Krzysztof Liedel
Paulina Piasecka

Cyberspace – the 5th battlefield

Diagnosis and recommendations

BRONISŁAW KOMOROWSKI INSTITUTE

Konrad Adenauer Stiftung

BRONISŁAW
KOMOROWSKI
INSTITUTE

Krzysztof Liedel / Paulina Piasecka

CYBERSPACE – THE 5th BATTLEFIELD

Diagnosis and recommendations

The security of the state in the era of threats in cyberspace

The dynamics of changes in the security environment has noticeably grown over the recent years. Among the major reasons of this state of affairs is not only the exhaustive premium of security, stemming from the end of the Cold War 25 years ago, but also the emergence of new strategies as well as tactics used on the international stage by active state and non-state actors.

Another factor influencing the change in the perception of security and the need to create new mechanisms securing the state, its interests and citizens is the emergence of new features of security, which determines the change in its paradigm[1]. These features are: informativeness, networking, dissymmetry and inclusiveness, among others.

The informativeness of security, resulting from the information revolution, changes the paradigm of the security process, which is determined by the relations between two primary and the most fundamental factors of all human actions – energy and non-material – informational. Asymmetry of security is mainly caused by the political revolution, which includes the dissolution of the bipolar world and the increased importance of actions of non-state actors, mainly international terrorist networks. The networking of security stems mostly from the co-existence of two phenomena: information revolution and globalization. The last of the new features of security is its inclusiveness, which means combining military efforts (defensive) and non-military (preventive, supportive) within the framework of the security process.

The term inclusiveness is directly connected with the concept of cross-sectoral security, which first occurred in the National Security Strategic Review, issued by the National Security Bureau of Poland on the request of Bronisław Komorowski, President of the Republic of Poland. According to the definition formulated in the Review **the cross-sectoral (universal) areas of national security** (state security) are "parts of the integral national security incorporating at the same time issues related to different subjects, domains and sectors of this security (for example internal or external security,

[1] Koziej S. "Nowa jakość bezpieczeństwa na progu XXI wieku", source: https://www.bbn.gov.pl/pl/wydarzenia/2562,quotNowa-jakosc-bezpieczenstwa-na-progu-XXI-wiekuquot-wystapienie-Szefa-BBN-w-AO.html

or issues related to modern transnational processes and asymmetrical phenomena and security processes such as for example information security, **including cyber security**, counter-terrorism security, preventing proliferation of weapons of mass destruction, combatting organized crimes). They are often separated due to qualitatively new and urgent nature of practical needs in a certain period of time, which do not have a clear addressee in the existing executory structure of the subject)".

Having in mind the ongoing change of the security paradigm, ministers of defense of NATO member states made the decision at the Warsaw NATO Summit in 2016 to recognize cyberspace as the 5th battlefield (next to the land, air, sea and space). As stated in the "Warsaw Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016".

- cyber attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack;
- cyber defense is part of NATO's core task of collective defense;
- NATO has a defensive mandate, and recognize cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea.

This constatation influences the perception of threats in cyberspace and determines the need for a broader reflection on the borders of state security and necessary actions, which shall be taken to protect them.

Information security as the supreme category

The category of cyber security shall be considered with reference to the overall area of national security. The term information security is particularly important in the context of placing cyber security on the national security map.

Information security of the state, hence the security process carried out in and for the needs of information society, is a cross-sectoral sphere of security, which applies to the information society of the state (including cyberspace). The goal of this process is to guarantee on the one hand security in the functioning of the state within the information space through controlling its own, internal, domestic info-sphere and on the other hand to guarantee an effective protection of national interest within the external (foreign) info-sphere.

This can be achieved by the execution of tasks such as assuring an adequate protection of possessed information resources and protecting against hostile disinformation and propaganda actions (in defensive dimension). Simultaneously, the capacity to conduct offensive actions in this area towards enemies (states or other entities) shall be ensured.

An information society is a set of persons, organizations and systems, which collect, process, distribute and act on the basis of information (including cyberspace). This kind of community is composed of three correlated dimensions, which constantly interact with persons, organizations and systems: cognitive (human factor), informative (data and information) and physical ("real" world)[2]. The physical dimension consists of command and control systems, key decision-makers and underpinning infrastructure, which enable entities and organization to achieve their objectives. It also contains communication networks and physical platforms for data processing. This dimension encompasses i.a. people, communication and control tools, newspapers, books, computers, smartphones, tablets and any other components, which can be physically measured.

The informative dimension refers to where and how the information is collected, processed, distributed and protected. In this dimension the process of command and control takes place and the intentions of main decision-makers are conveyed. Actions taken in this dimension influence the content and the flow of information.

The cognitive dimension refers to people's minds, which convey, receive, react or operate on the basis of information. It relates to processing, perception, judgement and decision-making process of an individual or of a group. It is influenced by several different factors, such as cultural believes, norms, sensibility, motivations, emotions,

[2] *Information Operations*, Joint Publication 3-13, Incorporating Change 1, Joint Chiefs of Staff, 20 November 2014.

experience, morals, education, mental health, identity and ideology. Defining these factors in a given environment is crucial for understanding and knowing, what the most efficient way to influence the mind of the decision-maker is and how to achieve the expected results.

There are several information threats related to the functioning in cyberspace, for example: disinformation, trolling, hostile propaganda, disrupting the execution of crucial tasks of public administration and private sector; attacks resulting in the disruption in the functioning of information and communication technology networks in sectors and institutions with a higher level of vulnerability, including those creating the critical infrastructure; the existence of the technological loopholes, which give a way for an even non-visible incursion in the content of web portals as well as the ability to operate in cyberspace.

Key terms and operational areas: cyber security and security in cyberspace

The planning of actions aimed at ensuring cybersecurity of the state, its public and private sector as well as its citizens, requires specification of terms related to this field of security systems' functioning. Referring to "the cyber security doctrine of the Republic of Poland", it is possible to distinguish two distinct terms describing the security of a state in the context of its functioning in cyberspace.

The first one is **the notion of cybersecurity** – the security of the state in cyberspace. This term is defined as the process of securing the safe functioning of the state as a whole in cyberspace. The state is understood as its structures, natural and legal persons, including entrepreneurs and other entities without legal personality as well as information and communication technology networks and information resources in the global cyberspace, which the state has at its disposal.

Another term described in the Doctrine is the security in the cyberspace, hence a part of the cybersecurity of the state, which encompasses a set of actions: organisational and legal, technical, physical and educational, which need to be undertaken. They aim at ensuring the functioning of the national cyberspace without any disruption, providing the public and private critical information and communication technology networks as well as guaranteeing the security of the processed information resources.

Among the most important objectives of actions ensuring cyber security, it is possible to identify the following:

- the evaluation of cybersecurity conditions, including the recognition of threats, risk assessment and identification of changes,
- prevention (counteracting) of threats, reduction of risks and the use of opportunities,
- defense and protection of their own systems and gathered resources,
- combat with (de-organizing, disrupting and destroying) the sources of threats (active defense and offensive actions),
- after a potential attack – the reconstruction of the ability and functioning of the systems; creating cyberspace.

There are also several **practical undertakings**, which aim at ensuring the effectiveness of state's actions in cyberspace, such as:

- guaranteeing the state's capacity to defend itself and its own information and communication technology networks together with collected data as well as capability to actively defend and conduct offensive actions in cyberspace, integrated with other national military forces,
- creating and enhancing military structures designated for the execution of tasks in cyberspace, capable of identifying, preventing and combatting cyber threats,
- coordinating research and development initiatives for cyber security, also within the framework of civil-military cooperation,
- coordinating the cooperation of specialized (departmental) centers of cyber security in order to acquire complete information about the situation,
- monitoring and enhancing security of networks used to distribute and store information qualified as classified,

- developing counter-intelligence measures within cyberspace through the optimization of solutions on the level of software development together with physically securing the networks,
- implementing systems, which shall counter the plausible breaching of systems in real-time:
    - placing its own passive sensors computer systems in cyber environment in order to detect potentially malicious codes in the data package received from the internet;
    - reducing and consolidating external points of internet network access in order to minimalize risks for networks used for state's security systems,
- enhancing educational efforts in the field of cyber security with a with particular focus on training programs in the field of defensive and offensive capabilities in cyberspace,
- promoting long-term partnerships and cooperation between public and private sector, especially with regards towards private providers of key elements of information and communication infrastructure of the state.

It is important to underline that the protection of its own interest in cyberspace as well as the protection of information in the security environment is directly linked to the **development of cryptographic systems**. Big potential in the field of cybersecurity lies in fields of science such as informatics and mathematics. They both give the opportunity to develop national systems for cybersecurity and cryptology, including cryptography, guaranteeing a sovereign control over the information and communication systems owned by the state. Encryption devices are the most important elements of information and communication systems. In order to achieve a certain level of efficiency of an encryption device, it is necessary to have a full control over this device and in particular over its algorithm and cryptographic key, which as a result leads to the preferential acquisition of such devices produced domestically. However, this technology is difficult and not easy to implement, hence the number of local producers is very limited[3].

Categories of hostile actions and operations in cyberspace

It is possible to understand, what operations in cyberspace are, only after giving points of reference and certain borders to other concepts related to it. Considering that it is a relatively new area of actions, which had had to been swiftly integrated with the already existing actions of different military forces, it became necessary to develop a framework of concepts essential to conduct planning on the operational and tactical level.

Methodological considerations based on direct effects of operations in cyberspace allow us to indicate six categories of external hostile actions[4]:

1. scanning – based on either checking or scanning in order to find weak (vulnerable to attacks) points of the system – this category completely excludes the possibility of taking actions, which would aim at getting access to this system, based mostly on scanning ports and following the movement in the network;
2. intrusion – based on receiving access to the computer system (even without stealing/ destroying data), often taking an advantage of weak system's security;
3. data collection – deliberate collecting of private, protected data ("private" defined as "not belonging to the public domain"), does not always requires the breach of the system and can be executed by communication's monitoring or signals intelligence etc.
4. cyberattack – external operation in cyberspace, causing the disturbance in the functioning or damage (logistical or physical) with relations to data or systems

[3] In Poland there are many polytechnics, where research in the field of cryptography isconducted (i.a. WAT – Military University of Technology in Warsaw; construction works were conducted at WiŁ – Military Communication Institute)

[4] Robert Belk, Matthew Noyes, *On the Use of Offensive Cyber Capabilities. A Policy Analysis on Offensive US Cyber Policy*, Harvard Kennedy School of Government, 2012, p. 42-111.

(this can include actions such as distributed denial of service – DdoS or manipulation of industrial processes – for example Stuxnet)[5];

5. cyber counter attack – limited external cyber-operations with the aim of containing hostile actions in such a way that it influences the computer systems of the enemy;

6. cyber force – refers to cyberattacks of such far-reaching physical effects that should be considered in accordance with international law as "the use of force" (however it remains highly challenging for the international community to classify the term "the use of force" in the context of new technologies and methods of attack).

The cyberspace operations lexicon created for the American army serves as a good example of a practical approach toward the classification of operations in cyberspace[6]:

- cyberspace operations (CO) – the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid (DODIN – Department of Defense Information Networks)[7];
- network operations (NetOps) – activities conducted to operate and defend the DOD's Global Information Grid;
- cyberspace superiority – the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, sea and space forces at a given time and sphere of operations without prohibitive interference by an adversary;

[5] Authors of the analysis apply different than the most common definition, where „attack" is not defined as every unauthorized entrance to the system but only this kind of entrance that causes damage.

[6] "DOD Cyberspace Operations Lexicon", Joint Chiefs of Staff, source: http://www.hsdl.org/?abstract&did=734860&advanced=advanced

[7] GIG – Global Information Grid, a term often replaced by DODIN – Department of Defense Information Networks, including networks used by the U.S. Defense Departament.

- cyber warfare (CW) – an armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber attack, cyber defense, and cyber enabling actions;
- advance force operations – an operation which precedes the main effort in an objective area in order to prepare the objective for the main assault by conducting network systems or nodes – pre-emplacement or clearing of weapons – such as minesweeping, preliminary bombardment, underwater demolitions, or cyber access and/ or weapon implants – and air support;
- computer Network Attack (CNA)[8] – a category of fires employed for offensive purpose in which actions are taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy information resident in the target information system or computer networks, or the systems/ networks themselves. The ultimate intended effect is not necessarily on the targeted system itself, but may support a larger effort, such as information operations or counter-terrorism, e.g., altering or spoofing specific communications or gaining or denying access to adversary communications or logistics channels.
- cyber attack – a hostile act using computer or related networks or systems, and intended to disrupt and/ or destroy an adversary's critical cyber systems, asses, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves – for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery.

[8] Replaces the term CNE – Computer Network Exploitation– the support of operational capacities and collecting of information through computer networks is a collection of data about the aim or automatized information systems of the enemy; the protection of computer networks; operations within computer networks.

As it can be easily seen, the understanding of offensive capabilities and operations in cyberspace is inextricably linked with the support of kinetic actions **due to the fact that apart from being the 5th battlefield, cyberspace has become presently a component of command and control in all other areas of combat operations.**

The use of offensive capabilities in cyberspace

The efficiency of the carried-out operations seems to supports the argument to use cyberspace in order to attain the intended strategic and tactical objectives. The scale effect, which is also visible in the environment of combat operations, is invaluable. A single code might theoretically shut down the entire class of the enemy's combat systems. Above all, operations conducted in cyberspace are carried out with the speed, which is unreachable form the perspective of other traditional measures of managing and leading conflicts[9].

The diversity of operations carried out with the use of cyber weapons is limitless. They can serve for both offensive as well as combat operations in their full scale. On the other hand, the effect of operations in cyberspace can be reversible and serve at all phases of conflict –from the destruction to the reconstruction.

If actions of a particular cyber weapon are addressed against a concrete system of the enemy, they can be used to attack it at different points of time – from the moment of their creation/development (causing problems with operating reliability) up until the decision to use them (a successful disabling of at least one device of a certain class causes uncertainty about the credibility of the entire class beyond those created by kinetic attacks) until countering the effects of the use of a particular weapon after launching an attack with the use of this weapon[10].

The research conducted on the offensive use of the state's capacities within cyberspace focuses i.a. on distinguishing cyber operations according to the level of their utilization – strategic, operational or tactical[11]. On all these levels, cyber attacks are

[9] Maren Leed, *Offensive Cyber Capabilities at the Operational Level. The Way Ahead*, CSIS & Georgia Tech, September 2013, source: http://csis.org/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf, p. 1.

[10] Ibidem, p. 1.

aimed at the denial of access, interruption or deterioration of enemy's capabilities, indirectly (through disinformation) or directly.

On the strategic level, commanders will be more interested big information nodes or those, which are perceived as particularly important by the enemy. Temporary interruption of their functioning might suffice to disrupt the way the enemy acts. However, the complete destruction of the functioning might also be the goal of these operations. The aims of such attacks are chosen in advance, often for several years, which stems to certain extend from its definition. Their characteristics encompass not only their size but also the amount of connections with other nodes and networks. The definition of the strategic goal in cyberspace might concern command and control nodes of the enemy's command and the infrastructure supporting it. These goals will be to large extend static and well-protected not only in cyberspace but also physically.

On the tactical level, commanders will rather perform cyber attacks on the local scale, in order to support the operations led on the scene, which is already controlled by them. This might result in the higher likelihood of ad hoc choices of attacked targets once they are within the range of such attack, for example in the wireless network.

There will also be another approach towards information protection of operations performer in cyberspace, depending on the level they are carried out on. Due to political consequences as well as benefits, which might be lost in the future, if the attack is detected during its execution, from the point of view of the command, the strategic level of discretion of the carried-out attack is of particular importance. Dissimilarly, from the tactical/operational level of command, stronger emphasis might be put by commanders on the speed of the conducted attack than its discretion[12].

It is worth noticing that from the point of view of political and psychological effects, a cyber weapon has immanent limitations (inability to intimidate the enemy or boost the authority of the state as a result of displaying available offensive resources together with simultaneous risk of undermining the authority of the state and its trust).

[11] Ibidem, p. 3.

[12] Ibidem, p. 4.

What is more, in case of well-secured systems, the efficient use of cyber weapon goes hand in hand with the need to use the human component[13].

Network-centric warfare (warfare in the age of high information technology)

While analyzing various aspects of cyberspace impact on the understanding of contemporary security – not only in terms of its definition but also in terms of its practice – the role and influence of high technologies of communication and data processing on the contemporary battlefield shall not be omitted. This development resulted in the creation of the concept of network-centric warfare.

The network-centric warfare is "[…] an emerging theory of war in the Information Age. It is also a concept that, at the highest level, constitutes the military's response to the Information Age. The term network-centric warfare broadly describes the combination of strategies, emerging tactics, techniques, and procedures, and organizations that a fully or even a partially networked force can employ to create a decisive warfighting advantage"[14].

The adjustment of armed forces of a modern state to the new way of waging warfare is not dependent on the ability to find appropriate solutions for technological dilemmas. However, with no doubt without them the new battlefield would never came into existence. The root of the change is in the behavioral matter – the behavior of both, individuals and organizations operating in the networked environment.

A crucial aspect of the new battlefield if the advantage resulting from more common situational awareness. Without any doubt it serves as an argument for a maximal use of the networking character of the battlefield.

The acceleration of the cycle "observation – orientation – decision – action" is a direct effect of the networking of forces[15]. It is an abstract construction, describing the sequence of events, which take place in every military confrontation. The actor of the conflicts has to observe the situation on the battlefield, analyze the tactical situation,

[13] Thomas Rid, *Cyberwar and Peace. Hacking Can Reduce Real-World Violence*, source: http://csis.org/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf.

[14] *The Implementation of Network-Centric Warfare*, op.cit , p. 3.

[15] Carlo Kopp, *Understanding Network Centric Warfare*, op.cit.

make a decision and act. This process is of fundamental importance from the point of view of military operations, which applies not only to the tactical level but also to the strategic one. It is important to notice that this process takes place in every predator-victim relation.

The possibility to accelerate the pace of this process is crucial from the perspective of gaining advantage over the enemy and keeping it in a defensive position. A quick observation and orientation not only ease the decision-making process. Processing data on the battlefield in real time is crucial to form the ability to modify the course of action also during the confrontation – the ability to adjust according to the changing situation in the combat environment.

The increase of the dependence of pace and the way security operations are carried out within the networked environment has at the same time many negative aspects. Among the most important boundary condition, which must be fulfilled in order to benefit from the potential offered by security systems in network environment it is possible identify the following[16]:

1. security of transmission: since the importance of SIGNIT and the proper cryptographic protection of transmission is understandable for all participants of the conflict, it shall be assumed that each side puts maximum effort in recognizing, eavesdropping and decrypting at all stages of the operation; hence, not only the content of the transmission but also the fact of its execution can be a signal, which, if detected, might mean the failure of the operation;
2. robustness of transmission: not only the intended actions of the enemy such as transmission impairments, but even natural events of unpredictable character can put the security of the mission at stake – solar flares or simply bad weather can impair transmission at a key moment of the operation;
3. transmission capacity: in the age of unlimited information sources, including those, which provide digital transmission of high resolution images, video

[16] Ibidem.

recordings and other big data packages, which simultaneously have to be secured against infiltration or impairment (it also reduces the efficiency of links) capacity, which guarantees the smooth transmission is a critical factor;

4. message and signal routing: the transmission of data and commands in networks of variable topology, in a fluid operational environment requires the guarantee of reliable data transmission directly to the addressee;
5. signal format and communications protocol compatibility: one of the most important factors is an interoperable convergence of communication formats – presence in different platforms and systems require the assurance that the incompatibility in signal modulation and digital protocols will not impair efficacy of communication in military environment.

Organizations of the information age: the need for (r)evolution

The information age requires changes not only in the way it functions but also in the way it is organized. It requires the evolution of old and the creation of new structures, which would be able to respond to challenges of modern security environment.

The need of adjustment of the organizational security structures to fulfill requirements of the networked security environment poses a specific challenge. Operating in a network-centric environment requires the construction of organizations, which achieve their objectives due to flexibility of their roles and actions as well as the speed of command[17]. This organizations, which are advanced in the use information technologies, base their actions on innovative structures of command with the aim to cut the enemy from the possibility of taking actions in the quickest possible way. What is also typical for this kind of organization is that they take parallel actions, which due to their multiply effect, achieve an added value by surprising the opponent.

[17] Kishore Sengupta and Carl R. Jones, *Creating Structures for Network-Centric Warfare: Perspectives from Organization Theory*, Naval Postgraduate School, Monterey 1999, source: http://www.dtic.mil/dtic/tr/fulltext/u2/a458996.pdf, s. 1.

In order to fully effectively function in a networked environment such organization needs to have self-designed features and constantly adjust to changing conditions. The theory of organization consists of two concepts, which serve as the basis for discussion over the creation of new type of organization with military structures[18]:

1. the concept of modified organizational forms based on information technologies;
2. the concept of organizations capable of rapid change and innovation.

The concept of modified forms of organization includes virtual organization, strategic alliances, partnerships and networked organizations. What seems to be of particular importance in the context of discussion about network-centric warfare is the approach towards a virtual organization. They can consist of an ad hoc collected group of individuals, coming from more than one institution, with different field of specialization created to execute one specific project.

Even though flexibility and multitasking of a virtual organization, such as for example a combined tasks forces, have many advantages, it is important not to overlook problems, which their use might cause. The dependency of the effectiveness of performed actions on successful communication, which in an organization with a non-tested coordination might fail at a crucial moment, is one of the most important problems. Another one is connected to difficulties with defining the status, authority and scope of competences of the organization. The answer to these problems could be a specified and detailed doctrine of actions, which however should be implemented for a longer period of time until the moment of mutual recognition of the elements of such system[19]. The concept of organizations capable of innovation and rapid change for an effective adjustment to new challenges is based on the precondition that such organizations change in a continuous way, which is determined by difficult conditions (the rule of "adjustment to survive").

[18] Ibidem, p. 3.
[19] Ibidem, p. 5.

MAIN RECOMMENTATIONS FOR THE LONG-TERM DEVELOPMENT OF CYBERSECURITY SYSTEMS AND CAPACITIES OF OPERATING IN CYBERSPACE

1. To perceive obligations to execute tasks in cyberspace in the same way as in other crucial fields guaranteeing national security.
2. To prepare a roadmap of barriers regarding cyber security, with particular focus on the cross-sectoral character of cyber security as well as the need for action on the level of cooperation and coordination within interministerial framework, together with a plan on how to eliminate these barriers, schedule and financial forecasts.
3. To formulate and implement operating algorithms, specifying good practices and rules of interministerial cooperation together with entities of private sector, especially operators of critical information and communication technology, and in case of the execution of interministerial actions in the field of cyber security. They should be implement as an obligatory element of the training preparing for anti-crisis measures.
4. To facilitate the exchange of information within the area of cyber security threats and actions aimed at countering them (the exchange of information between central administrative bodies, competent services, governmental agencies and institutions as well as self-government administration is of particular importance), also on the international level.
5. To conduct policies with funds for the creation of new systematic solutions, ensuring not only the sustaining of the current level of security and capabilities of operating in cyberspace, but also monitoring of the development of new offensive and defensive technologies together with their implementation to national system of cyber security.

6. To actively engage organizations representing private sector and civil society in the process of creating internal guidelines and training policies as well as evaluating and collecting good practices together with identifying challenges and threats.
7. To economically support initiatives connected with cyber security in individual organizations (initiatives of public-private character shall receive prizes for swift reactions to cyber security problems and penalties for an inadequate approach; for example tax advantages or insurances offered under preferential terms).
8. To put stronger emphasis on a good projecting of system, realized with the use of the role of the government as the key receiver of cyber technology.
9. To support interdisciplinary research and scientific research on cyber security.

Summary

Despite the fact that it became a reality that society (and the state) 2.0. is highly depended on network and its constant use on nearly each and every level of its functioning, a lot remains to be done in order to practically adjust structures responsible for security to the needs of this new center.

This applies in particular in security structures. Due to a traditional approach towards organizing itself and the habit to use rigid and hierarchical structures, also from the point of view of cultural organization, the evolution toward a more flexible and networking character of the organization might prove to be a challenge not on a technological level but on the level of mental and psychological abilities to adjust of both, those who give and follow commands.

Their transformation is necessary in order to fully respond to challenges posed by the hybrid – simultaneously material and digital – battlefield. Efforts to limit "the conflict of future" to one of this two dimensions seem to be a major mistake. What seems to be the most likely, is that in the future we will observe a parallel conflict, which will take place at the same time on different levels of material and digital reality. Although there are objective and subjective challenges, which this evolutions might face, it appears to be inevitable and proper preparation for it shall be the commitment to present and to the future of the state.

Authors: Paulina Piasecka, dr Krzysztof Liedel

Editor: Anna Radwan

Translation: Aleksandra Żebrowska

Konrad
Adenauer
Stiftung

This report is the result of expert meeting organized by The Bronisław Komorowski Institute in cooperation with the Konrad Adenauer Stiftung.