STUDIA KRYTYCZNE | Nr 10/2021: 63–72 | ISSN 2450-9078
https://czasopisma.uni.opole.pl/index.php/sk

BOGUSŁAW OLSZEWSKI*
Badacz niezależny

The contemporary multi-layered cybersecurity landscape and emerging nano-threats. An overview

Współczesny wielowarstwowy krajobraz cyberbezpieczeństwa i pojawiające się nano-zagrożenia. Przegląd

CYTOWANIE
Olszewski, Bogusław. 2021. "The contemporary multi-layered cybersecurity landscape and emerging nano-threats. An overview". *Critical Studies* 10: 63–72.

ABSTRACT
Presented article attempts to identify the key node located in the three-tier model of cyberspace, the node which is characterized by the greatest potential impact on the other elements essential for the functioning of the whole network, especially in the security context. Based on the network analysis, it was proposed to place the 'persona' in the center of interest, in other words the human factor. In this way – regardless of the future direction of the further development of artificial intelligence – an individual adversary is able to dispose the historically unprecedented ability to put an impact on the critical and – potentially – military infrastructure of the state. Thus, individual digitally-skilled person is capable of destabilizing the post-industrial society not only in the context of network/computer security, but also physical security (through the cyber-physical systems).

KEY WORDS
cyberspace, persona, cyberpersona, layers, cyberwar, adversary

Introduction

Cyberwar has become logical development of the previous forms of military operations, characteristic for the past ages: pre-industrial and industrial one, and the same regrading to the civilian critical infrastructure. To explain the role of an individual in this new type of warfare,

* e-mail: boguslaw.olsz@gmail.com

tailored model has been adopted based on the well-known three-layer view of the cyberspace. The presented model constitutes a kind of simplification, as the actual scale of events and relations in the dynamic system of the layers is huge. The strength and density of linked nodes change constantly as devices are frequently connected and disconnected, creating evolving, temporary state in regional and global security architecture. Followed analysis is introducing modified layered model to expose the most important elements of the structure.

The aim of this publication is an attempt to define the key point of this layered structure of cyberspace – the crucial element which is being currently the most important source of threats to the security of the networks and computer systems. The research hypothesis is to highlight the role of single adversary [a human] as the most influential source of potential impact, an animator who is able to induce the destabilization of civilian and military network systems on a large scale, acting as an independent unit by itself. The starting – as well as the main – point of reference for the following considerations becomes layered model of cyberspace, in relation to which the network analysis will be applied. All of that will allow to select the key node influencing the state of institutional/civilian cybersecurity and the cyberspace in the military context as well.

The terminology used in this article includes the terms 'cyberspace' and 'cyberwar'. Cyberspace will be treated here as a three-tier structure, 'global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers' (Congressional Research Service… 2021). The cyberwar will be considered as an aim to detabilize and destroy civilian critical infrastructure via network, and – in the case of military operations – to weaken the ability to conduct digital-wepon-related operations in cyberspace, as well as to reduce effectiveness of the conventional, active warfare on the contemporary, digtalized and networked battlefield. In the military perspective, 'offensive Cyberspace Operations, intended to project power by the application of force in and through cyberspace. These operations are authorized like operations in the physical domains' (Congressional Research Service… 2021).

Layers of cyberspace

Nowadays, the structure of cyberspace is most often presented in the form of layered model, partially based on specific standards derived from computer science: ISO/OSI and TCP/IP models. Three-tier model of cyberspace stands as a reference point but the first and third layer are complex, allowing de facto five levels to be distinguished in the de-

tailed model. Physical layer (all the tangible elements of the network infrastructure along with their geographical location) constitutes the first layer. The second layer, logical (syntactic), is the plane of data, algorithms and software. The third, social (semantic) layer consists of natural persons (individuals, humans) and their digital images, as well as access devices and their virtual identifiers on the telecommunications networks.

Fig. 1: Three-tier model of cyberspace

The general view of the network in social sciences is two-folded. The first line to that issue, indeed a highly formalized, is related to mathematical tools (graph theory) used for description and analysis of the social relations (network analysis). The second approach is treated "as a theory (or sometimes only a metaphore) of social organization" (Mueller 2010, 31). Graph theory is one of the first attempts at network interpretation and analysis, a mathematical conceptualization of networks. Graph – an object consisting of vertices and edges – presents a given type of relation, it can be directed (edges have a direction; in the model below they are directed) or undirected as well. There are multiple concepts (political, economic, sociological) concerning the factors influencing the final shape of the definition of network organization. Following Marian Surmaczyński's (2010, 33–34) point of view that

> For a political scientist, the use of research techniques belonging to other social sciences sometimes becomes a cognitive necessity (…) In this way, a political scientist (e.g. graduate student or doctoral student) creates his own methods helpful in re-

> search. (…) However, it is best to create your own methods. They can be hybrid connections – it depends on what topic becomes the subject of research (…) In this way, many issues will come together and simply a fragment of political science research will be created,

we can adopt and transform aforementioned model of cyberspace to try to localize crucial element in a pretty complex cyber threat landscape.

The network science, as derived from sociology, social psychology and anthropology, includes: network theory (network science is currently area of the intense interdisciplinary research), social network theory, social network analysis (using statistical methods and algebra as a basic tools), making the public, biological or economic system the point of interest: "A common concept in the network science is to understand and study the complex structures and behaviors that occur between entities that are the subject of network research" (Ujwary-Gil 2017, 21). This approach, emphasizing the universal nature of networks in the real world, has emerged and has been observed since the end of the 20th century, operating within the network paradigm shaped by empirical research on the information and social networks. It is an extremely useful analysis tool that reduces reality to a system of nodes and connections, which emphasizes the relationships between interdependent system factors, the structure and properties of the network, and its dynamics (processes). At the level of the entire network there are factors such as, for example: network density (ratio of relationships to all the possible connections in the "Individual or collaborative hackers engaged by states become *ad hoc* hubs within the network paradigm, *ad hoc* network poles that are the subject of the digital and kinetic attacks" (Olszewski 2019, 7) – the higher the density, the higher the degree of its cross-linking (completeness); centralization of the network (relative dominance of a single node over the other in the network, measured by number of direct links between them).

Focal point of the digital threats

Following analysis concerns a dynamic network (Olszewski 2019) what cyberspace in fact remains: "The dynamic aspect of the network (dynamic networks) refers to the relationship and interaction between entities in which information, knowledge or resources exchange and flow. Entire networks in which actors are involved, also constantly change their shape" (Ujwary-Gil 2017: 59). The network analysis has been simplified and transformed to apply it adequately to the chosen research object: cyberspace as a socio-technical system. Thus qualitative network analysis – the network science is based on the three approaches: mathematized social network analysis (SNA), qualitative methodology and the study of complex networks (within the framework of complexity theory) – has been adapted to the three-layer model of

cyberspace using the concept of a graph: vertices (nodes, actors) and edges (connections, relations, connections, links, relations) as the elements of the structure enabling the presentation and examination of dependencies between objects, which are currently functioning in the context of ongoing militarization of cyberspace. This simplification, while maintaining the formal dimension of the analysis, allowed to probe and expose those elements of the social organization which are occurring in virtual reality, and that affect the cyberwar-related issues.

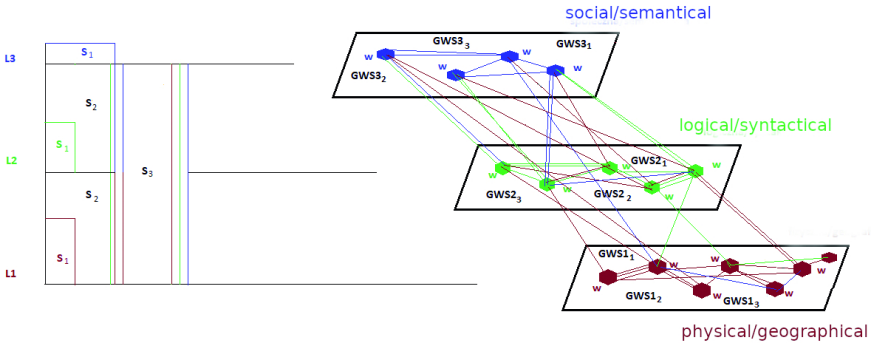

Fig. 2: Modified network analysis levels based on three-layer model of cyberspace

Layer 3 (L3) – social layer, consists of real individuals who are currently paticipating in the network (persona), and their network identifiers or cyber identities, such as e-mail address, IP or MAC-address of the access device, mobile phone number etc. (cyberpersona). A given participant or adversary may have multiple cyber identities (a few access devices, e-mail addresses, social media-related accounts), and one cyberpersona may reflect several users (personas) e.g. a commonly used single account in an online store).

Layer 2 (L2) – logical layer, consists of a network component in the form of logical connections existing between nodes (W) of a horizontal but parallely hierarchical network. The node can be logical aspect of any device connected to computer network: in a network running with the TCP/IP internet protocol, the node is any host; in a private VPN network – authorized IP address; in an intranet network – computers connected to the local network (Ethernet IP address range); resources on the server, database-related content etc.

Layer 1 (L1) – physical layer, composed of geographical component (physical location of the network nodes) and physical network components: hardware and the basic elements of the infrastructure (incl. wired and wireless media) which provides network functionality, and supports physical forms of connection (wires, radio frequencies, modems, routers, servers). In the context of the political science, geopolitical boundaries are replaced on this layer by some physical constraints at the hardware level (vide the Great Firewall).

On each of the layers (L), it is possible to identify and describe the nodes (W) as well as the bonds with a specific orientation, number and strength (S), and density (G). Nodes interact with some force: within the same cyberspace layer (S1), between two adjacent layers (S2) and through all the layers (S3). Nodes located on the layers can be elements of critical infrastructure of the given state, resources located on the government servers, state institutions, state-sponsored entities, non-state actors, commercial entities, criminal organizations, single adversary, NGOs, network devices, microprocessors, private VPN networks, legal norms, key politicians and commanders of the armed forces, so on. Their "significance does not always depend on the number of connections but results from their quality, and the importance of the other nodes connected to. The digitized and networked security environment is not hierarchical and, according to the network paradigm, the boundaries between national (external) security and internal security are blurred. The security and international relations environment has a network structure – in this perspective, its elements (states, societies, institutions, individuals) become nodes of global social, political, military, criminal networks etc., due to the fact that the boundaries of the systems are blurred" (Dissertation: 10). Nodes are relatively constant or random (chaotic). There are connections between the nodes on the layers, with the strength and density adequate to the status or the role playing by the node in the entire model. Many nodes are not static or they can't be unequivocally assessed, such as in the case of the stealth adversaries (most of their connections can't be determined then), or botnet devices where the dormant software is waiting to be activated by the bot herder (*ad hoc* nodes).

Introducing the nano-threat

Due to the minor scale of the source of presented threat, considered here as a single part of the vast collection of the users who are being currently online – 5.03 billion (Digital around the world 2022) – the adequate prefix 'nano' will be introduced. On the basis of the analysis of the nodes and relations connecting them, we can finally distinguished two key actors in the adopted model of cyberspace, related to its militarization: an adversary on L3 (in fact, because of some inconsistency visible in the layered model, the adversary is physically located on the L1, as a biological time-space being not only as an abstract social individual on L3 – persona) – and the physical attributes of the nation-state (incl. its physical network resources) on L1. The interaction takes place at the L2 layer, where the adversary may theoretically be identified by the IP or MAC-address of his device, and on the L3 layer (cyberpersona). In case of a cyberattack, the state government may try to block involved cyberpersona by limiting its functionality on the L2 layer (using fire-

wall, Intrusion Detection System, Intrusion Prevention System, SIEM tools, SOC analysts, threat hunters and similar). But the most probably, state's attempts to influence adversary's cyberpersona through L2 won't be successful at all or will remain without any significant effects, because attacker may change the access device or the cyberpersona itself (spoofing) making these efforts unsuccessful. Therefore the key factor from the adversary's point of view is, inter alia, social engineering – enabling the acquisition of the parameters of another cyberpersona for authorization on another access device and allowing of further malicious activity on L2. The virtual nature of cyberpersona makes it difficult or even impossible to identify the real human/persona on L3 through L2 even if it's more probable to find/localize the device used by.

An adversary can, for example, influence politician (w) L3 by attacking his cyberpersonality (w) L3 (hijacking a social account, revealing sensitive stored data, using cyberbullying, deep fake, information warfare and many others). Adversary's attack on the cyber-physical plane (CP) is a destructive influence on an individual (persona) (w) L3 through nodes on L2 aimed to (w) L1: IoT elements like pacemaker, autonomous car, drug dispenser, home automation, elements of communication infrastructure of smart city (to arrange politician-schedule-based traffic collision). If the given individual is a key node in the state's hierarchical structure (president, prime minister, commander of the armed forces), the flow of interactions between nodes on L3-L2-L1 and L3-L2-L1-L3 layers enables the sudden destabilization of the social structure. Along the L3-L2 line, the adversary can obtain sensitive data, modify or destroy them, gain access to the government secrets.As a cyberpersona – he can interact in the sequence (w) L3 – (w) L3 to obtain effects on (w) L1 (impersonating decision-maker in order to influence the physical component of the critical infrastructure through another physical individual, e.g. causing a network device to be turned off, granting access to the network by forcing someone to obey an order.

It is worth underlining once again: having a micro-force, adversary is able to destabilize the whole state-government only through L3-L2-L1 sequence (destruction or deprivation of functionality of the elements of critical infrastructure) and L3-L2-L3 (discreditation, blackmail or physical elimination of a politician), and L3-L2 (data interference, or protocols); not forgetting that L1 as a transmission medium-related plane is essential in all the cases. Distant adversary interacts via L2 – if has no access to L1, then to L2 as well, and won't reach any persona and cyberpersona on L3, or any cyber-physical elements on the L1 (destructing of three-dimensional and geographically-located foundations of the global web, switching off particular transmission devices or disrupting actuators, switching off power plant), nor to the digital resources on L2. Moreover, in the frame of L3 alone the adversary is not able to fully operating but only passively: as a source of instructions placed in

social media or as a code-delivery source. The same in the case of the state which lacks of L1-related attributes – *vide* micronations (virtual states) without its own physical territory nor physical infrastructure resources; virtual representation of the physically existing state is only its complement/tool/extension but not the state itself. Thus the authorities cannot get rid of their own network infrastructure on L1 and logical layer L2 (they can isolate networks using network protocols, firewalls, encryption, and physical separation), it practically means to remove the network in general. But – when taking a look at Chinese Great Firewall – the state is able to isolate the entire critical infrastructure, sub-networks of the public administration, and citizens as well.

As a result of the network analysis carried out, I came to the conclusion that in the contemporary cyberwar, the central and the most important position of a node in the entire network does not result from the huge number and strength of the connections, but spring from the ability to operate effectively on all the layers, and that the cyberpersona-state dyad reveals the most unfavorable position of the state ever. Single, well-skilled adversary (even if still a team-player), is the crucial one just because of micro-force, as a contrary to the massive armies of the past Napoleonic and industrial wars. Therefore, although the state exercises formal control over L1, L2 and L3, in order to successfully eliminate the adversary it have to take physical action on L1 (classic kinetic attack) and L1-L2 layers (kinetic but with the use of intelligent weapons, such as a combat drone, cyber-physical elements). Adversary, functioning initially in the L3 layer (persona and cyberpersona) but physically localized on L1 as well), obtains an asymmetric advantage over the state only through the logical layer, whether it is used the network infrastructure (w) L1, data and digital resources of the state (w) L2, or ultimately a directed cyber attack on the public figures (w) L3. Therefore the adversary is able to use all the layers of the model.

That's why single adversary has become a belligerent party, according to the provisions of Tallinn Manual 1.0 based on the humanitarian law regulations regarding classical model of warfare (kinetic). Adversaries have become combatants despite their exclusive influence through the L2 layer, as they attack another persona and cyberpersona (L3), causing logical (L2) and kinetic (L1) damages, and – similarly – can be physically eliminated on (L1-L3) – through the state's kinetic actions initiated in the real world.

Summary

The knowledge society generates more and more specialized technology-driven adversaries, and they become the most important nodes in the cybersecurity world and the cyberwar as well. This fact makes single person extremely effective in the process of animation of the

digital-performance shaping factors, influencing on the key nodes of cyberspace. It also determines the single human's ability to influence the course of combat in the military sense, including waged by the kinetic means of war. Theoretically, it allows for potential destabilization of complex military operations or specific tactical tasks of specific types of troops (signal corps, artillery, tanks etc) if perfectly tailored to it. It is a significant and unprecedented – quantitative and qualitative – change, even if compared to the historical, well-known successful one-man-performed acts of sabotage, affected the broader context of the past military operations of the industrial era. Of course, excluding single person decision making related to launching the procedure for the use of nuclear weapons.

* * *

Supplement

The hiring process for the security operations center as a vulnerability

The transfer of the former employees to another company results in the outflow of not only skills, knowledge and know-how but also loss of the living information-base about both employer's and/or customer's networks: key elements of their topologies, IP addresses and DNS names, the most frequent rising alerts and threats, modus operandi of cybersecurity analysts, as well as on internal and external procedures. It allows for identification of the key individuals and for obtaining their professional and personal data (industrial espionage in general). It is important to emphasize the role of former employees as a source of potential information, not only related to the former employer, but also of entities supported by.

But additionally, the potential employee (masked adversary) in the 'transition mode' is dangerous not only for the current but for the potential employer as well. The situation related to the job change is normal from the perspective of the potential employer – seeking for a job is business as usual. Hiring interview can be very useful from the standpoint of the adversary, delivering a lot of valuable information about the company. All of that put recruitment process in the social engineering context – the HR department itself as well as all the employees involved in the interview. Any truthful (especially technical details) information provided to candidate during the recruitment process, which is not strictly related to the issues tied with remuneration and job-related responsibilities in general (dress code or working hours) creates a vulnerability, and should be treated as a part of the reconnaissance phase.

Thus, the creation of temporary false identities on the company side should be considered for the purposes of the recruitment process: fake

social network profile of the recruiter, interim phone number and email address; moreover, job interview should be conducted by individuals not directly related to the cybersecurity department.

Bibliography

Bousquette, Antoine J. 2009. *The scientific way of warfare: Order and chaos on the battlefields of modernity*. New York: Columbia University Press.

Congressional Research Service. 2021. *Defense primer: Cyberspace operations*. "FAS Project on Government Secrecy". December 1. Accessed: June 20, 2022, https://sgp.fas.org/crs/natsec/IF10537.pdf.

Digital around the world. 2022. "Datereportal", [no date]. Accessed: June 20, 2022, https://datareportal.com/global-digital-overview.

Harris Shane. 2014. *@War: The rise of the military-internet complex*. Boston, MA: Houghton Mifflin Harcourt.

Kaldor, Mary. 2012. *New and old wars: Organized violence in a global era*. Cambridge: Polity Press.

Mazanec, Brian M. 2015. *The evolution of cyber war: International norms for emerging-technology weapons*. Lincoln: Nebraska Press.

Mueller, Milton L. 2010. *Networks and states: The global politics of Internet governance*. Cambridge, MA: MIT Press.

Olszewski, Bogusław. 2019. *Legal and international aspects of the militarization of cyberspace*, Wroclaw: UWr, PhD dissertation. "ResearchGate". Accessed: June 20 2022. https://www.researchgate.net/publication/340448510 _Prawnomiedzynarodowe_aspekty_militaryzacji_cyberprzestrzeni_Legal_and_International_Aspects_of_the_Militarization_of_Cyberspace.

Shakarian, Paulo, Shakarian Jana and Andrew Ruef. 2013. *Introduction to cyberwarfare: A multidisciplinary approach*. Amsterdam: Syngress.

Surmaczyński, Marian 2010. *Podstawowe problemy metodologioczne nauk społeczno-politycznych*. Wrocław: Wydawnictwo Uniwersytetu Wrocławskiego.

The United States Army. 2010. *Cyberspace operations concept capability plan 2016–2028*. "TRADOC Pamphlet 525-7-8". February 22. Accessed: January 16, 2022, https://irp.fas.org/doddir/army/pam525-7-8.pdf

Ujwary-Gil, Anna. 2017. *Audyt zasobów niematerialnych z wykorzystaniem analizy sieci organizacyjnej*. Warszawa: Wydawnictwo Naukowe PWN.