create profiles on various social media sites, which are used during influence operations. During the influence operations, they can use such automated software – online persona management services –, which allows one operator to manage multiple user accounts simultaneously, ensuring the quick and effective influencing of opinions;[51]
- The manipulation of various social groups begins,[52] that intensify the social tensions. In an effort to increase social tension, they send different messages to va-

[48] Phising is a method to gather information from the victim via use of deceptive and infected e-mails, websites and links.
[49] Social engeneering attacks typically combine methods and techniques that take advantage of human gullibility and other weaknesses, in order to get information, spread different malware, and gain access to information technology systems by influencing and manipulating the victim. For more information, see: DEÁK Veronika: A social engineering humán alapú támadási, Biztonságpolitika.hu, 2017.
[50] Advanced persistent threat: the term was first coined by US Air Force Colonel Greg Rattray in 2006, which later became a well-established technical term for defining a set of high expertise requiring, stealthy and continuous attacks aimed to gather intelligence. For more information on APT attacks, see: ARSENE Liviu: The Anatomy of an advancedpersistent threat, DarkReading, 2015.
[51] For more details on this topic, see: BENEDICTUS Leo: Invasion of the troll armies: from Russian Trump supporters to Turkish state stooges, The Guardian, 2016;PAGANINI Pierluigi: PsyOps and Socialbots, Infosec Institute, 2013
[52] For this, the attacker makes detailed analysis and evaluation on the historical, cultural, political, economic and social background of the target country, as well as on the demographic, ethnic and religious composition of the population. Afterwards, they select the target groups to be influenced.

rious groups.[53]With the leaking of sensitive information begins the demolition of the credibility of the government.[54]

SECOND STEP – COORDINATED CYBER-OPERATIONS (DESTABILIZATION)

Main objective: The main objective of the second step operations is the paralyzation of critical infrastructures and services, the disruption of the decision-making system, the creation of social insecurity and ultimately the causing of social collapse. All this significantly reduces the defense capabilities of the targeted country.

Cyberspace

- By exploiting the vulnerabilities identified in the first step, the preinstalled malicious software placed in the network are activated;
- Massive DDoS attacks[55] launches by using a variety of tools (*botnets[56] networks based on IoT tools*) cause malfunctions in the proper operation of information technology systems and services;
- Deface-type attacks[57] may launches against major news agencies and government websites, fake news spread rapidly, which further increase panic;
- Critical infrastructures and information technology systems can become completely paralyzed (paying special attention to energy services, telecommunications, banking and financial sectors).

Cognitive space

- Based on the alternative media network built in the first step, a comprehensive propaganda and disinformation campaign is launched, the objective of which is to support the alternative reality planted during the first step, to manipulate the per-

[53] An example of this, we can cite the increase in Russian activity during the United States' social tensions in 2016 and 2017. According to some sources, at the beginning of 2017, the Russian state-connected Internet Research Agency created a group called the Black Fist, which in one of their operations, sought out a well-known Afro-American MMA fighter in order for him to launch a self-defense course for young black people. To this end, they financially supported the launch of self-defense groups, and posted advertisements to increase the number of members. In exchange for the support, they requested video material from the course and information regarding the participants, which could be used to enhance social tension. For more information on similar operations, see: HANULA Zsolt: Putyin trollhadserege: ezer ember, havi egymillió dollárért, Index.hu, 2017

[54] According to some opinions, the US presidential election campaign has become one of the main fields of struggle between Russia and the United States, after Wikileaks and the Anonymous hacker group – according to some sources, with the help of the Russian secret service – leaked tens of thousands of e-mails. For more information, see:GREENBERG Andy: Trump's Win Signals Open Season for Russia's Political Hackers, Wired, 2016

[55] The term used for networks consisting of infected computers – bots – connected to the Internet.

[56] Distributed Denial of Service (DDoS) attacks aim to overload various servers.

[57] Deface attacks allow an attacker to replace the site's homepage and display their own message.

ception of the population in the desired direction, to expiry the government, to increase uncertainty, to intensify differences and to destabilize the society;

- The activity of state-sponsored trolls increase on various social media sites, they attack the official narrative of events with false and misleading information and attempt to undermine the credibility of the government;
- Through the intensification of influence operations, the primary objective is to increase social tension and to lead the potentially erupting unrests, or mass riots into a violent direction. By raising internal tension and provoking violent acts, they undermine the stability of the hinterland, greatly reducing defense capabilities.

THIRD STEP – INFORMATION OPERATIONS AFTER THE OUTBREAK OF AN ARMED CONFLICT

Main objective: After the first two phases, the crisis can escalate into a direct armed conflict, during which coordinated information attacks are launched to support military operations in all domains.

Cyberspace

- The main efforts are aimed at paralyzing the enemy's command and control system, as well as gaining information superiority and dominance.

Cognitive space

- The primary objective is to deceive enemy forces, influence public opinion, and paralyze political decision-making.

Physical space

- The destruction of designated military and civilian information infrastructures with kinetic strikes.

Electromagnetic space

- Blocking the enemy's communication with the electronic jamming devices of the troops, blocking the various elements of the command and control system.

Overall, it can be said that the intensity of the activities carried out in the pre-war periods is steadily increased, after the preparations, the efforts are aimed at weakening the target and thus creating ideal conditions for gaining superiority and achieve victory fast in a case of an armed conflict.[58]During the information attacks, all those information infra-

[58]GILES Keir: Handbook of Russian Information Warfare, Research Division NATO Defense College, 2016.

structures may become targets that are connected to the global, national or defense information infrastructure and possesses ICT systems and networks. After the outbreak of the actual conflict, information operations are launched in all domains of the information environment with the following objectives:

- **Information attacks carried out in cyberspace** aim to map out the vulnerabilities of information systems and networks, to interfere with and influence the proper operation of these systems, to paralyze various services and control processes, and, if all else fail, to cause physical damage.
- **Main targets**: All elements of critical infrastructures that possesses computer systems and networks.
- **Cognitive attacks carried out in the cognitive dimension** aim to influence the population of the opposing side, to deceive its political and military leadership, to paralyze its decision-making systems and to reduce its ability to react quickly .
- **Main targets**: decision-makers, experts, population.
- **Kinetic attacks carried out in the physical dimension** aim to destroy the information systems of the opposing side and to paralyze their operation.
- **Main targets**: physical elements of the critical information infrastructure (power stations, power grids, load distributors, telecommunication nodes, server rooms) – it is important to note that the majority of these can be attacked with information tools (cyberweapons).
- **Attacks carried out in the electromagnetic spectrum** aim to reduce the communication capabilities of the opposing side, and to interfere with and block its command and control system (C2C).
- **Main targets:** Electronic equipments of the command and control system, wireless communication systems.

Depending on the political objectives, the focus of which infrastructure is the most important to attack can change. The greater the desired effect, the more preparation is required and the more domains of the information battlespace will be affected by the attacks.

CONCLUSIONS

According to many authors, the information era has brought significant changes to the field of warfare, all new theories – hybrid warfare, fourth-generation warfare, unrestricted warfare, etc. – dealing with this topic highlight the increasing role of indirect strategies and non-military means in conflicts.[59]

Based on the events of recent years, we can state that we are living in a transitional era, where operations carried out in the information space are increasingly determining the

[59] In his infamous article published in 2013, General Valery Gerasimov states that in the new types of conflicts, non-military means outweigh military force 4:1. For more information, see: GERASZIMOV Valerij: Cennoszty nauki v predvigyenyii., Vojenno-promislennij kurjer, 8.évf. 476. sz. 2013.

outcome of conflicts, but military tools and traditional kinetic operations still have a significant role to play. Today, conventional military force is no longer the primary element of the strategic toolset – however, its role will remain decisive as the "ultima ratio" tool for resolving international crisis and conflicts between states.

Due to the constantly evolving technology, coordinated information attacks have now become a violent tool for state and non-state actors, through the usage – coordinated information attacks against the strategic center of gravity of the enemy's critical infrastructure – of which, the set strategic objectives can be realized.

Strategic information warfare examined in this paper offers a much wider understanding of the phenomenon than the traditional approach to information operations, which greatly aids a more accurate understanding and processing of the experiences of the events – including the US presidential campaign and Russian disinformation operations – of recent years. As the concept of information operations only covers periods of war, however, past years have proven that information warfare between the great powers continues during both periods of peace and war, and is capable of causing impacts of strategic importance.

Within the framework of strategic information warfare during peacetime, the main objectives include: gaining control over information processes, detecting vulnerabilities inherent to the information systems of the other side, undermining the social order of the enemy, confusing its decision-making system, and following the outbreak of the conflict, achieving strategic paralysis. The growing dependence on information systems means that the side capable of destroying or paralyzing the information infrastructure of the other side, while defending its own, will be able to gain decisive strategic superiority in an armed conflict. Those who do not adapt to the changed circumstances of the information age and the challenges of information warfare will come out on the bottom in the future;

Based on the experiences of recent years, we can conclude that the wars of the information age will increasingly take place in the cyber and cognitive domains in order to influence the population and decision-makers and to control information processes. All this leads to the fact that the existence of a conventional superiority alone will not be enough to achieve strategic objectives, because the side who wins the struggle in the information space can reduce the social support of the other side, can interfere with decision-making processes, thus denying the opposing side the information resources needed to continue the war.

It is crucial that events in the information space are kept under constant surveillance, as a coordinated attack originating from cyberspace can shut down the vital systems of a country, the decision-making system may become paralyzed, causing a major social and political crisis. Influence operations, which play a central role in strategic information warfare, go beyond the borders of cyberspace, thus it is imperative to apply a system-wide approach to all domains of the information space. Furthermore, the early detection of attacks, the identification of the intent and strategy of the attacker, as well as the develop-

ment of a coherent communication strategy are indispensable for counteracting influence and cyberspace operations.

Strategic information warfare is a cost-efficient and effective tool in the toolset of states – and non-state actors –, that is why in the future it is expected that conflicts will increasingly intensify in the information space, which can even spread to the physical domain.[60] As a result of the intensification of information warfare, it is in the states' fundamental national security interest to pay particular attention to the protection of information systems, within the framework of which, it is essential to develop a comprehensive cybersecurity strategy reflecting on potential risks and threats, to create the legal and organizational background of information security, and to secure resources to implement them. The expansion of the circle of threats also means that a complex approach to the information space is needed, taking into account the most vulnerable and most attackable system elements, which, in most cases, are the users and the people – the cognitive sphere. This is why, on one hand, it is necessary to raise information security awareness – which should be included in education, even at high school level – and, on the other hand, to find the appropriate measures to neutralize the propaganda and disinformation attempts spread within the framework of influence operations. All this requires a complex and comprehensive approach where active cooperation and exchange of information is needed between government agencies and market participants in which the involvement of internet services (such as Facebook, Google) and the media is essential.

BIBLIOGRAPHY

1. 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200166.tv (Letöltés ideje: 2018. 08. 25.)
2. 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról. https://net.jogtar.hu/jogszabaly?docid=a1300065.kor (Letöltés ideje: 2018, 04. 20.)
3. ANDERSON, Berit, HORVATH, Brett: The Rise of the Weaponized AI Propaganda Machine There's a new automated propaganda machine driving global politics. How it works and what it will mean for the future of democracy., 2017, Scout. https://scout.ai/story/the-rise-of-the-weaponized-ai-propaganda-machine (Letöltés ideje: 2018.08. 30.)
4. ARQUILLA, John: The Advent of Netwar, Rand Corporation, 1996.

[60] The decisions made at the 2016 Warsaw Summit of the NATO have increased this possibility considerably. For more information, see: SZENES Zoltán: MEGLEPETÉSEK NÉLKÜL: A varsói NATO csúcs értékelése, Biztonsagpolitika.hu, 2016

5. ARQUILLA, John, RONFELDT, David F.: Swarming and the Future of Conflits, Rand Corporation, 2000.
6. ARSENE, Liviu: The Anatomy of an advanced persistent threat, Dark Reading, 2015. https://www.darkreading.com/partner-perspectives/bitdefender/the-anatomy-of-advanced-persistent-threats/a/d-id/1319525 (Letöltés ideje: 2018. 08. 10.)
7. Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=EN (Letöltés ideje: 2018. 04. 10.)
8. BENEDICTUS, Leo: Invasion of the troll armies: from Russian Trump supporters to Turkish state stooges, in: The Guardian, 2016. https://www.theguardian.com/media/2016/nov/06/troll-armies-social-media-trump-russian (Letöltés ideje: 2018. 08. 10.)
9. CLAUSEWITZ, Carl V.: A háborúról, Zrínyi Kiadó, Budapest ,2013.
10. DEÁK Veronika: A social engineering humán alapú támadási, 2017, Biztonságpolitika.hu. http://biztonsagpolitika.hu/wp-content/uploads/2017/04/Deak_Veronika_a-social-engineering-humán-alapú-támadási-technikái.pdf (Letöltés ideje: 2018. 08. 15.)
11. FEKETE Csanád: Információ és hadviselésháború a kognitív hadszíntéren II., in: Szakmai Szemle, 2016. 4. sz.
12. GERASZIMOV, Valerij: Cennoszty nauki v predvigyenyii., 2013, Vojenno-promislennij kurjer No. 476. http://www.vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf (Letöltés ideje: 2018. 08. 20.)
13. GILES, Keir: Handbook of Russian Information Warfare, 2016, Research Division NATO Defense College. https://krypt3ia.files.wordpress.com/2016/12/fm_9.pdf (Letöltés ideje: 2018. 08. 12.)
14. GOLD, Daniel: Unit 61398: Chinese Cyber-Espionage and the Advanced Persistent Threat, in: Infosec Institute, 2013. http://resources.infosecinstitute.com/unit-61398-chinese-cyber-espionage-and-the-advanced-persistent-threat/ (Letöltés ideje: 2018. 08. 20.)
15. GREENBERG, Andy: Trump's Win Signals Open Season for Russia's Political Hackers, 2016, Wired. https://www.wired.com/2016/11/trumps-win-signals-open-season-russias-political-hackers/ (Letöltés ideje: 2018. 08. 20.)
16. GYURÁK Gábor: Kritikus infrastruktúrák védelme hálózati behatolás jelző rendszerekkel,Hadmérnök, X. Évfolyam 2. szám,, in: Hadmérnök, X.évf. 2. sz. http://hadmernok.hu/152_20_gyurakg.pdf (Letöltés ideje: 2018. 06. 05.)
17. HAIG Zsolt. et al.: A kritikus információs infrastruktúrák meghatározásának módszertana, Budapest, 2009., ENO Avisory Kft. http://www.cert-hunga-

ry.hu/sites/default/files/news/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf (Letöltés ideje: 2018. 08. 22.)

18. HAIG Zsolt: Az információs hadviselés kialakulása, katonai értelmezése, in: Hadtudomány, 2011, 21. évf. 1-2. sz.
19. HAIG Zsolt. et al.: Kritikus infrastruktúrák és kritikus információs infrastruktúrák, Budapest, 2012, Nemzeti Közszolgálati Egyetem. https://www.uni-nke.hu/document/uni-nke-hu/kritikus_infrastrukturak.pdf (Letöltés ideje: 2018. 08 24.)
20. HAIG Zsolt, VÁRHEGYI István: Hadviselés az információs hadszíntéren, Zrínyi Kiadó, Budapest, 2005.
21. HAMMES, Thomas X.: War evolves into the fourth generation, 2005, Contemporary Security Policy No. 2.
22. HANULA Zsolt: Putyin trollhadserege: ezer ember, havi egymillió dollárért, 2017, Index.hu. https://index.hu/tech/2017/11/06/putyin_trollhadserege/ (Letöltés ideje: 2018. 08 24.)
23. HOFFMAN, Frank G.: Conflict in the 21st century - The rise of hybrid wars, Potomac Institute for Policy Studies, Arlington, VA, 2007.
24. KOVÁCS László: Információs hadviselés kínai módra, in: Nemzet és Biztonság, 2009, II.évf. 2. sz. Budapest. http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/1012/kovacs_laszlo-informacios_hadviseles_kinai_modra.pdf?sequence=1&isAllowed=y (Letöltés ideje: 2018. 08. 25.)
25. KOVÁCS László, KRASZNAY Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint, in: Nemzet és Biztonság, 2017. 1. sz.
26. KRAJNC Zoltán, GÖNCZI Gabriella: A légi hadjáratok (műveletek) stratégiai szintű tervezésének és az üzleti (vállalati) stratégiaalkotásnak a konvergenciája (egy. PhD-témaválasztás indoklása)., in: Repüléstudományi Konferencia, 2009, Szolnok. http://epa.oszk.hu/02600/02694/00048/pdf/EPA02694_rtk_2009_2_Krajnc_Zoltan-Gonczi_Gabriella_1.pdf (Letöltés ideje: 2018. 08. 30.)
27. KRAJNC Zoltán, GÖNCZI Gabriella: Korunk meghatározó légierő teoretikusa: John A. III. Warden, in: Hadmérnök, 2010, V.évf. 1. sz. http://hadmernok.hu/2010_1_gonczi_krajnc.pdf (Letöltés ideje: 2018. 08. 30.)
28. MOLANDER, Roger C.RIDDILE, Andrew, WILSON, Peter A.: Strategic Information Warfare - A New Face of War, Rand Corporation, 1996.
29. MUHA Lajos (szerk.): Az informatikai biztonság kézikönyve - Informatikai biztonsági tanácsadó A-tól Z-ig, Verlag Dashöfer Szakkiadó, 2000-2005.
30. PAGANINI, Pierluigi: PsyOps and Socialbots, 2013, Infosec Institute. resources.infosecinstitute.com/psyops-and-socialbots/ (Letöltés ideje: 2018. 08. 10.)
31. PENSITON, Bradley: Army Warns that Future War with Russia or China Would Be 'Extremely Lethal and Fast', 2016, Defense One.

http://www.defenseone.com/threats/2016/10/future-army/132105/ (Letöltés ideje: 2018. 08. 30.)
32. SZABÓ József: Kis magyar hadelmélet illetve mire készítsük fel a honvédtiszteket a XXI. században, 2012, Hadtudományi Szemle pp. 378–384. http://epa.oszk.hu/02400/02463/00013/pdf/EPA02463_hadtudomanyi_szemle_2012_3-4_378-384.pdf (Letöltés ideje: 2018. 08. 24.)
33. SZENES, Zoltán: Katonai kihívások a 21. század elején, Budapest, 2005, Hadtudomány No. 4. http://www.zmne.hu/kulso/mhtt/hadtudomany/2005/4/2005_4_5.html (Letöltés ideje: 2018. 08. 20.)
34. SZENES Zoltán: MEGLEPETÉSEK NÉLKÜL: A varsói NATO csúcs értékelése, in: Biztonsagpolitika.hu, 2016.
35. WARDEN, John: Air Theory for the Twenty-First Century, in: Airpower Journal, 1995.