MILITARY NATIONAL SECURITY SERVICE

Issue 2. 2019

NATIONAL SECURITY REVIEW

BUDAPEST

Scientific Periodical of the
Military National Security Service

Responsible Publisher:

Lt. Gen. János Béres, PhD Director General
Chairman of the Scientific Board

Postal Address:

Katonai Nemzetbiztonsági Szolgálat Tudományos Tanácsa
1111 Budapest, Bartók Béla u.24-26.
1502 Budapest, Pf. 117

E-mail: natsecreview@gmail.com
Webpage: http://www.knbsz.gov.hu

TABLE OF CONTENTS

DÓRA DÉVAI

THE EVOLUTION OF THE UNITED STATES CYBER COMMAND AND THE INTEGRATION OF CYBERSPACE CAPABILITIES

Abstract

The creation and integration of cyberspace capabilities into full-scale military operations and organizations has been an increasingly prevalent challenge for national armed forces. In the US, this trend has strongly manifested itself by the establishment of US Cyber Command June 2009 and later on by its elevation to the tenth independent unified combatant command of the US Department of Defense (DOD) on 4 May 2018. Parallelly, the four major US military brancheshave built cyber capabilities within their own cadre. Besides the standardized framework pertaining to the joint force operations, the US Army, Navy, Air Force and the Marine Force have considerable freedom in the way they build and deploy their cyberspace forces due to their distinct service needs, paradigms and organizational units. This case study pursues this two-tier integration process putting in focus the organizational and operational structure of the Cyber Command. Subsequently, the development of the joint operational planning process is examined.

Keywords**:** US Cyber Command, Service Cyberspace Component (SCC) commands, Military cyberspace operations (CO)

Introduction

Military cyberspace operations (CO) have been ongoing since the first appearance of computers long before the Internet, and their role in traditional military operations has been growing in parallel with the spread of computerized technology. Consequently, cyberspace by now has been operationalized as a military domain and thus, cyberspace operations are becoming an integral part of military operations. Over the past years, both NATO and the European Union have been actively engaged in constructing cyberspace operations capabilities, and thus member states, including Hungary are compelled to develop their national military cyberspace structures. Nonetheless, as there is no unified blueprint for such capability development. As a result, nation states are learning on the job and strive to make use the lessons learnt from other nation states too. Therefore, an overview of the US development process might provide some useful insight for foreign audience as well.

While earlier on, COs were used as a strategic asset deployed through a highly compartmentalized procedure, and commanders may have conducted CO to specifically support information operations, the aim today is rather to use COs more broadly to support other types of military objectives whenever this necessary and suitable enhance operational efficiency. Cyber forces are to be integrated on a regular basis not just at the strategic, but also at the operational and tactical levels through

appropriate cells and working groups, and cyber planning needs to be synchronized with and integrated into other military operations planning and execution.

This article examines some fundamental questions in order to better understand how this comprehensive integration process has evolved in the US military. This article first examines the organization and relationships of United States Cyber Command (USCYBERCOM). How have the mission and organization of Department of Defense cyberspace activities have changed as a result? What are the responsibilities of the United States Cyber Command (USCYBERCOM) and the Service Cyberspace Component (SCC) commands?

A large part of the primary source literature related to cyberspace is classified. The publicly available unclassified or declassified joint force and service doctrines, procedure descriptions, fact sheets and Congressional Testimonies were used as primary sources. Published interviews with USCYBERCOM and Army cyber officers served as secondary resources for this case study.

Throughout this study cyberspace is defined in accordance with the latest Joint Staff doctrine as "the domain within the information environment that consists of the interdependent network of information technology (IT) infrastructures and resident data. It includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[1] In terms of cyberspace operations (CO) the same source is used where COs are broadly defined as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[2]

The Evolution of Cyber Command

The Antecedents

The US Department of Defense and early computer security researches sponsored by DOD propelled the development of sophisticated computer penetration technologies. In the 1960s researchers at RAND (Research and Development) Corporation, IBM and the National Security Authorities (NSA) warned that attempts to penetrate military and civilian systems is a factor to take into account.[3] By the early 1990s, the various US military services independently developed and integrated offensive and defensive cyberspace capabilities with other information operation elements. By the end of the 1990s, several efforts were made to bring together these separate capabilities. For example, the National Security Agency created the Information Operations Technology Center to help bring together the capabilities being separately developed in each of the services.[4] It is beyond the scope of this study

---

1 Cyberspace Operations. Joint Publication J-P 3-12. June 2018. p. I-1.

2 Ibid.

3 US Government Computer Penetration Programs and the Implications for Cyberwar. Edward HUNT, IEEE Annals of the History of Computing, Volume 34, Number 3, July-September, 2012, pp. 4-21.

4 William ARKIN: The Cyber Bomb in Yugoslavia; Washington Post, October 25, 1999. Cited in Addressing Cyber Instability. Edited by Dr. James C. MULVENON and Dr. Gregory J. RATTRAY. Cyber Conflict Studies Association, US. 2012.

to overview all the organizational stages of the current Cyber Command. The aim is rather to highlight the principal line and pace of development.

Initially, the security and military thinking revolved around strategic-level computer attacks. The Joint Task Force for Computer Network Defense (JTF-CND) was established on December 30, 1998 by the DoD as a joint warfighting unit and to defend against strategic computer network attacks. By the time of achieving full operational capability, the total personnel was 24. A Task Force is a purpose-built component within a force organized for a specific task or tasks. A Joint Task Force is drawn from multiple military branches.[5] JTF-CND was linked to the Global Operations and Security Center of the Defense Information Systems Agency (DISA) in Washington, DC. At first, the JTF-CND was not allotted to an unified command, so its commander reported through the Chairman of the Joint Chiefs of Staff to the Secretary of Defense.[6] It was also a priority to build connection with services and regional warfighting commanders through a command arrangement. Less than a year later, JTF-CND was placed under the U.S. Space Command with responsibilities that included DoD-wide defense actions to stop computer network attack (CNA) and computer network exploitation (CNE) efforts and to mitigate the effects of any attacks.[7] In 2008, the JTF-CND's mission was to ensure that the Global Information Grid GIG operates *"as a single, unified, agile, and adaptive enterprise capable of providing responsive and resilient support to multiple simultaneous mission areas under uncertain and changing conditions."*[8] This can be summarized as mission assurance and business continuity of mission.

Offensive computer network attack was assigned too to U.S. Space Command, and the JTF-CND was renamed to Joint Task Force-Computer Network Operations (JTF-CNO) in April 2001. The new commander was dual-hatted as Vice Director, DISA. In 2003, JTF-CNO was realigned under the new U.S. Strategic Command (USSTRATCOM) which came about through the merging of U.S. Space Command and the existing U.S. Strategic Command.[9] In terms of size, in February 2003, the JTF-CNO personnel was 122 with a yearly budget of yearly budget of about $26 million.[10] In 2004, for the first time in network operations a governance model and the complete command lines were established from the secretary of defense to the STRATCOM commander, to the JTF commander, to each of the appointed component commanders within the military services and representatives within the

---

5 Targeting in Cyber Operations: FOIA release discusses considerations of US military targeting doctrine. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2019-09-05/targeting-cyber-operations-foia-release-discusses-considerations-us-military-targeting-doctrine. (downloaded 15 May 2019)

6 Jeffrey L. CATON: Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications; Strategic Studies Institute & U.S. Army War College Press, January 2015.

7 Ibid.

8 Department of Defense NetOps Strategic Vision; https://dodcio.defense.gov/Portals/0/Documents/DIEA/DoD_NetOps_Strategic_Vision.pdf (downloaded 15 May 2019)

9 Army Support of Military Cyberspace Operations (2015) op. cit.

10 Joint Task Force – Computer Network Operations. Fact File. US Strategic Command. http://www.iwar.org.uk/iwar/resources/JIOC/computer-network-operations.htm (downloaded 15 May 2019)

combatant commands and defense agencies.[11] The JTF-commander was responsible for the proper operation and defense of the DoD global information grid (GIG).

In 2003, the DoD offensive cyberspace mission of network attack was transferred to a Network Attack Support Staff also under the operational control of USSTRATCOM but allotted to the National Security Agency. Besides being a member of the intelligence community that focuses on national-level intelligence priorities, the National Security Agency/Central Security Service is also a Combat Support Agency – a component of DOD – that addresses military intelligence priorities and provides information assurance support to the military.[12] In January 2005, this staff became the Joint Functional Component Command–Network Warfare (JFCC-NW), and the Director of the NSA was designated as the commander of the unit. As a result, the offensive cyberspace mission was separated from the defensive cyberspace mission carried out by the Director of DISA in the role of commander. USSTRATCOM has also begun to develop tactics, techniques, and procedures and other concepts designed to integrate cyberspace capabilities into cross-mission strike plans.[13] In 2007, Lieutenant General Keith Alexander Director, NSA and commander, JFCC-NW referred to the Task Force' activities as:

"We are developing concepts to address warfighting in cyberspace ... . These concepts, and the cyberspace effects that they focus on, are clearly based on the military concepts of strike, fires (supporting and suppressing), and defense. ... In order to fully engage in the development of joint doctrine within the cyberspace domain, it is also necessary to develop a definition of exactly what warfare within cyberspace — or cyberspace warfare — is."[14]

In 2008, the arrangement of two separate task forces was restructured when operational command of JTF-GNO was placed under JFCC-NW. Hence, instead of separating offensive and defensive missions, this move reflects the intention to integrate information assurance, computer network operations and intelligence services.

Finally, in June 2009, the creation of a new sub-unified command under USSTRATCOM – U.S. Cyber Command was directed. The new command achieved full operational capacity in May 2010 incorporating the existing DoD cyberspace units such as the service component and agency connections. JTF-GNO and JFCC-NW were merged into the Joint Operations Center.[15]

Under the dual-hatted leadership the USCYBERCOM commander is also the head of the National Security Agency and Central Security Service, channeling in national security cryptology, signals intelligence, and information assurance into the cyberspace operations mix. At the same time, military services also had to establish cyberspace commands to support USCYBERCOM. By October 2010, the following

---

11 Army Support of Military Cyberspace Operations (2015) op. cit.

12 Defense Cybersecurity: DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened; US Government Accountability Office. August, 2017. p. 8.

13 Army Support of Military Cyberspace Operations (2015) op. cit.

14 Keith ALEXANDER: Warfighting in Cyberspace; Joint Force Quarterly, Issue 46, 3rd Quarter 2007, p. 61.

15 Army Support of Military Cyberspace Operations (2015) op. cit.

component support commands were up and running: Army Cyber Command (ARCYBER), Fleet Cyber Command, 10th Fleet (FLTCYBER); Marine Forces Cyber (MARFORCYBER); and 24th Air Force (AFCYBER).

USCYBERCOM thus have five types of command elements: Headquarters Cyber National Mission Force (HQ CNMF), Joint Force Headquarters – Cyber (JFHQ-C), JFHQ-DODIN, Combatant Commands, and Services Component Commands. Each Services Component Command comprises the service specific Joint Force Headquarters – Cyber to support the geographic and functional combatant commands across the globe, which constituted a meaningful first step to integrating cyberspace operations to deliver effects in support of combatant commanders.

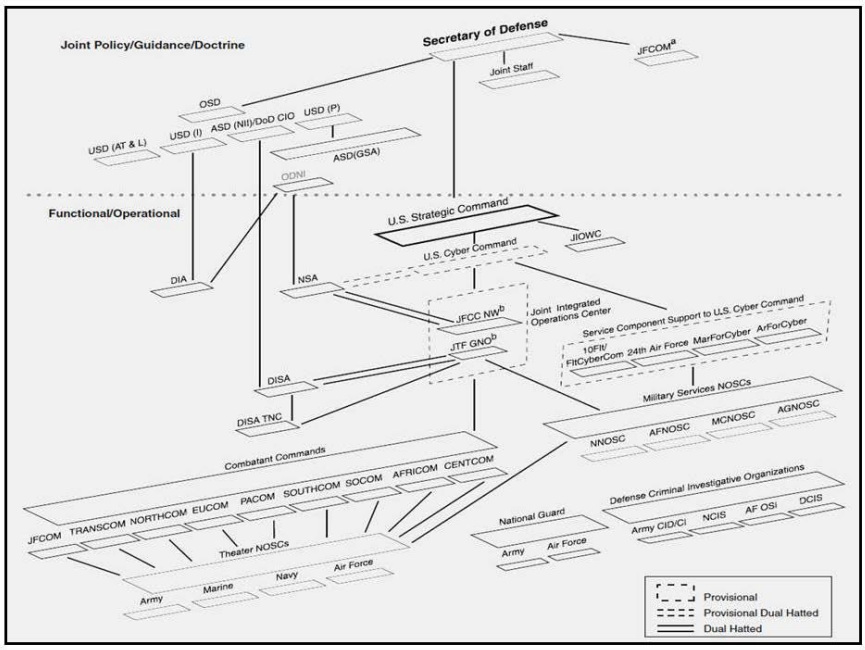


Figure 1. USCYBERCOM Formation and DoD Cyber Organization *(March 2010)*[16]

The Current Organization and the Relationships of Cyber Command with the Military Branches

Cyber Command's overarching task is to provide unity of effort through planning, coordination, integration, synchronization and conducting activities to: "direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military

[16] Defense Department Cyber Efforts: DoD Faces Challenge in its Cyber Activities," Report GAO-11-75, Washington, DC: U.S. Government Accountability Office, July 2011, p. 18.

cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."[17]

The creation of trained and ready cyber forces has also been a principal priority from the beginning. In March of 2013 the first task order (TASKORD) ordered the service components to begin the process of building Cyber Mission Force (CMF) teams.[18] The 2014 QDR called for a total of 133 cyber teams to be available by fiscal year 2019.[19] The first wave of CMFs with a total number of 6200 personnel announced full operational readiness in May 2018. Nevertheless, audit report shows that there is still a long way to go till the actual combat readiness of the teams.[20] This force gathered military and civilian talent from across the DOD and Intelligence Community. CMF troops are provided, trained and equipped by the individual services, but all according to the unified training regime of USCYBERCOM. The CMF teams are considered as elite units of services top most cyber talents.

Cyber Mission Force Training

The standardized training of the CMFs by CYBERCOM is a powerful tool to achieve unity of effort and interoperability across services. Figure 2. presents the training roles and responsibilities.

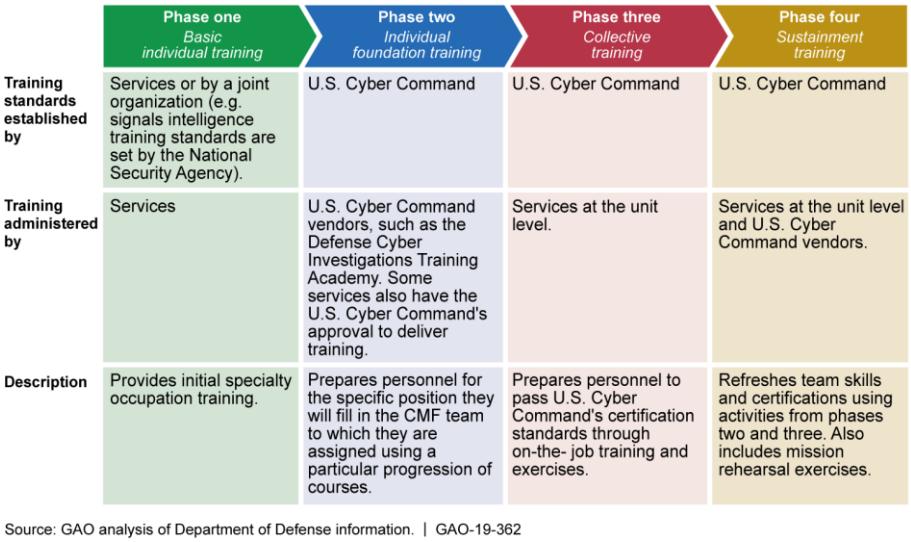
---

17 U.S. Cyber Command (USCYBERCOM). Factsheet from U.S. Strategic Command http://www.stratcom.mil/Portals/8/Documents/CYBERCOM_Fact_Sheet.pdf. (downloaded 15 May 2019)

18 Preparing for Computer Network Operations: USCYBERCOM Documents Trace Path to Operational Cyber Force. National Security Archive. George Washington University. https://nsarchive.gwu.edu/news/cyber-vault/2019-05-03/preparing-computer-network-operations-uscybercom-documents-trace-path-operational-cyber-force. (downloaded 15 May 2019)

19 Department of Defense, Quadrennial Defense Review 2014, Washington DC: U.S. Government Printing Office, March 4, 2014, pp. 14-15.

20 Future Warfare. Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations. US Government Accountability Office. August, 2019.



	Phase one *Basic individual training*	Phase two *Individual foundation training*	Phase three *Collective training*	Phase four *Sustainment training*
Training standards established by	Services or by a joint organization (e.g. signals intelligence training standards are set by the National Security Agency).	U.S. Cyber Command	U.S. Cyber Command	U.S. Cyber Command
Training administered by	Services	U.S. Cyber Command vendors, such as the Defense Cyber Investigations Training Academy. Some services also have the U.S. Cyber Command's approval to deliver training.	Services at the unit level.	Services at the unit level and U.S. Cyber Command vendors.
Description	Provides initial specialty occupation training.	Prepares personnel for the specific position they will fill in the CMF team to which they are assigned using a particular progression of courses.	Prepares personnel to pass U.S. Cyber Command's certification standards through on-the- job training and exercises.	Refreshes team skills and certifications using activities from phases two and three. Also includes mission rehearsal exercises.

Source: GAO analysis of Department of Defense information. | GAO-19-362

Figure 2. Cyber Mission Force (CMF) Training Model Phases[21]

CYBERCOM entrusted to the Army the lead role in the development of a Persistent Cyber Training Environment. The goal of that training environment is to provide on-demand access to scenarios to enhance the efficiency of phase three (collective) and phase four (sustainment) training and exercise events. CYBERCOM uses simulated operational events on networks to support the certification of CMF teams. For example, CYBER KNIGHT is a training event offered periodically by CYBERCOM for CMF teams to exercise national and non-national mission sets. CYBER FLAG and CYBER GUARD, also conducted by CYBERCOM on a periodic basis, utilize a dynamic joint cyber training environment and train all types of CMF teams. [22]

CMF structure

CMFs are divided according to mission areas and command order. Figure 3. presents the division of the CMF teams according to mission areas. Figure 4. shows the service contributions to the different teams. Figure 5. presents the command relationships of the teams in the DoD.

[21] Source: DOD Training U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force. US Government Accountability Office. March, 2019.

[22] Ibid. p. 13.

Mission Team	Mission Area
13 National Mission Teams with 8 National Support Teams	Defending national critical infrastructure
27 Combat Mission Teams with 17 Combat Support Teams	Providing cyber support to combatant commanders
18 National Cyber Protection Teams (CPTs)	Operating and defending the DoD information networks
24 Service CPTs	
26 Combatant Command and DoD Information Network CPTs	

Figure 3. Cyber Mission Teams
(Figure prepared by the author)

National Mission Teams are typically aligned to a malicious cyber actor, meaning they are often in "red space" and "grey space" meaning conducting on-network operations in adversary and in neutral territory in order to get indications and warning of adversary cyber activities, and enabling cyber effects when authorized and directed. CNMF is has a wide range of response options tailored to specific cyber actors and scenarios. The CNMF plans, directs, and synchronizes full-spectrum cyberspace operations to defend the U.S. homeland and vital interests from disruptive or destructive cyber attacks of significant consequence. Headquartered at Fort Meade, Maryland, it has forces in Georgia, Texas, and Hawaii, and engages with partners around the world. It synchronizes efforts across different geographical locations and optimizes the balance between on-site and remote operations effects. The success of the CNMF mission relies on establishing seamless partnerships with the NSA, DOD, and Intelligence Community. The CNMF is strengthening partnerships with the Department of Homeland Security (DHS) and FBI and expanding its partnerships to include other Ffederal agencies, industry, academia, and the international sphere.[23]

National support teams support the mission teams, they are, for example, linguists and analysts and they serve in an intelligence role, providing analytical and planning support to the national mission and combat mission teams. Combat mission teams and combat support teams plan and implement offensive cyber operations to achieve or directly support combatant commander objectives. Cyber protection teams either work distantly or they are deployed to locate and mitigate the threat and then get out.[24]

---

[23] Beyond the Build How the Component Commands Support the U.S. Cyber Command Vision. The U.S. Cyber Command Combined Action Group. Joint Force Quarterly, 80, 1st Quarter 2016. NDU Press. https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643106/beyond-the-build-how-the-component-commands-support-the-us-cyber-command-vision/ (downloaded 15 May 2019)
Here's How DoD Organizes Its Cyber Warriors; Mark POMERLEAU, Fifth Domain, July 25, 2017. https://www.fifthdomain.com/workforce/career/2017/07/25/heres-how-dod-organizes-its-cyber-warriors/ (downloaded 15 May 2019)

[24] Here's How DoD Organizes Its Cyber Warriors. Mark Pomerleau, Fifth Domain, July 25, 2017.

Each service cyber component focuses on configuring and operating the security of its service-specific networks, but JFHQ-DODIN has to ensure the unity of effort for the operation and defense of the entire DOD information environment. This is an enterprise-wide effort in which the components work in collaboration with their parent Services, USCYBERCOM, JFHQ-DODIN, the DISA, and the NSA. The Service cyber components function at the operational and tactical levels of this domain and rely on JFHQ-DODIN to ensure lateral coordination, information sharing, and synchronization. The director of DISA is dual-hatted as the commander of JFHQ-DODIN. Services retain 24 CPTs, but the 6 DODIN CPTs report directly to JFHQ-DODIN and typically implement DODIN operations mission. JFHQ-DODIN is also responsible for threat information sharing. Before 2010, information regarding the attack of a service might be shared with other interagency partners, but there was no joint mechanism to alert the rest of the vast force of DOD network operators to a new threat.

Active Service Component	Total CMF Teams	Cyber National Mission Force	Cyber Combat Mission Force	Cyber Defense
Army	41	7	14	20
Marine Corps	13	1	4	8
Navy	40	7	13	20
Air Force	39	6	13	20
Coast Guard	1	0	0	1
Total	134	21	42	69

Figure 4. Service Contributions to CFM[25]

Cyber Operations Classification[26]

Cyberspace operations (CO) are categorized as offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), or DODIN operations:

- The DODIN operations mission includes operational actions taken to secure, configure, operate, extend, maintain, and sustain DOD cyberspace and to create and preserve the confidentiality, availability, and integrity of the DODIN. These are network focused / threat agnostic.
- DCO missions are executed to defend the DODIN, or other DOD cyberspace forces have been ordered to defend, from active threats in cyberspace. These are mission focused and threat specific. DCO operations have three subcategories:

[25] Source: Jeffrey L. CATON: Implications of Service Cyberspace Component Commands for Army Cyberspace Operations. Strategic Studies Institute and U.S. Army War College Press. February 2019. p. 49. Edited by the author.

[26] This categorization is based on: Cyberspace Operations. Joint Publication J-P 3-12. June 2018. p. II-2 – II-6.

a) Defensive Cyberspace Operations-Internal Defensive Measures, where authorized defense actions occur within the defended network or portion of cyberspace.

b) Defensive Cyberspace Operations-Response Actions are the form of DCO mission where actions are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected.

c) Defense of Non-DOD Cyberspace. Military cyberspace forces prepare to defend any US or other blue cyberspace when ordered. DOD operations rely on many non-DOD segments of cyberspace, including private sector and mission partner networks.

- OCO are missions intended to project power in and through foreign cyberspace. All CO missions conducted outside of blue cyberspace with a commander's intent other than to defend blue cyberspace from an ongoing or imminent cyberspace threat are OCO missions.

Integrating Cyberspace Operations into Joint Operational Planning

Combatant commands have almost half of the CMF assigned to support them that is 20 CPTs under their direct command. Another 44 teams are commanded by the 4 service Joint Force Headquarters – Cyber (JFHQ-Cs). The four services provide the Combat Mission Forces in support of the Combatant Commands through their JFHQ-Cs. The assignment of combatant commands to JFHQ-C is as follows:

- JFHQ-C MARFORCYBER (Marines): U.S. Special Operations Command;
- JFHQ-C ARCYBER (Army): U.S. Northern Command, U.S. Central Command, and U.S. Africa Command;
- JFHQ-C FLTCYBER (Navy): U.S. Pacific Command and U.S. Southern Command;
- JFHQ-C AFCYBER (Air Force): U.S. European Command, U.S. Strategic Command, and U.S. Transportation Command.[27]

[27] Army Support of Military Cyberspace Operations (2015) op. cit. p. 50.

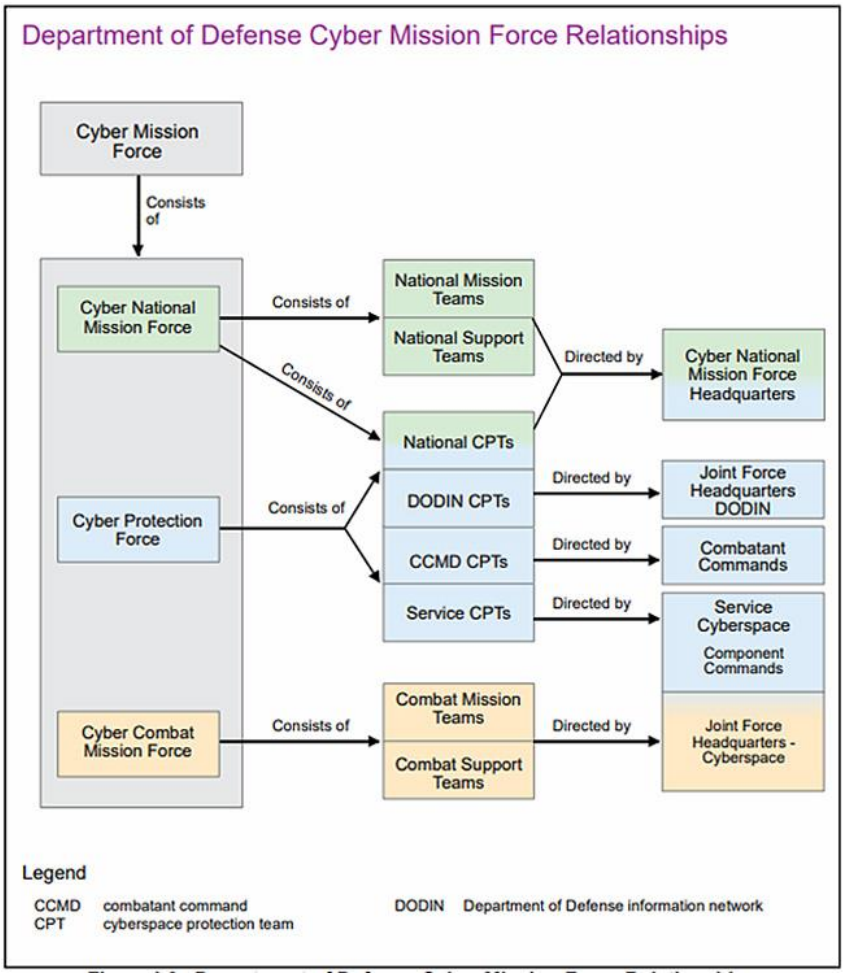


Figure 5. DoD CMF Command Structure[28]

Joint forces by design may each contain CMF teams from more than one service component. Cyber teams from across the services work through the Joint Force Headquarters-Cyber. Each service has its own JFHQ – C which are dual hatted with given service commander. These provide a connective tissue with Cyber Command as well as with the Combatant Commands, as discussed above. In addition to overseeing CMTs and CSTs, these units also provide planning, targeting, intelligence and cyber capabilities to various combatant commands. In 2017, Pentagon leaders tasked the service commands with creating permanent planning cells within the various combatant commands. These cells, known as cyber operations-integrated planning elements (CO-IPEs), include small staffs to help better coordinate and deconflict offensive and defensive cyber operations by a reach-back element in the JFHQ-C, and also by liaising with other cyber-related entities including allies. Increasingly complex task as multiple friendly forces – such as globally focused

[28] Cyberspace Operations. Joint Publication J-P 3-12. June 2018. p. I-10.

defensive cyber teams, teams focused on protecting the homeland abroad or teams from other combatant commands – could potentially bump into each other in cyberspace.[29] CO-IPEs are expected to be fully operational by 2022.

These planners are not operators, and they exist within joint intelligence, operations, plans and development – respectively known as J2, J3, J5 and J7. This system is almost identical to that of the U.S. Special Operations Command at each combatant command, said Bill Leigher, director of DoD cyber programs at Raytheon.[30] According to experts, the significance of this new structure lies in the fact that commanders have access to cyber planners 24/7 and thus can familiarize themselves in-depth with this new capability, involving cyber planners right from the beginning of traditional military operations.[31] *"Just like air, land, sea and maritime power projections, what we're working with the combatant commands to do is project power in, from and through cyber, integrate it in their battle plans so it's timing and tempo is set by the commanders in the field based on the scheme of maneuver that they have on the ground,"* Maj. Gen. Christopher Weggeman, commander of 24th Air Force/Air Forces Cyber, said in 2017.[32] Therefore, CO-IPEs are envisioned as an important tool for seamlessly incorporating cyber operations into traditional operational planning, as well as being an instructive instrument changing the commanders' mindset transforming what was previously a reactive, maintenance-based planning approach to a more operationally focused strategy, plans, and execution process.[33]

The axis of the service JFHQ-Cs plays a major role in cross-service command and control, intelligence, planning, targeting and force co-ordination of CMF in Combatant Commands. By 2013, CYBERCOM has defined the mission essential tasks and the certification criteria for the service JFHQs.[34] In addition to C2, JFHQs: exercise SIGINT authorities and Intelligence oversight; plan and direct Cyber ISR (intelligence, surveillance, reconnaissance), Cyber OPE (operational preparation of the environment) Cyber Attack and – when directed – Cyber Defense actions; coordinate, integrate, synchronize CO with other JFHQ-C, NMF-HQ operating in the same networks, at the tactical level, to maximize operational effectiveness; conduct intelligence operations; coordinate JFHQ-C support functions for attached and for co-

---

29 What the Pentagon learned from Cyber Lightning 2019. Mark Pomerleau. Fifth Domain. July 5 2019.

30 Cyber Command stands up planning cells at combatant commands. Mark Pomerleau. Fifth Domain, October 11, 2017. https://www.c4isrnet.com/show-reporter/ausa/2017/10/11/cyber-command-stands-up-planning-cells-at-combatant-commands/ (downloaded 15 May 2019)

31 Ibid. Cyber is being normalized with traditional military operations. Mark Pomerleau. Fifth Domain. September 14, 2017

32 Cyber is being normalized with traditional military operations. Mark Pomerleau. Fifth Domain, September 14, 2017.

33 Beyond the Build How the Component Commands Support the U.S. Cyber Command Vision. The U.S. Cyber Command Combined Action Group.

34 Preparing for Computer Network Operations: USCYBERCOM Documents Trace Path to Operational Cyber Force. National Security Archive. George Washington University. https://nsarchive.gwu.edu/news/cyber-vault/2019-05-03/preparing-computer-network-operations-uscybercom-documents-trace-path-operational-cyber-force (downloaded 15 May 2019)

located CMF with USCC, NSA, service and functional components; direct CMF training, exercise, and readiness requirements.[35]

Conclusion

USCYBERCOM kept and built largely on the preceding organizations and mechanism. The interim goals of putting in place the envisioned cyber forces and the institutional and physical infrastructure supporting them have been fulfilled as well. Its long-term mission to ensure the unity of effort through information sharing, standardization, synchronization and interoperability, and to enable combatant and service commanders to use cyber capabilities as integral mission components is still in the making. Offensive cyberspace operations at strategic and operational level still remain in the remit of Cyber Command due to the high demand of resources and the high level of risk. The US's path with the largest military capabilities and with its immense defense economics cannot be set to follow for Hungary. Still, the pattern of capability components, the structural framework and the connections between them might provide some useful lessons worth considering.

Bibliography:

- Keith ALEXANDER: Warfighting in Cyberspace; Joint Force Quarterly, Issue 46, 3rd Quarter 2007.
- ARKIN, William: The Cyber Bomb in Yugoslavia; Washington Post, October 25, 1999. Cited in Addressing Cyber Instability. Edited by Dr. James C. Mulvenon and Dr. Gregory J. Rattray. Cyber Conflict Studies Association, US. 2012.
- Beyond the Build. How the Component Commands Support the U.S. Cyber Command Vision. The U.S. Cyber Command Combined Action Group. Joint Force Quarterly, 80, 1st Quarter 2016. NDU Press. https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643106/beyond-the-build-how-the-component-commands-support-the-us-cyber-command-vision/. (downloaded 15 May 2019)
- CATON, Jeffrey L.: Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications. Strategic Studies Institute and U.S. Army War College Press. January 2015.
- CATON, Jeffrey L.: Implications of Service Cyberspace Component Commands for Army Cyberspace Operations. Strategic Studies Institute and U.S. Army War College Press. February 2019.
- Cyberspace Operations. Joint Publication J-P 3-12. Joint Staff. Department of Defence. June 2018.

[35] USCYBERCOM, "JFHQ-C Certification: Framework to Operationalize the JFHQ". Preparing for Computer Network Operations: USCYBERCOM Documents Trace Path to Operational Cyber Force. National Security Archive. George Washington University.

- Defence Cybersecurity. DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened. US Government Accountability Office. August, 2017.
- Defence Department Cyber Efforts: DoD Faces Challenge in its Cyber Activities," Report GAO-11-75, Washington, DC: U.S. Government Accountability Office, July 2011, p. 18.
- Department of Defense NetOps Strategic Vision; https://dodcio.defense.gov/Portals/0/ Documents/DIEA/DoD_NetOps_Strategic_Vision.pdf (downloaded 15 May 2019)
- Department of Defence, Quadrennial Defence Review 2014, Washington DC: U.S. Government Printing Office, March 4, 2014.
- DOD Training U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force. US Government Accountability Office. March, 2019.
- Future Warfare. Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations. US Government Accountability Office. August, 2019.
- HUNT, Edward: US Government Computer Penetration Programs and the Implications for Cyberwar. IEEE Annals of the History of Computing, Volume 34, Number 3, July-September, 2012, pp. 4-21.
- Joint Task Force – Computer Network Operations. Fact File. US Strategic Command. 2003. http://www.iwar.org.uk/iwar/resources/JIOC/computer-network-operations.htm (downloaded 15 May 2019)
- POMERLEAU, Mark: What the Pentagon learned from Cyber Lightning 2019. Fifth Domain. July 5 2019. https://www.fifthdomain.com/dod/cybercom/2019/07/05/what-the-pentagon-learned-from-cyber-lightning-2019 (downloaded 15 May 2019)
- Cyber Command stands up planning cells at combatant commands. Fifth Domain, October 11, 2017. https://www.c4isrnet.com/show-reporter/ausa/2017/10/11/cyber-command-stands-up-planning-cells-at-combatant-commands/. (downloaded 15 May 2019)
- Cyber is being normalized with traditional military operations. Fifth Domain. September 14, 2017.
- Here's How DoD Organizes Its Cyber Warriors. Fifth Domain, July 25, 2017. https://www.fifthdomain.com/workforce/career/2017/07/25/heres-how-dod-organizes-its-cyber-warriors/ (downloaded 15 May 2019)
- Preparing for Computer Network Operations: USCYBERCOM Documents Trace Path to Operational Cyber Force. National Security Archive. George Washington University. https://nsarchive.gwu.edu/news/cyber-vault/2019-05-03/preparing-computer-network-operations-uscybercom-documents-trace-path-operational-cyber-force. (downloaded 15 May 2019)

- U.S. Cyber Command (USCYBERCOM). Factsheet from U.S. Strategic Command. 2010. http://www.stratcom.mil/Portals/8/Documents/CYBERCOM_Fact_Sheet.pdf. (downloaded 15 May 2019)

SÁNDOR BABOS

MILITARY CULTURES IN THE LIGHT OF HYBRID WARFARE

Abstract

Hybrid warfare is one of the most intensively researched fields of military science today, and interest in it by other disciplines, such as political and legal science, has also become apparent through studies published so far.

Nonetheless, in the military science approach to hybrid warfare, it can be stated that it has not yet been fully explored and the research methods and specifics of the discipline have not been fully exploited.

Of these shortcomings, the examination of hybrid warfare was conducted with regard to basic research in the reference framework of military cultures partly with the purpose of initiating an academic discussion and partly to fill in a gap.

***Keywords*:** hybrid warfare, military culture, military science

Hybrid warfare is a topical issue in today's military science - and in many cases other disciplines[1] -that has been intensively engaging the scientific community since the beginning of the Ukrainian conflict. At the same time, however, it should be noted that many aspects of hybrid warfare have not as yet been subject to research.[2] In terms of the field of military science, it is at the forefront of hybrid warfare research in terms of the number of works published but has not yet carried out specialized analysis in its own field that would be necessary to plan practical implementation - a specific action - against hybrid warfare. At the same time, however, it is essential that we first identify theoretically the characteristics of hybrid warfare that determine the range of manoeuvre, given the characteristics of the aggressor.[3]

The limits of a hybrid warfare party's activity can be examined from several perspectives[4] , but a fundamental analysis from the perspective of military science can

1 For example, in political science, HOFFMAN, Frank G. (2007): Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies, Arlington; from the point of view of law, Ádám FARKAS: From the Total State to the Total War to Total Defence. MTA Law Working Papers 2015/34., Budapest

2 Such as the international legal judgment of hybrid warfare in the light of human rights, or the economic security aspects of foreign influence in the preparation of the hybrid war, etc.

3 It is readily apparent that a state with a major position, a third country in economic difficulties, or an international civil society organization with a solid financial background have other options for the use of means and methods classified as hybrid warfare.

4 E.g. economic, IT, government support, geographical location, etc.

be made by comparing each military culture[5], and what aspects of this mode of warfare may be in the non-military (civil) sphere.[6] Due to the above described reasons, in this phase of theoretical research of hybrid warfare it is appropriate to first review what the options of the different military culture[7] are, taking into account the specificities of this warfare in preparing and carrying it out. However, it is not possible to examine this without defining hybrid warfare within the scope of this writing, as it currently has no generally accepted definition, either internationally or within military science.

About hybrid warfare

While the use of the term ' hybrid warfare' is becoming more commonplace in our daily lives, we cannot, from a scientific point of view, state that there is a commonly accepted definition in the international literature. In several works[8] we can find definitions that cover the content of this activity, but they are too practical in terms of the exploration of military cultures within the framework of this dissertation. Because of our active publication and development work on and due to our membership in NATO[9], I find it appropriate to use the definition of the NATO Parliamentary Assembly – most notably the definition of the term in the political and security science sense[10] – that "*hybrid warfare is an asymmetric tactic that uses non-military means (e.g. political and economic intimidation and manipulation) and seeks to detect and exploit weaknesses, backed by the threat generated by conventional and non-conventional military means."*

At the same time, however, it is important to emphasize that, according to traditional military science, asymmetric tactics are used by the weaker party in in terms of military power. All this in the case of hybrid warfare, by its very nature, is reversed and used by the stronger party. The reason for the use of asymmetric tactics in the traditional sense was precisely the scarce resources available, but in the case of hybrid warfare, the aggressor's priority is to cover the activity in a sense that it cannot be linked to it in any way.[11] At the same time, however, keeping the conflict below

---

5 The topic of military cultures in writing KOVÁCS, Jenő (1995): Hungarian military strategy (complex research topic). Theoretical research area. II. R., is processed on the basis of the Hungarian Academy of Sciences' National Excellence in Social Science Research Grant Application, Budapest

6 Can some of the means and methods of hybrid warfare be used by civilian, extremist, and terrorist organizations against states or alliances, and if so, to what extent does this fall within the field of military science?

7 Material-centric, movement-centric, guerrilla

8 HOFFMAN (2007) op. cit.; RESPERGER, István: Crisis Management and Hybrid Warfare. Dialóg Campus Publisher, Budapest, 2018

9 Over the past five years, NATO and the Parliamentary Assembly have published a number of reports that have served as a reference for the scientific works I have processed, including the overwhelming majority of the wording of the hybrid warfare that is being described.

10 NATO Parliamentary Assembly Defence and Security Committee: Hybrid Warfare: NATO's New Strategic Challange? General Report [166 DSC 15 E bis], 2015, paragraph 12, https://www.nato-pa.int/document/2015-166-dsc-15-e-bis-hybrid-warfare-calha-report (downloaded: 06. 05. 2019.)

11 MARTON, Péter: Conditions of the occurrence of hybrid warfare. Nation and Security 2018/3., Budapest, p. 96.

the level of war is of paramount importance, as the aggressive state's requirement of keeping international crisis management operations away from the country of destination is a basic requirement.[12] It should be noted, however, that the causes of traditional asymmetry appear to be that, while the aggressor may be said to be stronger overall, the country under pressure still has fewer resources than the (governmental) forces operating on the domestic base.

The reason for this is that special operations units appearing in the hybrid warfare system are up to a few thousand, while the defence and law enforcement forces of the target country are many times superior, and they obviously have better local knowledge, relations and in some cases popular support than the aggressor.

In our classic military science, war is the continuation of politics by other (violent, military) means in order to force our opponent to carry out our own will.[13] In the case of hybrid warfare / war, we can adapt the above statement, since the military leadership assigned to achieve the policy objectives also uses non-military means to perform its task, so we can say that *hybrid warfare is the continuation of warfare by other (non-military) means.* As (Ret.) Maj. Gen. Ferenc Réczey, who annotated Clausewitz's cited work, puts it[14] *"... war is none other than the continuation of politics with violent means and subordinated to this, depending on the intensity of the political relations, it is sometimes more, sometimes less than «war»."* Accordingly, the military forces and non-military assets are used alternately or in parallel.

The wide range of these 'other (non-military) assets', which generally include all the means and methods available to the state, and otherwise the fact that they are constantly used (though not specifically for the purpose of pursuing a coordinated hybrid warfare) means *that, at the moment, every state is engaged in hybrid warfare against almost every other state in the world.* Of course, we must not accept this in a literal sense, but rather as a factor to be taken into account, since the activities of states , such as the continuous intelligence with regard to countries of interest, endeavour to shape economic processes in their favour, or even political and financial support for entities that identify with their values and share their interests, are areas in which they have extensive experience. In the context of a possible hybrid warfare activity, the conduct of these activities is not only conceivable, but is also necessary when concrete implementation takes place.

Overall, the novelty of hybrid warfare is not that it introduces new means or methods, as it is just one form of state warfare, and as with other forms, it relies on the full range of state power tools, since every war has such non-military means application that influenced its course.

The novelty of hybrid warfare lies in the fact that military and non-military assets *are* deployed in a *coordinated manner* and are *controlled by designated military command.* Today's military science focuses on the analysis of the operations of the

---

12 RESPERGER (2018) op. cit. p. 21.

13 CLAUSEWITZ, Carl von: On War. I-II. Vol. Zrínyi Publishing House, Budapest, 2014.

14 CLAUSEWITZ, Carl von: On War. Volume I. Zrínyi Publishing House, Budapest, page 8. Translated and annotated by Major General RÉCZEY, Ferenc (Ret.) (1961)

Russian Federation in connection with the events in Ukraine[15], and it should be noted that although its investigation is timely, it does not fully satisfy the research of the theoretical bases stated in this paper. With regard to the ' Russian hybrid warfare', it should also be noted that although many scholars, such as Mark Galeotti , mentioned above, or the national literature, András Rácz[16] clearly identify the works of Army General Gerasimov as according to which the Arab Spring was the a result of the intervention in the domestic affairs of the target by Western countries and the logic behind it is that the Russian Federation also has the right to engage in similar activities, with many questioning it and appraising it for providing post factum explanations[17], or even for misunderstanding the concept of the United States as a major threat[18]. In addition to these contradictions, however, research into hybrid warfare in the aftermath of the Ukrainian conflict has produced military science findings that can be used to investigate it and the responses given to it[19].

Concerning the events in Ukraine, István Simicskó[20] explains that while Western military science identifies them as ' Russian hybrid warfare' and, for its articles and lectures[21] , attributes its development to Army General Valery Gerasimov, a military

---

15 The 2014 events in Ukraine and " Gerasimov placed first scientific presentation of see parallels between doctrine ‘. GALEOTTI, Mark (2014): The' Gerasimov Doctrine 'and Russian Non-Linear War. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ (downloaded: 08/05/2018.)

16 RÁCZ, András (2014): The Hybrid War of Russia in Ukraine. Foreign Trade and Foreign Affairs Institute for Studies 2014/1, Foreign Affairs and Foreign Trade Institute, Budapest. https://www.academia.edu/8833545/Oroszorsz%C3%A1g_hibrid_h%C3%A1bor%C3%BAja_Ukrajn%C3%A1ban_Russias_Hybrid_War_in_Ukraine_ (downloaded: 08. 05. 2019.)

17 MCDERMOTT, Roger N. (2016): Does Russia Have a Gerasimov 's Doctrine? In : US ArmyWar College: Parameters (Spring 2016) https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ pp 97-105 (downloaded: 08. 05. 2019.)

18 BARTLES, Charles K. (2016): Getting Gerasimov Right. https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art009.pdf , In: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January- February-2016 / , pp. 30-38., (downloaded: 08. 05. 2019.)

19 It should be noted, however, that in addition to disguising the hybrid warfare on the part of the aggressor, we must also consider the response, which is of paramount importance in the phase of hybrid warfare when the aggrieved party is already identified. is looking for supporters in the international community and can't afford to take the biggest possible loss. This is especially true when law enforcement and possibly defence organizations have to be deployed against foreign fighters or even their own rioting populations.

20 SIMICSKÓ, István: History and current issues of hybrid warfare. Military Science 2017/3-4., Budapest, pp. 6-7.

21 GERASIMOV, Valery (2013): Tsennost nauki v previdenii./The value of science lies in foresight. Vojennij Promislennij Kurjer No. 8. (476), https://www.vpk-news.ru/articles/14632 (downloaded: 08. 05. 2019.)
Army General Gerasimov’s further writings on the subjectt: Пути активации инновационной деятельности в оборонной промышленности и Вооруженных Силах Российской Федерации./Main trends in the activation of innovations in the activities of the defence industry and the Armed Forces of the Russian Federation. Vestnik – Journal of the Russian Military Academy, No.1. (42) 2013. http://www.avnrf.ru/index.php/zhurnal-qvoennyj-vestnikq/arkhivnomerov/534-vestnik-avn-1-2013 (downloaded: 08. 05. 2019.); Будущее закладывается сегодня./The future is

dictionary in the author's possession, the activity is identifiable as 'strategic deterrence': "*…strategic deterrence is a coordinated system of military and non-military means (political, diplomatic, legal, economic, ideological, scientific-technical) aimed at deterring a military action against Russia that would inflict strategic damage."*

With regard to the definition of ' hybrid warfare' by the NATO Parliamentary Assembly and ' strategic deterrence' in the Russian military terminology dictionary, there is indeed agreement on the use of non-military assets, the exemplary listing of which does not correspond precisely, but in practice both refer to the use of a wide range of means available to the State. The essential difference is that while the definition of hybrid warfare does not include its aims, it can be stated that in the case of strategic deterrence it was given a precise description *"... to deter a military action against Russia, which would cause strategic damage"* In connection with the Ukrainian conflict in relation to this goal of Russian foreign, security and defence policy[22] it acquires meaning along the sense that NATO's priority, but any other international organization-wide expansion effort (i.e. military action) – especially in the directly adjacent states – particularly serious violation of national interests, if they are military. On this basis, it can be seen, if not clearly demonstrated, that Ukraine's previous accession aspirations and the situation following the events on Majdan Square violated the interests of the Russian Federation in addressing them by introducing a strategic deterrence - practically applying the Gerasimov conflict model - was necessary on the basis of the Russian strategic documents in force.

In this sense, while Moscow is defensive in the ideology of its alleged activities in Ukraine, it is nevertheless an intervention in the internal affairs of another state that illustrates one of the main features of Russian movement-centric military culture, the priority of attack over defence.

War Cultures[23] in the light of hybrid warfare

The observation and writing of the differences in the means and methods employed in waging war in relation to individual peoples and ethnic groups dates back to the Renaissance and early Modern Age, whose emergence is considered to be the "first sprout" of military culture.[24] In the words of Jenő Kovács, a prominent Hungarian researcher of the topic, military culture: *"…is the sum of military, intellectual and material values affecting warfare, which represents the basic direction of dismantling enemy forces and preserving their own troops. Military culture can be called the orientation (stream) of military science, the character of the army, but also differently."*[25] In his research, Jenő Kovács came to the conclusion that

based on the present. Vojennij Promislennij Kurjer No .10. (478), 2013. https://vpk-news.ru/articles/14865 (downloaded: 08. 05. 2019.)

22 Presidential Decree No 683 of 31 December 2015 on the National Security Strategy of the Russian Federation

23 KOVÁCS, Jenő (1995): Hungary's military strategy (complex research topic). Theoretical research area. II. R., based on the National Grant for Social Sciences Research Grant, Budapest

24 FORGÁCS, Balázs (2017): Military Theory – The History of Hungarian Military Thinking and Military Cultures. Based on Dialóg Campus Publishing House, Budapest, page 24.

25 KOVÁCS (1995) op. cit. p. 17.

depending on their culture and socialization, individual leaders, peoples, countries organize and lead their forces. show differences in their application and capabilities. The nature and structure of the armed forces, the country's defence system, the structure of state and military leadership, the nature of military service, military complement and military training, mobilization and supply, standards of conduct against the enemy, and conscious and emotional motives associated with the army are determined by the beliefs, prejudices, insights, beliefs, customs and beliefs of the community and the leader, which are thus embodied in military culture. At the same time, according to Jenő Kovács, these differences of forces can be grouped into three subdivisions, thus defining the framework of three basic military cultures: movement-centric, material-centric, guerrilla, between which the dividing line is deeper and embodied in national strategies (security, military).[26]

Motion-centric war culture

Considering the military culture of our country in the 20th century, it can be stated that until the 1990s, following the Russian-Soviet military theory, it was one of the movement-centric military cultures whose method was the complete destruction of the enemy through vigorously attack and seizing its territories by deploying the army service branch, given the geographic features of our country. Defence played the role of auxiliary tactic in military thinking, aimed at re-establishing the conditions in the event of an attack. This idea can also be found in the German idea of the "Blitzkrieg" or lightning war, where defence is unnecessarily bad, and in the Russian-Soviet theories[27], which regarded defence as a combat mode forced upon us by the enemy. According to Jenő Kovács, these military schools are variants of each other, which considered offensive as the main mode of waging war[28] and it was particularly typical of states with a land army. It should be noted in particular that each *expressed a close idea of politics and military* because of the similarities in their objectives. In my opinion, in their case, Clausewitz's mentality takes the form that this military culture *regarded the armed forces as the primary means of achieving political ends.*

Today, of the great powers we can classify Russia as one of the movement centric military cultures which - as has been seen - regards NATO's expansion efforts as a threat, inter alia, and it follows from its doctrines described above that it interferes *offensively* in the events in Ukraine to prevent detriment to its interests. Hypothetically it could be shown that if it had not done so, it could have created a situation in which its neighbour is a NATO member, and consequently, following from its own strategy, would have damaged its national interests, it would have been forced to assume a defensive stance which were undesirable and even avoidable based on its own military

---

[26] It should be noted, however, that the boundaries of the military cultures being described are now blurred by scientific research, and that, depending on the change in the purpose of politics, the military is forced to use the methods of other military cultures, cf. FORGÁCS Balázs (2009): Today's War Cultures (Theory and Evolution of Warfare in the Modern Age). PhD Dissertation, Miklós Zrínyi National Defence University, Kossuth Lajos Faculty of Military Doctoral School, Budapest, Chapter 5.

[27] The main difference between the German and Russian-Soviet military theory is that the Lightning War conceptualized the simultaneous, rapid, and according to the Russians, the long-lasting strikes to destroy the enemy and seize his territories.

[28] Author's note: So far as Clausewitz's duality of war is concerned, the aim is not to exhaust but to destroy the enemy.

culture, so it ought to have striven after creating conditions for an offensive, but it does not have the conditions for an open war with NATO in the foreseeable future, so it would be in a paradox that it cannot resolve. It follows from the above - since Russia did not undertake a traditional war with Ukraine -, it had to assert its interests with the means of hybrid warfare.

In connection with the events in Ukraine it can be said that are reflected inside the Soviet-Russian movement centric features of military culture, which due to the hybrid nature of warfare is not present in the majority of military assets for the purposes of[29]:

- the exploration and exploitation of the weak points of the enemy: the presence of a majority ethnic Russian a referendum on secession of areas
- demoralization of the enemy through fast -paced attacks achieving success after success, unleashing protests in support of extremist and criminal groups, annexation of areas reducing the combat strength, fighting spirit and morale of the Ukrainian armed forces and law enforcement agencies
- penetration into the depths of the enemy, retaining territories, forcing their will on the enemy, seizing initiative: it was characteristic of military force mainly in the areas already annexed to it, but the entire territory of the Ukrainian state was seized by means of secret services,
- acquiring a "time advantage": postponing intervention and deployment of observers in international fora by continually denying involvement, engaging in various "ceasefire" talks, which, however, lead to a consolidation of the aggressor's position.

Material-centric military culture

Analysing the beginning of the review of this military culture for the first time from the point of view of our country, it can be said that the approach of our accession to NATO arose the need to change our movement- centred approach in order to promote proper integration. Prior to the change of regime, the military (offensive) main directions lost their legitimacy, and given that we had no enemy image, we resolved to develop circular defence, and then to contribute to and rely on collective defence within the Alliance system.

In my opinion, although the transition to this approach and the long-term introduction of material-centric warfare culture within the *Alliance system* – with strong support and joint operations only with our partners – are feasible, we are capable of undertaking tasks commensurate with our role until we have a collective defence mechanism in place – we are currently neither capable of preparing for the fatigue of a material-centric war culture[30] nor of creating the conditions for a movement-centric war culture. In my opinion, in such a situation, the warfare culture of the guerrilla warfare to be described below should be prepared for warfare with the

[29] It should be noted, however, that movement-centric military culture is not fundamentally characterized by the use of non-military means, since its purpose is to destroy the enemy by seizing the territories which it seeks to achieve by the rapid and destructive application of military force.

[30] With regard to the Clausewitz duality of war, the aim is not to destroy the enemy, but to exhaust it and break its will in this way.

support of the population until the Alliance's defence mechanism comes into effect, and so should national defence plans be prepared accordingly.

In international terms, countries representing material-centric warfare - typically the Anglo-Saxon naval powers, e.g. the United States of America - achieves its military objectives by striking high-value destructive assets, for which it is essential to build the appropriate military infrastructure. In their case, the basic mode of warfare is defence, which aims not to create the conditions for an attack against a movement-centric military culture, but to defeat an attack based on (military) dominance. Non-military assets can play an important role in this war culture in the conventional sense of (open) warfare, as the exhausting nature of warfare provides ample time for economic pressure, appropriately designed propaganda and influence, and systematic and devastating diversified activities. to continue. Quoting Clausewitz and putting the ideas of material- centric war culture on the footing of theory of warfare: „*... defence has a negative purpose: retention, and attack has a positive one: conquest, since the latter multiplies its combat equipment, but the former does not, therefore we must say that the form of defence of the military leadership is, in itself, stronger than the offensive form."*[31] All these ideas also mean, and this military culture states, that there is a greater chance of destroying the enemy while defending, though , in addition, the survivability of own forces is enhanced although limited, they can gain an advantage over an attacking party.

The material-centric military culture thus considers defence to be the fundamental mode of combat activities and retention of the areas to be the key security requirement and uses offensive as a means to impede enemy movement, in order to take strategic facilities. Its purpose is therefore to thwart the enemy's successes.

The nature of military culture requires that, even in peacetime, not only its military strength, but also its other non-military resources, be carefully and systematically prepared for warfare, the success of which depends on the careful distribution of resources. As seen above, the plan is the "soul" of a material-centric military culture, which includes possible activity variants as well as the distribution of resources with clockwork precision This kind of rigidity poses a major threat to the unexpected success of a movement-centric offensive or the unpredictability of a war against guerrilla warfare, as we have seen in the Vietnam War or in Afghanistan. These weaknesses of material-centric warfare culture today are trying to eliminate this weakness by combining, where appropriate, the rules with decentralized leadership, delegating decision-making authority to lower levels, combined with the benefits of motion-centric warfare.

The following description by Jenő Kovács in relation to the Gulf War well illustrates the thoughtfulness and coherence of material-centric war culture: "The US military command desisted from taking possession of territories offered by military conditions. It did not penetrate Iraq, nor did it break down the forces of aggression. Conversely, citing the residual threat that this caused, they could deploy their military forces in the area and thus exercise military control over the countries of the oil-rich areas. Presumably, this common idea of political and military purpose will shape the American military strategy in the future. The main features of this strategy are military

[31] CLAUSEWITZ (2014) op. cit. Book Six, Chapter One, Item 2.

dominance, limited attack, influence/coercion/local war in the scale and circumstances. "In my opinion, all of these key features of the American strategy are capable of providing a rapid transition to non-military assets. switching to warfare, since limited (and possibly disguised) attacks, the politically determined end of the Gulf War (economic) target and close military base, local conflict and military supremacy can all be considered as part of hybrid warfare.

Summarizing material- centric military culture from the perspective of hybrid warfare it can be stated that the parallel use of non-military means has followed it throughout history. The novelty can only be experienced in leadership, since, contrary to what has been seen before, when non-military assets are deployed as politically determined, in the case of hybrid warfare, coordination of these assets can take place within the designated military staff.

The military culture of guerrilla warfare

By its very nature, guerrilla warfare does not have the general characteristics of movement-centric and material-centric military culture. In terms of methods, intensity, and its set of equipment, it is most similar to hybrid warfare, although asymmetry is here expressed in the traditional sense, as it is pursued by irregular groups with scantier or fewer resources than the enemy, usually existing or oppressive foreign powers. What distinguishes guerrilla warfare from hybrid warfare is that it is neither necessary nor desirable to cover the acts that have been carried out here, since the support of the population and, in some cases, the winning over of the international community can only be achieved by openly committing their actions, and they have to prove towards both the population and the international community that this group would be able to govern the country.

As regards irregular guerrilla warfare troops, it should be noted that, unlike terrorist organizations, they fall within the scope of the Hague[32] and Geneva[33] Conventions, and are therefore actors of war recognized by international law. Of course, this also implies that the activity should not, for these reasons, include acts contrary to the rules of general international law, which must remain within the limits of generally acceptable violence. For this reason, the guerrilla warfare, when appropriately grouped in its resources, is continually employing non-military means (e.g. propaganda, aiding the general public, influencing the Internet, strike, demonstration, etc.) whose objectives are supported, and in this sense armed struggle and violence only plays a complementary role. Generally speaking, during the use of guerrilla warfare, armed struggle may be intermittent, or may be interrupted for longer periods.

From a military point of view, the prerequisite for continuing the guerrilla warfare is the establishment of a secure military base either domestically or abroad[34], which contributes to the training and relaxation of forces and provides an appropriate assembly area for the operations.

---

32 The Hague Convention (1899) II. Chapter IV of the Hague Convention (1907) chapter
33 Geneva Convention (1949) II. protocol
34 KOVÁCS (1995) op. cit. p 40.

The strategic objective of guerrilla operations is to exert pressure on the opposing power, its hinterland[35], or its forces, which contributes to their disintegration, exhaustion[36] and the establishment[37] of an appropriate bargaining position[38]. For all these reasons, the main feature of combat-level guerrilla activity is the application of surprise and rapid course, which, when consistently observed, causes a series of actions to confuse the opposing party. Over time, decentralized deployment of the initial smaller subunits in guerrilla warfare has been replaced by increasingly organized strike measurement, centralized command and control. Given that guerrilla activity is aimed at achieving a political goal, it is not surprising that guerrilla troops generally turn out to be committing violent (military) acts when transformed into parties. Facilitating the transformation into a party can also be a goal for the opposing party, especially if it fails to win over the population and can only put an end to the guerrilla troops by cutting off recruits and support.

Regardless of the events in the conflict in Ukraine, troops deployed in the eastern regions were apparently engaged in guerrilla warfare[39], but these units were part of a regular force, and their command was centralized, which is unthinkable for real guerrilla troops. the party would have already been transformed into a party that would have given up fighting.

Based on the above, the use of guerrilla warfare by troops[40] can therefore be classified as guerrilla military culture, but it should be noted that they differ in their operational environment, opposing party, current level of organization, etc. On the other hand, it is precisely because of these essential factors that we cannot speak of a guerrilla military culture. Guerrilla warfare in each country depends more on opportunities than on historical cultural roots.

Summary, conclusions

In the hybrid warfare model, the aggressor's activity can be described as one that includes the offensive-centric approach of motion-centric military culture, the activities based on asymmetric resource allocation of material-centred military culture, furthermore the exhaustion activity of some guerrilla (or at least designated as guerrilla) troops, as well as further typical means of the various military cultures. All of these may emerge in such a way that one particular military culture may employ methods taken over from the other two military cultures, as seen by the aggressor in Ukraine, whose *primary military culture* is alien to the use of non-military assets

35 Such were the consequences of the guerrilla warfare used during the Vietnam War.
36 Such as the tactics of Mao Zedong.
37 2016 peace agreement between the Colombian government and the FARC left-wing guerrilla organization.
38 With regard to the Clausewitz duality of war, the aim of the guerrilla warfare is to render the enemy fatigued and thus break his will, and the destruction plays a secondary role.
39 The conditions for this were given: the supportive action of the population, the political aim (secession) against the "oppressive" (Ukrainian majority) power, the existence of a foreign military base.
40 Some of which are irregular as troops recognised by the Geneva and the Hague Convention and as such fall within the scope of martial law.

(resource dominance - material-centric) method of obtaining local support from the populace (guerrilla).

Based on the above, the examination of military cultures for hybrid warfare, in my opinion, supports the conclusion that some movement-centric, material-centric and guerrilla warfare entities (countries, irregular troops) still carry the main features of military cultures today, but consider their application as a tool.[41] On the basis of all these, it can be said that military cultures nowadays, mainly by the great powers, show increased *flexibility* compared to pre-modern times.

With regard to the smaller countries, especially the states of the post-Soviet region, it can be stated that although they possess the most characteristic features of a military culture, they are not able to fully implement it in practice. In the case of our country, the requirement to move from a movement-centric to a material-centric military culture before NATO accession was dissonant, as the high- resource-intensive exhaustion activity associated with it would be limited due to its inability to perform independently. For these reasons, I consider it necessary to further explore military cultures with particular regard to the political environment, economic opportunities, and parallel examination of alliance affiliation.

With respect to military cultures, it may be necessary to consider assigning a *primary military culture* to each country to determine their degree of *flexibility in the* light of these considerations.

With regard to hybrid warfare, it has been stated that its novelty lies not in the use of military and non-military means, but in the manner in which they are used. During these warfare, alternating use of military and non-military assets under military command and control ensures effective pursuit of political objectives, while making it difficult for the affected country to win over the international community and public opinion. Military power itself is mostly designed to support non-military assets through the ever-sustained threat.

Bibliography:

- The Hague Convention of 1899.
- The Hague Convention of 1907.
- Supplementary Protocol to the Geneva Conventions, signed on 12 August 1949 (Protocol II).
- BALOGH, Fatime – FEKETE, Csanád – NÉMETH, András – NÉMETH, József Lajos: Hybrid warfare with particular focus on mobile communications. Military Engineer, Volume X, Issue 4, Budapest, 2015

[41] FORGÁCS, Balázs (2017): War Theory – The History of Hungarian Military Thinking and War Cultures. Dialóg Campus Publisher, Budapest, pp. 79-87.

- BARTLES, Charles K.: Getting Gerasimov Right. 2/27/2016, https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art009.pdf , In: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition - Archives / January-February-2016 / (downloaded 08. 05. 2019.)
- CLAUSEWITZ, Carl von: On War. Vol. I-II, Zrínyi Publisher, Budapest, 2014. ISBN: 9789633275993.
- CLAUSEWITZ, Carl von: On war. Volume I. Zrínyi Publishing House, Budapest, 1961. Translated and annotated by Major General (Ret.) RÉCZEY, Ferenc
- FARKAS, Ádám: From the total state through the total war to total defence. MTA Law Working Papers 2015/34., Budapest, 2015.
- FORGÁCS, Balázs: War Theory - The History of Hungarian Military Thinking and War Cultures. Dialóg Campus Publisher, Budapest, 2017.
- FOGÁCS, Balázs: Today's War Cultures (Theory and Evolution of Warfare in the Modern Age). PhD Dissertation, Miklós Zrínyi National Defence University Lajos Kossuth Faculty of Military Doctoral School, Budapest, 2009.
- GALEOTTI, Mark: The ' Gerasimov Doctrine' and Russian Non-Linear War. 06.06.2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ (downloaded 08. 05. 2019.)
- GERASIMOV, Valery: Tsennost nauki v previdenii. VPK, 2013. https://www.vpk-news.ru/articles/14632 (downloaded 08. 05. 2019.)
- GERASIMOV, Valery: Пути активации инновационной деятельности в оборонной промышленности и Вооруженных Силах Российской Федерации. / Main trends in the activation of innovations in the activities of the defence industry and the Armed Forces of the Russian Federation. Vestnik - Journal of the Russian Military Academy, No. 1 (42), 2013, http://www.avnrf.ru/index.php/zhurnal-qvoennyj-vestnikq/arkhivnomerov/534-vestnik-avn-1-2013 (downloaded 08. 05. 2019.)
- GERASIMOV, Valery: Будущее закладывается сегодня. (The future is based on the present.) Vojennij Promislennij Kurjer No. 10. (478), 2013., https://vpk-news.ru/articles/14865 (downloaded 08. 05. 2019.)
- HOFFMAN, Frank G.: Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies, Arlington, 2007.
- KOVÁCS, Jenő: Hungarian military strategy (complex research topic). Theoretical research area. II. R., Grant Application for National Research in Social Sciences, Budapest, 1995.
- MARTON, Péter: On the Conditions of Hybrid Warfare. Nation and Security 2018/3 issue, Budapest, 2018
- MCDERMOTT, Roger N.: Does Russia have a Gerasimov 's Doctrine? In: US ArmyWar College: Parameters (Spring 2016) https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ (downloaded 08. 05. 2019.)

- NATO Parliamentary Assembly Defence and Security Committee: Hybrid Warfare: NATO's New Strategic Challange? General Report [166 DSC 15 E bis], 2015. https://www.nato-pa.int/document/2015-166-dsc-15-e-bis-hybrid-warfare-calha-report (downloaded 08. 05. 2019.)
- PORKOLÁB, Imre: Hybrid warfare: a new form of warfare or an old acquaintance? Military Science 3/4/15 Issue, Budapest, 2015
- RÁCZ, András: Russia's Hybrid War in Ukraine. Foreign Trade and Foreign Affairs Institute for Studies 2014/1., Foreign Affairs and Foreign Trade Institute, Budapest, 2014, https://www.academia.edu/8833545/Oroszorsz%C3%A1g_hibrid_h%C3%A1bor%C3%BAja_Ukrajn%C3%A1ban_Russias_Hybrid_War_in_Ukraine (downloaded 08. 05. 2019.)
- RESPERGER, István: Crisis management and hybrid warfare. Dialóg Campus Publisher, Budapest, 2018.
- SIMICSKÓ, István: History and current issues of hybrid warfare. Military Science 2017/3-4., Budapest, 2017

ÉVA BEKE

TRENDS IN CYBER-ATTACKS, WITH SPECIAL FOCUS ON HEALTH CARE[1]

Abstract

With the arrival of Industry 4.0 data, the cyber and critical infrastructure protection became an even more important responsibility. Considering the interconnection of devices – able to carry out terrorist and cyber-attacks, besides traditional threats, such as industrial accident, sabotage or environmental hazard –, cyber-attacks would affect directly and indirectly national security, economy, and health care, and also would ripple through our everyday life. Critical Infrastructure protection, their continuous and reliable operations, their governance and maintenance are of utmost importance to all governments around the globe. It requires policies, priorities, and a balanced strategic planning. This paper focuses on the recent cyber-attacks and trends to raise awareness, how to protect critical facilities and the most valuable data: our personal and medical records. For research method, I have used content analysis, desktop research and secondary data analysis.

Keywords: data breach, critical infrastructure, health institutions' safety, cyber attacks

1. Introduction

This new digitalized and interconnected system rapidly revolutionized the products and services in the manufacturing, the transport, as much as in the pharmaceutical & biotechnology or in the military sector. In the financial sector, there has appeared a new type of payment method: crypto currency. All these technological advances – at the same time – brought the greatest challenge to protect our facilities, territory and data, whether they are real, cyber or virtual. The term "cyber-attack" covers a wide variety of actions, ranging from simple probes, to defacing websites, to denial of service, to espionage and destruction. Similarly, the term cyber war is used very loosely for a wide range of behaviors. In the virtual world, actors are diverse, sometimes anonymous, physical distance is immaterial, and offense is often cheap. Because the Internet was designed for easing the use rather than ensuring security, so the offense currently has the advantage over the defense. This might not remain the case in the long term as technology evolves, including efforts at "reengineering" some systems for greater security, but presently vulnerabilities causing the biggest concern.

[1] SUPPORTED BY THE ÚNKP-19-OE-RH,1415/38 2019 NEW NATIONAL EXCELLENCE PROGRAM OF THE MINISTRY FOR INNOVATION AND TECHNOLOGY.

Governments – within the EU – are looking into particular software-related issues regarding the mobile connectivity; interpersonal communications services (ICS), supervisory control and data acquisition (SCADA), smart infrastructures and the Internet of Things (IoT). They take an approach, which would include not only the technical, organizational, regulatory dimensions, but also the policy-making of NIS. (Network and Information Security). To regulate and organize the protection of cyber and critical infrastructure ENISA (European Union Agency for Cybersecurity) has been establishing a guideline for all member states, which would include, but not limited to

- „Promote network and information security (NIS) as an EU policy priority";
- „Support Europe in maintaining state-of-the-art network and information-security capacities".

The necessity of this established framework is mandatory because of the dependence on complex cyber systems. These structures support military, health and economic activities on regular basis and create new vulnerabilities in smaller or larger states that can be exploited by non-state actors.

Four decades ago, the Pentagon created the Internet, and today, by most accounts, the United States remains the leading country in both its military and societal use. At the same time, however, because of greater dependence on networked computers and communication, the United States is more vulnerable to attacks than many other countries, and in this content, the cyber domain has become a major source of insecurity.

2. Trends in attacks

The most recent larger attacks show that protecting critical infrastructure facilities from physical and cyber-attacks should be taken into serious measure. The very first recorded and published event happened in 2012 in Saudi Arabia where the oil and gas sector has been attacked. It took almost two weeks to reestablish the system's safety again. Followed by the German Still Mill's attack in 2015, a year later Europe-wide multiple energy companies have been compromised, while in 2017 Ireland's Electricity Supply Board was attacked.

Nowadays attacks considered mainstream cyberattacks. While 2017 admittedly has been the year of ransomware, where the attackers gained access to files and/or devices and blocked their real owner – or in the cases of larger organizations owners – to access them, unless they paid the demanded ransom in cryptocurrency. Although the trend has changed, there are still many sectors suffering from previous attacks, such as medical devices and institutions, where the medically used machines' clinical performance and functionality had been seriously compromised.

2018 can be characterized the year of cryptojacking or cryptomining, a clear shift from ransomware. These are new terms and are referring to an act where the attacker's program uses the victim's computer to mine cryptocurrencies, without the victim's consent. The change in the attacks can be explained by the facts that cryptojacking is simpler, due to the low barrier entry and a less disruptive way to make money. Although Bitcoin is the most known crypto currency, many alternatives have been

developed such as Monero, Zcash or Ethereum. They have an elevated level of transaction anonymity compared to Bitcoin, so it is much easier for cyber criminals "to fly under radar" in most cases.

In critical infrastructure, crypto mining attack was identified first in February 2018, in a water utility connected to the internet. This is not a unique attack – as the graph shows (Figure 1) – they are on the rise, since they attracted limited law enforcement attention from the beginning.

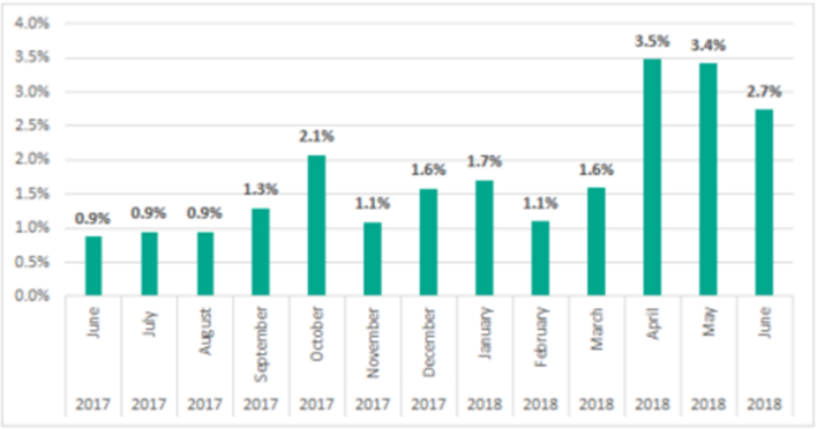


Figure 1. Share of ICS computers attacked by cryptomining malware[2]

During the first half of 2018, cryptominers have affected 42% of the organizations, globally compared to 20.5% at the end of 2017.

The five most notable cryptojacking threats are: Coinhive432 (30%), Cryptoloot460 (23%), Jsecoin461 (17%), XMRig423 (7%) and Authedmine462 (6%), which out XMRig423 is a file-based cryptominer, while all others are browser-based.

Cyber espionage is also becoming popular amongst nations or organizations. *"This threat typically targets industrial sectors, critical and strategic infrastructures across the world including government entities, railways, telecommunication providers, energy companies, hospitals and bank. Cyberespionage focuses on driving geopolitics, stealing state and trade secrets, intellectual property rights and proprietary information in strategic fields."*[3]

---

2 Source: https://securelist.com/threat-landscape-for-industrial-automation-systems-in-h1-2018/87913/ (downloaded 8 November 2019)

3 ENISA Threat Landscape report 2018 15 Top Cyberthreats and Trends, Final version 1.0 Etl 2018, January 2019

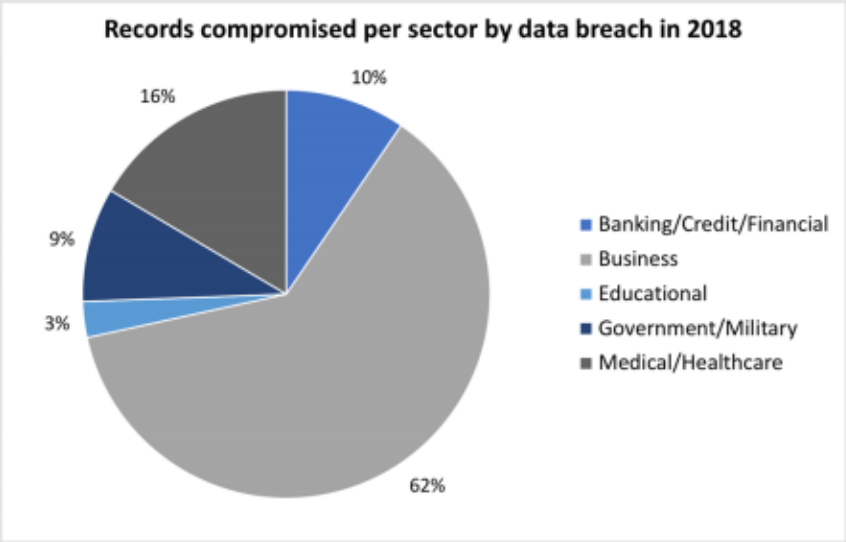


Figure 2. Records compromised by data breach in 2018, per sector[4]

3. Health care revolution

"Health care 4.0" is also here, because of basic data on molecular structure, physical and chemical properties becomes available for digitally transformed systems. Personalized medicines are showing the latest trends to cure illnesses. Future drugs will depend on our body's characteristics, such as fat, muscle weight, bone mass and on the DNA structure, so the treatment of rare diseases can be successfully treated. The time required to approve medicines will be accelerated, thanks to the digital transformation. Artificial intelligence and sensor driven systems bring positive changes to most areas of health, where data information and advanced molecular studies together drive the scientific research. Digital conversion opens the possibility to 3D print medicines, genetic re-design, portable devices, and individualized hormone therapy. In the event of an outbreak of epidemics, it will be possible to detect it in a very short time before it is affecting larger masses.

4. Health care institutions' vulnerabilities

Health care institutions are bound to be expanded from being the providers of the most necessities to use cloud computing, Internet of Things and consequent interconnectedness along with artificial intelligence and virtual reality, as Industry 4.0 brought a fundamentally different approach to this sector. This huge amount of stored data requires a well-implemented security system too, since the risks of data security increase naturally, not only in the field of research, where results already achieved, but also in the personal patient data management.

[4] Source: Ibid.

Avoiding misuse of these data is one of the major tasks in critical infrastructure protection. Security forces have changed in the last 6-8 years, from physical protection forces to cyber security personnel. Data sources available from individuals can easily be combined with financial accounts and other personal information (habits, addresses, workplace etc.), so their protection cannot be compromised. The acceptance of digital technologies and the explosive growth of connected devices have paved the way for new forms of data theft. The attack motivation does not need to have any special intent, computer warfare or even retaliation against a particular person. The strongest motivation of health care attacks is the financial value of information.

Health care has the highest per capita cost. The average rate of data breaches in the health care organization extremely high due to losing litigation and compensation cases. The number of crimes in the medical identity thefts also grows because the stolen medical identities make it possible for the criminals not only to get an accurate picture of the patient information, but can mislead future employers as well. Data breach and fraud are a complex problem that has cost the United States Government alone over $6, 40 billion in 2019.

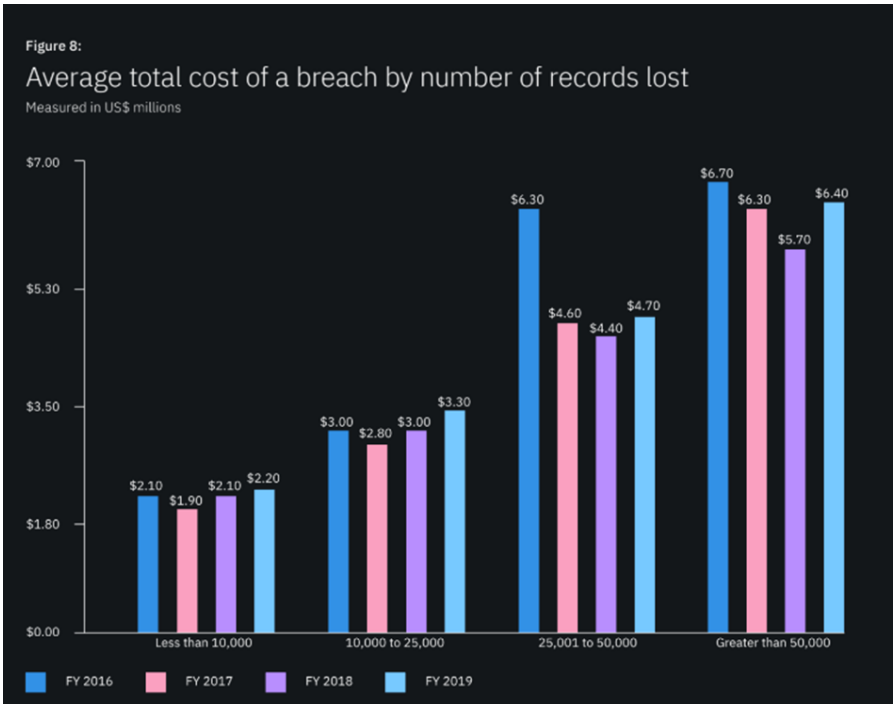


Figure 3. Data breach statistics from 2016–2019[5]

[5] Source: https://www.bluefin.com/bluefin-news/highlights-ibm-security-ponemon-institutes-2019-cost-data-breach-study/ (downloaded 8 November 2019)

Based on the findings of the Ponemon report of 2019, there was a 130% increase in data breaches between 2006 and 2019. The lifecycle of a data breach and the recovery time from it is longer than in any previous years. Malicious attacks were the most expensive root cause of the breaches with 51%, while system glitch caused by 25% and human error 24% of them. The cost of the average data breach in healthcare is 65% higher than in any other industry.

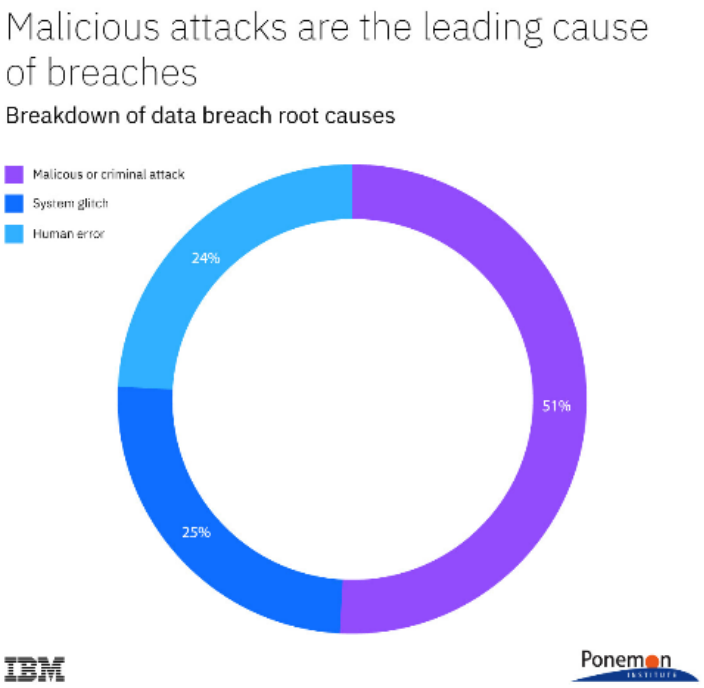


Figure 4. Statistical breakdown of data breach root causes[6]

5. Most recent attacks on health care institutions and what is behind

As the above diagrams and statistical analysis show (Figure 4.), the health care is the second of the most vulnerable entities amongst the critical infrastructures. There are several reasons for this susceptibility.

- The first is the value of healthcare data, which became a "black market currency". (Patient's health information could worth around $1000, so a large-scale attack could sum up to millions.) However, after an attack not only personal information, but also healthcare services and intellectual property assets (such as research phases) can be compromised, which could easily lead to the ruined reputation of the provider.

[6] Source: https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/ (downloaded 8 November 2019)

- Most healthcare institutions are rather spending on buying new devices and advanced pharmaceutical or surgical equipment than spending on ensuring security. Because of this misplaced attention and oblivion of the latest technology and IT security updates, the attackers have a fairly easy access to patients' data.
- The health sector is one of the most rapidly advancing fields, so their interconnected, systems with portable and wearable devices can be another reason for targeting them, since the hacking of an entry point can paralyze the entire system.
- Lack of financial sources to hire cybersecurity professionals, and to develop IT infrastructure for medical purposes can be more important than allocating money for security measure.

There is below a table, showing (Figure 5) some of the most known attacks in recent years, – although this is not an exhaustive list – , the volume of the attacks and their variables are alarmingly high.

METHOD	DATE	PLACE	LOCATION	DAMAGE
Ransomware	2016	Hollywood Presbiterian	Los Angeles	crippled the entire system, the hospital paid $17.000 crypto currency
Wannacry	2017		worldwide	attacked in 99 countries, 230.000 computers and demanded ransom in 28 languages
Malware	2017	Lucas Hospital	Neuss, Germany	blocked access to hard drives, operations were cancelled, data were hand recorded
Human Error	2018	Blue Cross	Philadelphia	an employee posted a file with 17.000 patients medical info
Phising	2018	Catawba Valley Medical Center	Minnesota	stolen health insurance cases, SS# and medical data of 21.000 patients
Data Breach	2018	Medicare, Medicaid	US nationwide	75.000 individuals enrollments have been compromised
Ransomware	2018	Hawaii Fetal Diagnostic Institute	Hawaii	48.000 patients records were stolen

Third party vendor error	2018	Orlando Orthopedic Center	Orlando	19.000 patients data have been posted
Misconfigured FTP server	2018	MedEvolve	Arkansas	205.000 record exposed
Malware	2018	St. Peters Hospital	New York	134.512 records were hacked
Ransomware	2019	Quest Diagnostic	US nationwide	7.7 million consumers data were exposed
Phising	2019	Montpellier Medical Center	Montpellier	infected more than 600 computers
Espionage	2019	US nationwide		stolen medical records were on sale on the Dark Web
Hacking	2019	Ramsay Health Services	Marseille	planned for a computer blackout for 120 hospitals

Figure 5. Author own edit – Cyber-attacks on health institutions

6. Biotechnology in the military

While new biomedical and technological developments are intended to improve efficiency and a quality of life, there is the potential for these technologies to be employed for sinister purposes, such as biological weapons. ***Biosensors*** are for detecting any harmful substance or material in the air, land or water and giving signals to soldiers. The direction of the research is to develop an entire biosensor system that can release an antidote or activate a protective mask. ***Biomaterials*** are organic materials that are compatible with the human body and its tissues. They have been developed to heal wounds, repair bones, and self-replicate. ***Microbiome*** is a bacterium that regulates our digestive track and provides digestive and mental health. If synthetic biology is able to develop a microbiome, it will have dual effects: by using it to enhance health in the army mentally and at the digestive system – both of them are important for warfighters – then it will have pharmaceutical benefits as well. However, by modifying or reengineering its structure can have adverse effects on the human body and a potential treats. Same rule applies to novel biological resins that are both lightweight and flame retardant. It could be easily incorporated into making lighter drones, building lighter airframes, or fortifying ship hulls. Biotechnology is one of the most versatile, exciting, and innovative technologies of the 21st century – but its benefits for defense have yet to be fully explored or realized. Governments should coordinate a strategic prioritization of its biotechnology needs, and communicate them clearly to the biotechnology and synthetic biology community. More innovative approaches to acquiring these capabilities could bring the tools of biotechnology into the hands of every warfighter.

Conclusions

Protection should always focus on vulnerabilities of one or in most cases more than one facilities or sectors. Because of the interdependences, an actual attack on one sector might have adverse effects on others. When implementing a protection plan, it should contain a clear guidance for the people and/or team involved. Assigning responsibility at all levels not only locally but also regionally, would be also a recommended step to be able to receive help as fast as possible when it is needed. Healthcare Infrastructure protection should be collaborative, with an improved IT security system. The assigned group should monitor and constantly evaluate the data of such institutions and all connected devices, in order to have a safe and uninterrupted service.

Institutions should develop a risk assessment methodology that allows for a correlated collection of data, enabling the institutions to identify the risk as accurately as possible. In order to develop effective prevention and rapid response systems in the area of health care cybersecurity, it is necessary to develop a connected operational management.

The medical and technological advancement can bring different kind of challenges to deal with. While the scientific research in the pharmaceutical industry is rather progressive, their risk in the form of biological weapons for military use cannot be ignored. Once these discoveries are being used or are put in practice, they can call for real security measure. Therefore, the ethical issues as well as the safety and security responsibility and the relevant policy-making and framework call for a rather prompt and effective action.

Bibliography:

- AHMED M. – BARKAT ULLAH A.S.S.M.: (2018) False Data Injection Attacks in Healthcare. In: BOO Y. – STIRLING D. – CHI L. – LIU L. – ONG K. L. – WILLIAMS G. (eds): Data Mining; AusDM 2017. Communications in Computer and Information Science, vol 845. Springer, Singapore
- ALCARAZ C. – ZEADALLY S., Critical infrastructure protection: Requirements and challenges for the 21st century, International Journal of Critical Infrastructure Protection 8, 53-66, 2015, https://www.sciencedirect.com/science/article/pii/S1874548214000791 (downloaded 8 November 2019)
- BANERJEE A. – VENKATASUBRAMANIAN K.K. – MUKHERJEE T. – KUMAR S. – GUPTA S.: Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber–Physical Systems Proceedings of the IEEE 100, 1, 2012 https://ieeexplore.ieee.org/document/6061910/ (downloaded 8 November 2019)

- BEKE É.: Industry 4.0 and its risks in the state administration, corporate and medical sectors National security review: periodical of the military national security service 2018/1. pp. 98-110, http://www.knbsz.gov.hu/hu/letoltes/szsz/2018_1_NSR.pdf (downloaded 8 November 2019)
- DI DOGARU – I DUMITRACHE: Cyber-physical systems in healthcare networks. In: 2015 E-Health and Bioengineering DOI: 10.1109/EHB.2015.7391368
- EDWARDS M., Critical Infrastructure Protection, Proceedings of the NATO Advanced Research Workshop on Critical Infrastructure Protection 2012, https://www.iospress.nl/book/critical-infrastructure-protection/ (downloaded 8 November 2019)
- ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends, Final version 1.0 Etl 2018, January 2019
- E. V. VASILIEVA: Developing the Creative Abilities and Competencies of Future Digital Professionals Nauchno-Tekhnicheskaya Informatsiya, Seriya 2: Informatsionnye Protsessy i Sistemy, 2018, No. 10, pp. 1–10. https://link.springer.com/article/10.3103/S0005105518050060 (downloaded 8 November 2019)
- HOKSTAD P – UTNE IB – VATN J: Risk and interdependencies in critical infrastructures Springer-Verlag London, 2012 DOI: 10.1007/978-1-4471-4661-2 https://www.springer.com/gp/book/9781447146605 (downloaded 8 November 2019)
- HORVÁTH T., Elektronikus megfigyelő-, és ellenőrző rendszerek objektumorientált kialakítása különös tekintettel a biztonsági kockázatok rendszerére PhD Thesis, 2017 https://bdi.uni-obuda.hu/sites/default/files/Doktori-(PhD)-ertekezes---Horvath-Tamas_2.pdf (downloaded 8 November 2019)
- JUNGERT E. a,n, Hallberg N. a,b, Wadströmer N.: A system design for surveillance systems protecting critical infrastructures Journal of Visual Languages and Computing 25, 2014. pp. 650–657, https://www.sciencedirect.com/science/article/pii/S1045926X14001001 (downloaded 8 November 2019)
- KOTZANIKOLAOU P. – THEOHARIDOU M. – GRITZALIS D: Interdependencies between critical infrastructures: Analyzing the risk of cascading effects in International Workshop on Critical Information Infrastructures Security CRITIS: Critical Information Infrastructure Security 104-115, 2011, https://link.springer.com/chapter/10.1007/978-3-642-41476-3_9 (downloaded 8 November 2019)
- KINROSS, J.: Cybersecurity and healthcare: how safe are we? BMJ 2017; 358 doi: https://doi.org/10.1136/bmj.j3179 (Published 06 July 2017) BMJ 2017;358:j3179

- MBOWE J. E. – OREKU G.S., Critical Infrastructure Protection, The International Conference on Digital Security and Forensics 2014, https://www.researchgate.net/publication/263617477_Critical_Infrastructure_Protection (downloaded 8 November 2019)
- Presidential Directive 7 of the United States of America. https://www.dhs.gov/homeland-security-presidential-directive-7 (downloaded 8 November 2019)
- RADVANOVSKY R.S – MCDOUGALL A: Critical infrastructure homeland security and emergency preparedness Taylor and Francis, Boca Raton, 2016 https://www.crcpress.com › Homeland Security › Disaster Planning & Recovery
- SETOLA R: Critical Infrastructures, Protection and Resilience (2016) https://www. springer.com/chapter/10.1007/978-3-319-51043-9_1 (downloaded 8 November 2019)
- STANKOVIC, John A.: Research Directions for Cyber Physical Systems in Wireless and Mobile Healthcare In: ACM Transactions on Cyber-Physical Systems – Inaugural Issue archive Volume 1 Issue 1, February 2017 https://doi.org/10.1145/2899006 (downloaded 8 November 2019)
- STERGIOPOULOS G. – KOTZANIKOLAOU P. – THEOCHARIDO M. – GRITZALIS D: Risk mitigation strategies for critical infrastructures based on graph centrality analysis in International Journal of Critical Infrastructure Protection 10, 34-44, 2015, https://www.sciencedirect.com/science/article/pii/S1874548215000414 (downloaded 8 November 2019)
- ZHANG W. – WANG N.: Resilience-based risk mitigation for road networksStructural Safety, Elsevier 62, 57-65, 2016, https://www.sciencedirect.com/science/article/pii/S0167473016300170 (downloaded 8 November 2019)
- YUSTA J.M. – Correa G.J. – LACAL-ARANTEGUI R.: Methodologies and applications for critical infrastructure protection: State-of-the-art – Energy Policy, Elsevier 39, (10), 6100-6119 2011, https://www.sciencedirect.com/science/article/pii/S0301421511005337 (downloaded 8 November 2019)
- WRIGHT, A. – AARON, S. – BATES, D.W.: J GEN INTERN MED (2016) 31: 1115. https://doi.org/10.1007/s11606-016-3741-z (downloaded 8 November 2019)
- https://www.stormshield.com/top-5-cyberattacks-against-the-health-care-industry/ (downloaded 4 November 2019)
- https://securityintelligence.com/series/2019-cost-of-a-data-breach-report/ (downloaded 8 November 2019)
- https://www.ibm.com/security/data-breach (downloaded 8 November 2019)
- https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF (downloaded 4 November 2019)

- https://mkogy.jogtar.hu/jogszabaly?docid=99600037.TV – (downloaded 28 December 2018)
- https://mkogy.jogtar.hu/jogszabaly?docid=99900074.TV – (downloaded 2 November 2019)
- http://www.kozlonyok.hu/kozlonyok/Kozlonyok/10/PDF/2008/31.pdf (downloaded 2 November 2019)

LÁSZLÓ SIMON – SÁNDOR MAGYAR PhD

THE THREATENING INFORMATION ENVIRONMENT AND TERRORISM

Abstract

The authors approach the general system-wide vision in the cyberspace of the terrorists' point of view. Terrorists are attacking the security of individuals in a new dimension. During their armed struggle, like guerrillas, they place information in the center of their operations, to which today's advances in information technology contribute. According to the media, information and communication can be both lethal and non-lethal weapons in the terrorists' fighting tactics.

Keywords: terrorism, cyberattack, information environment, information and network-centric warfare

Introduction

In the second half of the 20th century, the world's technical environment underwent revolutionary changes. Information and digital knowledge have become the focus of attention and has moved to the forefront of innovative industrial development. The long-known and well-controlled safety environment has completely changed. The implementation of digital technology with social, political, economic, social and, last but not least, military benefits has resulted in the development of information and communication networks that can affect not only technical systems but also human relationships.[1] In postmodern societies,[2] a new, idyllic (free, happy, and peaceful) image of people's coexistence is born. Globalization and the complexity of personal relationships and electronic systems simultaneously promised people the hope that information can be accessed on time, in accordance with their needs, even without limitation. This revolution, short in terms of technology, has built information societies by the 21st century.

The role of the Internet as a media shaping awareness and decision-making is growing. It can be the source of the rapid spread of online news, the news hunting of

[1] László SIMON: Information as a weapon? In: Professional Review 2016 pp. 34-60.

[2] At the end of the 19th century, American thinkers came to realize that politics should be interpreted not only within a nation-state framework, but also within a global context. In social theory, it was stated that politics cannot be interfering in people's lives. The postmodern (following the modern) approach to politics must become a servant and a facilitator. Jean-François Lyotard in his work entitled "La condition postmoderne" and published in 1979 used the concept for the first time when he analyzed the possibilities of social theory that appeared after the late industrial i (post-industrial) society and pluralistic democracy analyzed. In: János BOROS: Jean-François Lyotard, The Thinker of Diversity, An Attempt at an Approach to Knowledge Theory. Present Age: Literary and Art Magazine, XLII. EFV. No. 3 1999. pp. 298-306.

various Internet news portals, and even of intimidation, all at the same time. There is a growing opportunity of influencing the reader, the user, the Internet users, but also the system of artificial, automated, robotic or, as a collective term, "smart" services that are connected to the fulfillment of a wide range of human needs. In many cases, competition for news coverage and increased consumption results in a lack of verification or fact-checking. While consumer protection in the physical and financial dimensions of the traditional economy is consistently secured through decades of experience through government and non-governmental organizations, the influence of online communities and individual users ranges from "cuteness" all the way to a call for self-destruction.

Threats appearing in the information environment

The average user of the Internet identifies threatening pieces of information capable of influencing individuals and public opinion with the so-called the fake news (hoaxes). In the "virtual arsenal", these can cause effects similar to those of explosives. Influencing on the Internet[3] is already present in the electoral systems of countries, more and more news[4] of which is published. However, proving these activities is a difficult, often impossible task. From a legal point of view, it is difficult to identify the existence of the threat itself. Code-based information flowing through a virtual or info communication device system cannot become harmful if it is not connected to its physical dimension. Simply put, no one can become a "victim" without genuine user engagement and active involvement. Identifying fears arising from the indirect cognitive effects of information and assessing them as criminal acts presents and a new challenge in a new dimension that everyone has agreed to describe as cyberspace.

One of the peculiarities of cyberspace is that its users and their communities (criminals, spies, adulterers, religious communities, etc.), and also the terrorist organizations knowingly presenting the biggest threat use hidden communication, information sharing. Detection is extremely difficult, but it is not just a technical process. Information flowing through The physical equipment and information in the logical operations security vs. safety[5] has created a new paradox. The control of the technical transfer of data goes beyond the existing system of conventional voice recognition and interception. In the area of defense, thinking needs to be expanded to include Internet-based voice communication, encrypted channels, steganography, and various chat options, which can even take place on the message boards of multiplayer online games. The classic, point-to-point (including telephone conversations) information exchange identifiable in terms of technology has been pushed into the background in the conduct of the various forms of communications, their real and virtual elements cannot be clearly identified. An emotional sign (emoticon) or an

[3] László KOVÁCS – Csaba KRASZNAY: "For Theirs is the Power": The Impact of the Internet on Politics in the US Presidential Election 2016, Nation and Security 2017/3. pp. 3-15.

[4] MTI: Russian daily shows how US elections were affected; https://sg.hu/articles/it-tech/127765/orosz-napilap-mutatta-be-hogyan-befolyasoltak-az-amerikai-valasztasokat (downloaded 18 October 2017)
Macedonian youth influenced fund raising campaigns for children who were already dead.

[5] The Hungarian language uses the same word for safety and security – /Translator's note/

image can induce a different effect on the user (receiver) when posted as a message on the Internet. It should be emphasized here that the identification of the source (transmitter) with time constraints, as before, is no longer possible or easily possible in cyberspace. Strangely enough, the responsibility lies not only with the individuals producing, communicating and sharing content, but also the unsuspecting individual joining in the communication thread. And the endeavor that so far has been accepted with respect to credible authors, their valid and scientifically well-founded data, is being challenged time after time by new research on human behavior, consciousness, and perception. Higher demand for information control of content providers, the spread of cloud services[6] present a wide range of opportunities in the storage, concealment and even transmission of information to be protected.

Cyberspace has provided, is providing an interface, and perhaps now it can be stated that despite the most careful effort against it, will be providing support to the spread of extremist information, such as completion of personal aggression, in strengthening radicalization, but even recruitment in the case of terrorist organizations. Malevolent groups can propagate their ideology and propaganda videos hidden and open to the public without defining their specific target audience and making them widely available on the World Wide Web. Any reaction from any government or non-government organization seems like tilting at windmills. Although those who cannot identify with development without limits and control, the seemingly unstoppable posting of content portraying aggression make their voices heard in ever more often, they are fighting an uphill legal battle in the process of asserting freedom of opinion. (And a number of young men, influenced by recruitment conducted on the Internet, set off for the training camps of terrorist organizations, and many of them often go through irreversible radicalization.)

The deep WEB or dark WEB, hidden from or less known by crowds of Internet users, providing opportunities for the perpetration of computer crimes of malicious sources and criminal groups and terrorist organizations use it for purposes of illicit arms trafficking, but also for the propagation of a variety of attack techniques - the making of explosive devices, for example. Detection and defense are in reality like a cat-and-mouse game. The “good” side is to follow events, but identifying real people is extremely difficult and costly due to the volume of data traffic passing through the Internet and the use of encryption technologies. The hacker site is capable of testing the tools and technologies available on the market and, once vulnerabilities are discovered, exploit them, which in many cases can be used as "zero-day" vulnerability for months until they are discovered and the protection technology is published.

Based on this, computer and info communication networks available in countries, including Hungary, can be interpreted as a special operational environment. Individuals (groups) engaged in malicious (unlawful) acts appearing in this space are thus to be investigated not only as criminals.

---

[6] Cloud service: access to IT infrastructure owned by someone else that provides us with the information service (e.g. email, storage etc.)

The importance of information operations and their environment in cyberspace

As a consequence of the Information Revolution, classically separable social, natural and technical environments are increasingly overlapping. Approaching and effectively solving modern-day problems requires holistic analysis and evaluation.

In our view, scientific analysis models are primarily intended to enhance in-depth research in a particular discipline. Due to the interdisciplinary approach of the investigations required in certain areas, there may be unintentional contradictions or scientific competition. Science can advance through the rigorous criticism and debate of research results.[7] This is especially true for cyberspace research. The more we want to know about it, the less we can rely on the individual statements of a particular discipline. In our opinion, cyberspace can be both a technical and a social system, but at the same time it can be construed as a virtual environment similar to natural structures, organisms or even one showing laws of nature.

Following this concept, we approached European cyber space in a triple unity chosen by Zsolt Haig.[8] So, the fundamentals of research carried out in the context of the information society and security can be based not only on the operation of the physical devices (hardware) and relations, but also on society and everyday processes and consequences defining life as well. The activities of terrorist groups and terror (aggression) have been interpreted primarily as the combined effect of the processes carried out and mediated in this space. The objectives of terrorist organizations, independent of ideologies and religions, have a political background, directly or indirectly. In terms of targets, they focus primarily on intimidation, fear and creating panic.[9] The forces applied in terms of means and methods, respectively, as we observed them, are endless hate, destruction and chaos. According to the lessons of the 21st century, the armed attacks of terrorism, with limited fighting forces and resources, are aimed primarily at attracting and engaging the population, while attaining information superiority. As a result, the procedures known as "indirect operations" have by now been significantly increased during the armed struggle in the Middle East. These are indirect and cognitive, network-wide communications of any additional information or symbolic value (e.g. hacking, leaks, meme-making, community sharing). The terrorist attacks in the US and in Europe have had specific psychological and informational effects.[10]

For examining operations developed and applied in the military field, those interested may find strategies, doctrines, operational procedures, and other policies. Military science in this field has already responded successfully in the military and,

---

7 BERÉNYI, Dénes: How does a physicist today look at the world?; http://vigilia.com/regihonlap/2010/7/berenyi.html (downloaded 15 September 2017)

8 Zsolt HAIG: Information, Society, Security. NKE Services Ltd., 2015. pp. 93-122.

9 Read more: KIS-BENEDEK, József: Jihadism, Radicalism, Terrorism. Zrínyi Publishing House, 2016. p. 279

10 Read more: László SIMON: Increasing Terrorism in Europe and its Impact on Providing Military Mass Events. In: Professional Review, 2015 No. 2. pp. 145-162.

in many cases, civilian sense, on a number of issues to detect, obstruct, prevent, and combat hostile acts of the adversary with similar information content.[11]

At the NATO Summit in Warsaw on 7 and 8 July 2016, cyber-attacks were also declared a threat to the Alliance's security, which could have the same impact as conventional weapons. Therefore, due to the various military operations, cyberspace, in addition to the potential air, land and sea theaters of operations can already be considered an area of operation.[12] [13] Life is being supported by an increasing number of computer systems, the impact of losing which, especially with regard to critical infrastructures and information infrastructures, is a greater risk for nations.

Knowledge of the field of information operations helps to understand the strategic and local level of the indirect warfare of terrorism. Doctrine of information operations issued by the Hungarian Defense Forces in 2014[14] – NATO AJP-3.10 Doctrine[15] – list the following information operations:

- Psychological Operations (PSYOPS),
- Presence, Posture, Profile (PPP),
- Operational Security (OPSEC),
- Information Security (INFOSEC),
- Deception,
- Electronic Warfare (EW),
- Physical Destruction (PD),
- Key Leaders Engagement (KLE),
- Computer Network Operations (CNO),
- Civil-Military Relations (CIMIC).

Tibor Rózsa, in his doctoral dissertation in 2016, gives a complete overview of the tactical, local applicability of operations, referring to, among other things, the development levels of technology and national forces. He emphasized in his research that the main direction of the development of military use of information is can be completed with the gaining ground of indirect warfare[16] and its use at the strategic

---

11 MUNK, Sándor: Military Scientists and Their Research Areas, Part 1: Empirical Study of Military Science Subdivisions. Military Science, 1-2., pp. 4-16.

12 Theater of War: *"a three-dimensional geographic area in which warring (conflicting) parties concentrate and deploy forces, and conduct war activities on the basis of a unified military concept and plan."... "The development of military technology now makes the separation of theaters of war can extend to the full depth of the countries of the warring parties, as well as to the cosmic space."* József SZABÓ, (ed.): Military Lexicon. Volume 1, p. 472.

13 Now, in Warsaw, we are reaffirming NATO's defensive mandate and recognizing the cyberspace of operations in which NATO must defend itself effectively, on land, and at sea; Warsaw Summit Communiqué, pp. 70-71. http://www.nato.int/cps/en/natohq/official_texts_ 133169.htm#cyber (downloaded 31 July 2017)

14 General/57 Information Operations Doctrine 1st Edition, Hungarian Army Publication, 2014.

15 AJP 3-10. Allied Joint Doctrine for Information Operations pp. 1-3. http://info.publicintelligence .net / NATO-IO.pdf (downloaded: 09 September 2017)

16 Rozsa's dissertation deals only with traditional warfare, although indirect warfare is part of the guerrilla warfare culture. In: Tibor RÓZSA: Possibilities of using information operations in the task system of the Hungarian Defense Forces. NKE Doctoral (PhD)

level: "*In essence, the main objectives of war and the end-state to be achieved can be attained not only through the physical destruction of the targets, but also through strategic effects, including information operations. Consequently, the impact-based approach to operations focuses on achieving the intended end-state and, with this in mind, integrates the planning, implementation and evaluation of operations*."[17]

According to Hungarian military doctrine, during operations related to the "use" of information - for example, NATO, an ad-hoc alliance or (a) particular nation(s) - need to engage in coordinated communication activities also at higher operational levels in accordance with capabilities in order to achieve strategic goals. In the implementation of national tasks, interoperable tools of public diplomacy, media, military and public relations, and cooperation, as well as information and psychological operations, shall be addressed at the strategic communication level.

While conducting hostile actions, posting hostile messages in cyberspace, more and more communities claiming to be made up of jihadist fighters appear among the perpetrators. They act not only on the basis of criminal, individual or group motivation, "to meet their needs," but also as soldiers and warriors. In their case, the solution may be to expand and deepen the techniques used so far in military multinational solutions. Due to the diversity of cultural approaches, this requires an increasingly complex and constantly updated approach. Communication and information activities against offenders of different motives must be coherent in military terms. The participants need to mutually reinforce each other so that the messages they carry are coordinated at all levels (e.g. political, military, strategic, regional, local) and understandable and coherent in the implementation, also for "non-military" participants.[18]

In the complex system of conflict resolution and crisis management of the conflicts related to terrorism, cooperation between military and non-military elements must be established. At the same time, a unified approach to the implementation of interacting tasks requires an increasingly complex information approach and planning. The combatants' environment, the objectives and the target audience can be treated as a unit, as in the case of armed conflicts.

Because of the wide range of related social, technical, or ideological networks of individuals we must deal with not only physical violence, but also with the direct impacts of the information. The geographical and virtual space relationship is a "theater of war" in which the appreciation of the vulnerability of the cognitive domain must be faced. In this special information environment that is around everyone, terrorist organizations are able to demonstrate increasing effectiveness. Due to the complex social, environmental and technical relationships of individuals and the delivery of mediated messages, the previously mentioned influencing information

---

Dissertation 2016, http://hhk.uni-nke.hu/uploads/media_items/rozsa-tibor-ezredes-az-informacios-muveletek-alkalmazasanak-lehetosegei-a-magyar-honvedseg-feladatrendszereben.original.pdf (downloaded 09 September 2017)

17 Ibid. pp. 35-36.

18 General/57 Information Operations Doctrine 1st Edition, Hungarian Defense Forces Publication 2014.

(even as indirect operations[19]) have become network-centric. Attacking and protecting the systems that make up the networks, which has so far been most technically advanced, is augmented by operations that can be conducted in the related cognitive space (Figure 1). Because the operation of networks without their users loses its meaning, the security of individuals now has an added meaning. In this network-based information environment, users as citizens and voters, as well as public and social organizations (e.g. cultural, transport, educational, economic and other networks) that are dominantly involved in their lives, and last but not least, the communities concerned are also decisive symbols.

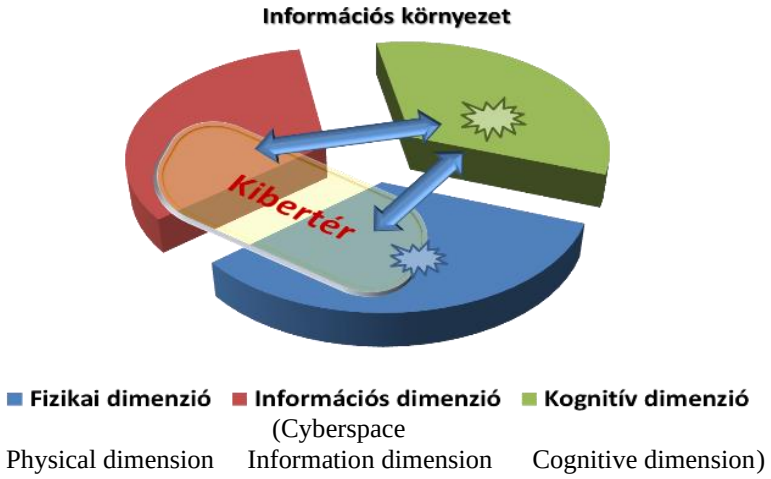


Figure 1: The information environment
(self-edited)

According to the current rational concept, cyberspace consists of its physical and information dimensions. In the information environment, this is complemented by the cognitive dimension. The battle in cyberspace is described in the military interpretation of cyber warfare: The achievement *of cyber* domination as part of information superiority is *"accomplished by cyber warfare within the information warfare."*[20] Interpretation shows that beyond the rational approach, the struggle in cyberspace is not just about destroying physical systems or, in the military sense, destroying enemy targets. In addition to the direct impacts of armed conflict, we believe that there is an abstract, cognitive element that includes the indirect impacts of this conflict. Coordinated attacks on certain elements of society, the economy, education, health care or public services or symbols of the communities, achieve the increase of fears precisely through their indirect impacts. Following what we may interpret as an indirect attack, restoring physical conditions, reviewing or modifying rules, and reorganizing protection (building a new hospital, school, or skyscraper) will no longer completely restore people's sense of security. Terrorism and the fight

[19] László SIMON: Information as a weapon? In: Professional Review 2016 pp. 34-60. ISSN 1785-1181

[20] HAIG (2015) op. cit. pp. 95.

against at this day and age enlarge our experience day after day. Some people become radical and aggressive under the influence of indirect information. There are those who, without direct contact, are killing in the name of ISIS or Al-Qaeda as a terrorist phenomenon. They do this by using airplanes or trucks, which in the traditional sense are not even considered a weapon.

Legal issues in cyberspace

The European Union's cyber security strategy addresses a number of comprehensive issues:

- *"achieving resilience to cyber-attacks;*
- *drastic reduction of cybercrime;*
- *developing cyber defense policy and capabilities for the Common Security and Defense Policy (CSDP);*
- *development of cyber security industrial and technological resources;*
- *developing a coherent international cyber policy for the European Union and promoting its core values."*[21]

Considering the above, the strategy contains only defensive capabilities. The issue of cyberattack is out of the agenda, which is difficult to interpret in the military sense, without action against terrorist and extremist organizations, active intervention and response.

When considering cyberspace operations from a legal point of view, there is no legal definition of support in the form of a pre-emptive attack or active attack. This is because, on the one hand, activities in cyberspace are difficult to prove and, on the other, activities are mainly aimed at preventing, detecting, or preventing damage. Therefore, in the military sense, it is often a question of whether cyber defense can produce defense-friendly results without attack, or whether it is necessary to set up an offensive capability at an organizational level capable of reducing the impact of an attack on systems and possibly neutralizing the attacker.

As stated in the National *Cyber Security Strategy*, Hungary aims to *"have effective prevention, detection, management (reaction), response and recovery capabilities against malicious cyber activities, threats, attacks and emergencies, as well as against unauthorized information leaks affecting the Hungarian cyber space."*[22] Here again, the activities are of a defensive nature, without mentioning active defense.

Incident management centers operate internationally to prevent cyberspace incidents,[23] are responsible for incident handling and official tasks, in addition to providing information and alerts. The role of so-called CERTs will continue to grow

---

21 European Union Cyber Security Strategy http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001 (downloaded 15 September 2017)

22 Government Decree 1139/2013 on the National Cyber Security Strategy of Hungary. (III. 21.) Government Resolution

23 Act L of 2013 on Electronic Information Security of State and Local Government Bodies

in the future as Internet-based technologies, in tandem with the spread of the Internet of Things (IoT).

Non-military offensive intent appears in Act C of 2012 on the Criminal Code in the Chapter on Violation of Information System or Data, which defines the sanction for unauthorized access to the information system by violating or circumventing the technical measure to protect the information system.[24]

Challenges for the military

Cyberspace differs significantly from traditional theatres of war. Presence in cyberspace requires an entirely different level of preparedness than in the army, air force or navy areas. In the case of "cyber warriors", "survival" is least expressed in terms of physical abilities, knowledge of IT, and the specific software and procedures they use are dominant. Completing the physical fitness requirements will screen many candidates suitable for the job and position.

Recruiting highly qualified IT professionals and keeping them in the military arises as a challenge as they can earn their military pay many times over in civilian life and the statutory regulations do not allow an upward deviation of their pay to the level of external pay.

Retention on the job is made more difficult by the fact that continuing training is necessary to maintain in order to achieve adequate efficiency, but it is very costly and further increases the soldier's knowledge of the market. Thus, only the most knowledgeable IT professionals remain within the organization. Appropriate training will ensure that the software is trained in critical security flaws and secure programming.

An example of Estonia is the voluntary cyber defense reserve system[25] can provide a solution to counteract cyber-terrorist operations and take the necessary counter-measures, but this requires a serious planning task. Csaba Krasznai has already summarized the reasons for the creation of the voluntary reserve cyber defense unit in 2011.[26] Cyber-attacks threaten critical information systems just as much as military operations. Targeted attacks can also threaten the peacetime and field systems of the armed forces by cyber groups in terrorist organizations. The leaked cyber-weapons, or the increasingly common blackmail viruses and their campaigns today, are a real threat. According to Károly Kassai, thinking in the field of "cyber defense" means the complex development of the information security policy defined in the

---

24 Section C 163 (1) of Act C of 2012 on the Criminal Code

25 KASKA, Kadri – OSULA, Anna-Maria – STINISSEN Jan: The Cyber Defense Unit of the Estonian Defense League, Tallin 2013. https://ccdcoe.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf (downloaded 15 September 2017)

26 Csaba KRASZNAI: Information security solutions for Hungarian e-government applications. ZMNE 2011. (PhD dissertation) http://krasznay.hu/presentation/szerzoi_ismerteto_krasznay.pdf (downloaded 15 September 2017)

ministerial order in the field of defense. The challenges can be grouped into the following areas:

- creating a favorable environment (delineation of the powers, tasks of the organizations concerned, including the specific case of the special legal order);
- increasing the level of security of electronic data-processing networks (technical tasks);
- development of the capability to counter cyber-attacks (issues of electronic incident management and monitoring of electronic information security tasks);
- increasing expertise (specialized training for users and operators, including cyber security practices);
- research and development (exploiting opportunities at national and international level);
- cooperation (to put it simply: with whomever it is thinkable, along lines of bilateral benefits).[27] [27]

Conclusion

The diverse resources, strategic and tactical vision of countries and their human communities, as well as their cultural and, inter alia, religious diversity, have resulted in many unprecedented processes. With the help of the aforementioned info communication networks, the media has taken the lead in informing people and presenting the reality of faraway conflicts, the reality of extremes and violence incomprehensible for many, beyond the "Janus-face" of knowledge. In the age of postmodern societies, the daily lives of European citizens as individuals ("security objects") were increasingly determined by access to, sharing and possession of data and information flowing through networks.

Cyberspace, as a new military theatre of operations, poses many challenges for the military thinking of the future. The complexity of information operations requires the setting up and strengthening of capabilities. The technical and human resources needs for cyberspace operations need to be assessed and consciously developed.

Bibliography:

- Act L of 2013 on Electronic Information Security of State and Municipal Bodies
- Act C of 2012 - on the Criminal Code
- Dénes BERÉNYI: How does a physicist see the world today? (2010) http://vigilia.hu/regihonlap/2010/7/berenyi.html (downloaded 15 September 2017)

[27] KASSAI, Károly: Cyber defense and the Hungarian Defense Forces. Military Engineer, Year VII., Issue 4, pp. 137-138.

- János BOROS: Jean-François Lyotard, The Thinker of Diversity, An Attempt to Knowledge Theory Approach, Contemporary: Literary and Art Magazine, XLII. EFV. No. 3 1999. pp. 298-306. ISSN 1588-0885
- Government Resolution No. 1139/2013. (III. 21.) – on the National Cyber Security Strategy of Hungary
- Zsolt HAIG: Information, Society, Security, NKE Services Ltd., 2015. pp. 93-122. ISBN 978 615 5527 08 1
- KASKA, Kadri – OSULA, Anna-Maria – STINISSEN Jan: The Cyber Defense Unit of the Estonian Defense League, Tallin 2013. https://ccdcoe.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf (downloaded: 09 September 2017)
- KASSAI, Károly: Cyber Defense and the Hungarian Defense Forces, Military Engineering, Year VII, Issue 4, pp. 137-138.
- József KIS-BENEDEK: Jihadism, Radicalism, Terrorism, Zrínyi Publishing House, 2016. p. 279. ISBN 978 963 327 739 3
- Sándor MUNK: Military Scientists and Their Research Areas, Part 1: Empirical Investigation of Military Fields, Military Science, 1-2., pp. 4-16. ISSN 1215 4121
- István RESPERGER – Péter Álmos KISS – Bálint SOMKUTI: Asymmetric Warfare in the Modern Age - Small Wars with a Great Impact Zrínyi Publishing House, 2014. pp. 13-44. ISBN 978 963 327 592 4
- RÓZSA, Tibor: Possibilities of applying information operations in the Hungarian Defense Forces
- SIMON, László: Increasing Terrorism in Europe and its Impact on Securing Military Mass Events, In: Professional Review, 2015 No. 2. pp. 145-162. ISSN 1785-1181
- László SIMON: Information as a weapon? In: Professional Review 2016 pp. 34-60. ISSN 1785-1181
- József SZABÓ (ed.): Military Lexicon, Volume 1 Hungarian Military Society, Budapest, 1995. ISBN 0469000676354
- W/o No.: AJP 3-10. Allied Joint Doctrine for Information Operations pp. 1-3. http://info.publicintelligence.net/NATO-IO.pdf (downloaded 15 September 2017)
- W/o No.: General / 57 Information Operations Doctrine 1st Edition, Proceedings of the Hungarian Defense Forces, 2014 NKE Doctoral (PhD) Dissertation 2016, http://hhk.uni-nke.hu/uploads/media_items/rozsa- tibor-colonel-the-information-operations-apply-options-in-hungarian-homeland-task-system.original.pdf (downloaded: 15 September 2017)
- W/o No.: The European Union's cyber security strategy. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001 (downloaded 15 September 2017)
- W/o No: A Russian daily described how they influenced the US presidential elections. MTI. 10/17/2017, https://sg.hu/articles/it-tech/127765/orosz-napilap-mutatta-be-howan-efollasoltak-az-amerikai-valasztasokat (downloaded 18 October 2017)

KATA REBEKA SZŰCS

MOBILE SECURITY BASICS TO IMPROVE PERSONAL AND CORPORATE SAFETY

Abstract

Humans are the weakest link in the security chain: their individual, personal decisions can have a huge impact on the security of organizations. Publicly accessible personal information about employees can be a vulnerability for companies and can be exploited by malicious players. Individuals can be used to get to organizations with cyber-crimes, for example with social engineering or phishing. These are common threats nowadays, against which awareness, constant questioning and taking some basic appropriate steps to increase safety are key. This article aims to raise alertness of this risk. The consequences of security breaches can be serious, enterprises can face enormous fines and their reputation can suffer, which can endanger the future of them. People spend substantial amount of time using their smart phones and accessing social media in their personal lives without considering the risks of this for their employer. In the following article I am going to introduce cyber-crimes and their tools to get to companies through employees. I am going to explain simple and practical methods to mitigate these kind of risks, with a special emphasis on mobile device security. I trust that even the simplest measures can help people and organizations to achieve a better state of security. In the last section of the article, I am going to present a survey, which aims to explore the current situation and habits of using the presented countermeasures in this regard.

***Keywords*:** Security, Mobile Security, Cyber Security, Risk mitigation

1. Introduction

Humans are the weakest link in the security chain. This sentence can be seen a lot lately, but we rarely think about the practical significance of it. The Internet, our smart phones and other smart devices, and social media are now important parts of our lives, but their usage is a risk not only for us, users, but for employers as well. Publicly, freely available data of employees or data obtained with malicious intent from the workers is a substantial vulnerability for companies. Malicious actors can easily get to firms with cybercrimes, such as social engineering or phishing, through unsuspecting employees. The consequences can be very serious for companies. According to the General Data Protection Regulation (GDPR, 2016/679 EP), which regulates the protection of personal data at the legislative level[1], companies can be fined up to 4% of annual global turnover or EUR 20 Million, whichever is greater. (Also lower amount of fines can be determined for various violated points using a

[1] ANDÓ, G.: Minden, amit a GDPR-ról tudni érdemes; kozlekedesvilag.hu, 30 04 2019. https://www.kozlekedesvilag.hu/2018/08/24/minden-amit-gdpr-rol-tudni-erdemes/ (downloaded: 06 October 2019)

tiered approach.)[2] Fines are not the only consequence, companies' reputation and trust can also suffer, which is enough to ruin them. Living online brings not only convenience, but great and ever-changing security risks. In 2018 more than half of the world's population (4 billion people) used the Internet, compared to 2015, when this number was only 2 billion. According to Cybersecurity Ventures, this ratio could rise to 75% of the expected global population by 2022.[3] While attacks earlier were aimed at destroying data or making it inaccessible, now data possession and monetization has become one of the main drivers. According to Verizon, money is the main motivation for 76% of cyber attacks. 73% of these are committed by people outside the organization, including 50% by organized crime groups and 12% by nation-states or state-linked actors.[4] Awareness, continuous questioning, and taking the right basic steps to increase security are key to reducing these risks. Anti-virus and anti-malware programs detect more than 10,000 different malicious files each day. In the first quarter of 2019 alone, 1.9 billion data records were leaked. The average cost of data leakage in 2018 was $ 3.86 million.[5] It is visible that this is a very dynamic, actual and real problem that companies need to be able to respond to. The seriousness of the topic is also illustrated by the fact that, according to an AT&T report, cyber security is a top technology priority for organizations: 82% of the companies they surveyed set to improve cyber security as their number one goal, followed by sales and marketing analysis improvement goals.[6] However, it is not enough for companies to take action, employees' personal decisions can also influence their safety, so training and awareness plays an important role. The purpose of this article is to raise awareness of the topic, and to provide employees with some simple, practical tips to protect their vulnerabilities to reduce corporate security risks.

2. Threats

Before the recommendations, it is important to have a look at the threats, the sources of the risks and the possible methods of attack. According to the Hungarian Information Security Act [2013], cyber security is the continuous and systematic use of political, legal, economic, educational, awareness-raising and technical tools to manage risks in cyberspace and provide an acceptable level of existing risk, making cyberspace a reliable environment for the smooth functioning and operation of social and economic processes. [7] Listing these risks and cyber security threats is really difficult because new forms are emerging every day. But in order to be able to defend

---

2 GDPR Key Changes; 21 04 2019. https://eugdpr.org/the-regulation/ (downloaded: 10 July October 2019)

3 S. MORGAN: Cyber Security Ventures- 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics; Cyber Security Ventures, 06 02 2019. https://cybersecurityventures.com/cybersecurity-almanac-2019/ (downloaded: 30 September 2019)

4 L. ANDRE: 51 Important Cybercrime Statistics: 2019 Data Analysis & Projections; FinancesOnline, 02 01 2019. https://financesonline.com/cybercrime-statistics/. (downloaded: 07 October 2019)

5 TechJury – 33 Eye-Opening Cybercrime Statistics to Help You Protect Your Business in 2019; TechJury, 07 06 2019. https://techjury.net/stats-about/cybercrime/. (downloaded: 01 October 2019)

6 L. ANDRE op. cit.

7 L. KOVÁCS: Kiberbiztonság és -stratégia, Budapest: Dialóg Campus Kiadó, 2018.

against them, it is important to know their potential sources and forms of appearances. The most popular and clear way of keeping track of threats is to keep an eye on the top lists, such as the operators' OWASP (The Open Web Application Security Project) top-list or the annual ENISA (European Union Agency for Network and Information Security) Threat Landscape Report. Almost every big security service provider publishes an annual report listing the most relevant and popular sources of threats as well, and it is also worth following certain sites dealing with cyber security. According to the ENISA 2018 (recent) list, without the intent to provide the complete picture, the top 10 cyber threats are as follows.

Malware: The top on the list was responsible for 30% of reported unauthorized access to data incidents in 2018, according to the report. The notorious WannaCry or Petya belong to this category. The most important trends in this area are the transition from blackmail viruses to cryptojacking (programs that use victim resources, CPU or GPU, to mining cryptocurrencies without his or her consent). In addition, file-less attacks and mobile threats are also on the rise.

Web-based attacks are infecting a user through web interfaces, browser, web page or plug-ins. It has many infamous forms, such as drive-by, watering-hole, man-in-the-middle and man-in-the-browser attacks.

Web application attacks: exploit weaknesses in web services and applications, often overlapping with the attacks mentioned in the previous paragraph. In other words, attacks of active or passive components of software available over the Internet. The OWASP list also refers to this type for example.

Phishing: Mails that use social engineering techniques to persuade the recipient to "catch the bait", in other words, opening malicious attachments or clicking on an insecure URL where they may enter credentials or give money to unauthorized people or sites. According to the ENISA report, this type of attack is so popular that it has contributed to 90% of malware infections and 72% of data leak incidents. It is worth mentioning that these attacks are increasingly targeted, more personalized, so they are often difficult to avoid, which is especially dangerous in corporate leadership roles. This type is also characterized by the growing importance of mobile threats as well as serving via https, which increases the chances of 'fishermen'.

Denial of Service (DoS) attacks: Their goal is to make the system inaccessible and unusable by overloading the system. Although the number of attacks of this type is increasing, there has been no real large-scale attack last year. It is noticeable that more and more providers are offering solutions to deal with these, which are in high demand from the corporate side.

Spam: Although it is losing popularity year after year, spam is still in the top 10. These are unsolicited messages and e-mails that are transmitted to users through botnets. As they evolve (switching to social media, getting better at personalizing credible companies, stories, etc.) and low cost to attackers, they are still a threat to users, using their storage space and bandwidth. It is promising that there are coordinated law enforcement actions taken to remove botnets and that spam filtering services are getting better and better.

Botnets: A device connected to multiple Internet sites, each running one or more bots (a robot that performs automated tasks on the Internet). These can be used to execute several of the attacks listed above, such as DoS or spam attacks. As they evolve rapidly and the source code of some of the more prominent ones are available, the threat they represent is significant.

Data breach: The only point in the list that is not a threat, but rather the result of a successful attack, is that some corporate or individual personal information is leaked and disclosed. These are serious consequences for a company (and of course, for the individual as well), not only are they facing heavy penalties due to the GDPR, but their reputation is also damaged. Interestingly, 48% of these incidents were reported by outsiders, 27% due to human negligence and 25% due to system failure.

Insider threat: A threat that comes from current or former employees. We can distinguish intentionally malicious, negligent and compromised insider threats. As we can see, although the term generally includes the employee's deliberate intent, this is not always the case.

Physical manipulation (damage / theft / loss): Although these are not strictly cyber attacks, they are still an important source of risk, which can lead to unauthorized access to data, for example. Typically, instead of physical theft, digital data theft has become more popular (using the tools above, for example). This includes, for example, limiting physical access (like access to buildings) and the myriad possibilities of using social engineering for this purpose, as well as genuine threats of negligence, such as sensitive data being thrown into communal trash instead of shredding.[8]

It is visible that the items in the above list are hard to separate into isolated types of threats, they are usually combined or one is a way to the other. On top of the above list, there are countless threats that can multiply, change and evolve daily, and the risks of which can be reduced by just a few simple steps. It can be seen that individual, personal decisions and possible negligence can also have a huge impact on companies, as attackers can often get near a company through the individual and through personal user accounts and mobile devices. The following are some of the areas where most of the threats may come from, where the precautions in each area do not require too much effort, but can mean survival for companies at these times.

3. Proposed countermeasures in practice

For the sake of simplicity, I present the most common sources of threats, which are also present in personal levels, in groups. The grouping is based on practical considerations. The following are all important sources and contributors to the exploitations that have been achieved using the methods listed so far. This is supported by, among other things, a study by security experts cited in the ENISA report, saying that phishing (67%), poor passwords or reusable passwords (56%), devices left unlocked (44%), and unsafe Wi-Fi networks (32%) account for

[8] ENISA: ENISA Threat Landscape Report 2018- 15 Top Cyberthreats and Trends; European Union Agency for Network and Information Security (ENISA), Athens, 2018.

vulnerabilities resulting from insider threats. In addition, excessive access rights granted to individual employees have caused incidents, which need to be monitored, constantly reviewed and kept up to date by employers. [9]

3.1. Passwords

Although this section is not mobile specific, the password issue has always been important for security and if easy, can make users targets effortlessly, so this is the first one in this list. Despite the constant mentions of this problem, there still seems to be room for improvement in the area.
There are several ways to crack a password, usually by trying, spying, decrypting, or even attacking the authentication system. Here are some examples of actual possible methods, first of all the trying method.

Dictionary attack: uses dictionary words to systematically test words in a password to crack it, chances are not changed much by combining multiple dictionary words together either.[10] Therefore, it is worth avoiding their use. Leetspeak (replacing a letter with an alike number) is already tackled by countless password crackers, so it doesn't add much security either. A practical and memorable way of converting a dictionary form or a person-specific password is, for example, to push all characters one letter away in one direction on the keyboard, making numbers and special characters harder to guess. We must note that this measure helps only if we consider the other practical advices in this paragraph.

Brute force attack: Attacks all possible alpha-numeric combinations. To counter these attacks, increasing the number of characters of a password can significantly increase your chances of not being hacked. It is therefore advisable not to protect yourself with a one-word password, but rather to use phrases or whole sentences.

Rainbow table attack: A decryption method that uses a predefined password list containing hashes (a one-way algorithm representing data as a unique string) to infer passwords to search for hashes. By another general grouping method, the password can also be obtained by **phishing**, **social engineering**, or **malware.** [11] The former will be discussed below, but the latter may include for example the use of keyloggers (a program that records each keystroke by a user to allow access to confidential information and passwords) and man-in-the-middle attacks (when intruding in a channel between two communicating parties, the attacker is able to observe and influence traffic unobtrusively). Some of these risks can be mitigated, for example, by recommended methods of protection in the following mail or wireless connection sections.
So one of the most basic problems is what the password should be. Since most people are looking for convenient solutions, we try to choose a password that is easy to remember (such as something personally linked to its owner) and we use it wherever possible. Of course, this is not a very safe practice. In my opinion, it is advisable to

---

9 ENISA (2018) op. cit. p. 72

10 V. HIGHFIELD: The top ten password-cracking techniques used by hackers," 26 06 2018. https://www.alphr.com/features/371158/top-ten-password-cracking-techniques. (downloaded 06 October 2019)

11 Ibid.

use at least three different types of passwords or groups of passwords, one for work accounts, strictly separating another for private purposes, and one for managing your finances. It is worth choosing something that is not personally related to the user, otherwise they can easily be guessed, for example, from social media with minimal research (with the help of social engineering). Examples include date of birth, the name of the child, or the names of the pets. It is also advisable to avoid passwords that are too easy for everyone to remember. For example, Kevin Mitnick, in The Art of Invisibility, mentions the 11 million passwords published by the Ashley Madison hack in 2015, the most common of which were: „123456", "12345", "password", "DEFAULT", "123456789", "qwerty", "12345678", „Abc123" és „1234567."[12] It is easy to see that breaking them does not require a lot of resources. If memorizing many user accounts and the associated passwords causes problems, many people grab paper and pencils, take notes, and make a list. In this case, it is worth providing a high level of protection, but it is best to avoid this practice. To replace notebooks and other insecure solutions, password management programs have been created that securely store our passwords across multiple accounts, and users need only remember one master password to allow access to the rest. However, we must note that this method can also cause problems: if we store all passwords in one program, it is enough to break that program and all of our accounts will be compromised. There have already been examples of an infected password management program being introduced in application stores specifically designed to misuse the data that was loaded into it.[13]

It is also a good idea to change every password you use from time to time. According to a penetration test expert, people usually sell passwords in 2-3 years on the dark web (the part of the web that is not seen by search engines), so if they are changed periodically (for example every year), they can no longer be used for abuse. Lastly, a practical tip for security questions that some service providers ask you to answer in the event of a password being forgotten. If we consider these to be possible sources of information about us that may be circumvented due to possible vaguely worded privacy policies, it is worth providing non-realistic or at least not personally relatable data on these questions (for example, writing hospital rather than a specific birthplace). (Hopefully these types of data releases are becoming less likely in Europe due to the General Data Protection Regulation (GDPR), but better safe than sorry.) Instead of password protection alone, consider using multi-factor authentication, which can use any combination of something the user knows (e.g. password), something that the user has (e.g. token) and something that the user is (e.g. biometric identification). Combined use increases security and makes it more difficult for malicious attackers to succeed because multiple fronts need to be attacked simultaneously. The aforementioned biometric identification is an automated technique that measures and records the physical and behavioural characteristics of an individual and uses them for identification and authentication.[14] The best known types are fingerprint, iris, face and voice recognition. It is important to know that these can also be hacked and not completely reliable, so again, combined usage can improve safety levels.

---

12 K. MITNICK – R. VAMOSI: The art of invisibility, New York: Hachette Book Group, 2017., p. 19

13 Ibid.

14 T. KOVÁCS – I. MILÁK – C. OTTI: A biztonságtudomány biometriai aspektusa; Pécs, 2012.

A hacked personal password can help attackers to get to companies in a number of ways: we often use personal passwords for corporate accounts as well, so they can use the cracked passwords to get into company networks and accounts. Another problem is that many of our personal user accounts (e.g. social media, mail) are opened from corporate laptops, so the threats that come through that platform can affect the company as well. Hacked accounts can also help attackers prepare the perfect phishing scam or personalize social engineering, which can also provide access to companies. Therefore, it is important to use passwords to mitigate this risk, not only in corporate but also in private usage, even when it is not mandatory (e.g. protecting laptops and smartphones at home).

3.2. Wireless connections

The use of wireless connections (such as Wi-Fi and Bluetooth) is becoming more common in both private and corporate life, and while it increases the mobility of users, it offers countless opportunities for malicious attacks as well. From an employee point of view, this area should be grouped into two main areas of use: wireless connections on home and mobile devices. This article focuses on Wi-Fi connections due to frequency of use, but Bluetooth can be considered with a similar way of thinking. During a war driving or war walking (the purpose of which is to discover the physical location of available wireless networks from the car or while walking) numerous vulnerable wireless networks can be found, some of which are publicly available. These publicly open access points pose a vulnerability to those who use them, even if they are encrypted. (Several security protocols are suitable for this purpose, such as WPA (Wi-Fi protected access) and WPA2.) Routers publicly show, among other things, the SSID (service set identifier), the device name which by default is provided by the device manufacturer. It is a good idea to change this, as attackers will immediately be aware of potential known vulnerabilities of the model, and usually the default login credentials will be available on the Internet (usually for example admin-admin). As a new name, it is worth choosing a non-personal name and protecting it with a strong password, as mentioned earlier. It is also possible to use whitelisting to increase security by specifying which devices can connect with MAC (physical) addresses and everyone else is blacklisted and unable to connect. Aside from the fact that this can cause inconvenience, there are tools (such as aircrack-ng) that can crack these lists and with the help of MAC spoofing (spoofing the physical address provided by the manufacturer for fraudulent purposes) or ARP (address resolution protocol) spoofing can connect to the router.[15]

Considering the other side, connecting to publicly available Wi-Fi also has its dangers. A connection can be called public if it is not encrypted or if the password is public or not required. The traffic through these can be easily compromised. It is important that some mobile operating systems monitor only SSID and password matching, and do not filter MAC addresses, so if an attacker makes a small effort to learn these, he or she can make the devices to connect to his or her network, which can have serious consequences. For example, if the attacker knows that the subject goes to a coffee shop frequently, where he or she accesses free Wi-Fi, if the attacker knows these access credentials and Wi-Fi name, that can mean a direct route to the target. Often, auto-connect is the default setting, so you might want to turn this feature

[15] MITNICK – VAMOSI (2017) op. cit.

off or limit it to Wi-Fi used in a trusted location, such as home and work. It is also recommended that you keep the Wi-Fi off and only re-enable it when justified or safe. Alternatively, you can use virtual private network (VPN), which allows you to send and receive data over a public network as if the devices were directly connected to a private network. This traffic is already encrypted. [16] However, there may be a back door built into the VPN managers available in the application stores as well, which the malicious actors have placed for later use. In the next section I will mention this topic in more details.

In summary, there are several dangers to using Wi-Fi, the most important of which is the creation of **rouge Wi-Fi access points**, which can be used to **execute man-in-the-middle attacks**. These intrusion attacks work, as I have already mentioned, by intruding between the two communicating parties and controlling and influencing the traffic between them. There are several ways to do this: the access point name can be changed without noticeable difference (for example, an attacker can mimic a known network name by swapping characters that resemble: l to capital i, or zero to O) which makes the user to connect to their own access point. The above mentioned automatic connections to known networks can also belong to this group, they also can be false access points. DNS (Domain Name Server) spoofing can also be used, which exploits the vulnerability of a domain name server to redirect traffic to another server.[17] SSL stripping (Secure Socket Layer, which keeps client-server connections secure) forces the client to communicate unencrypted with the server. If networks are not well protected, attackers can do many things, such as sniffing (attackers can sniff, see communications that are not meant for them), packet injection (they can add malicious packets to communications), and session hijacking (which can be used to take control of sessions when Web applications are logged in.) [18] These are also methods to carry out the abovementioned attacks. Through our private networks, attackers can reach us, and through us, we are potentially allowing them to reach employers. The results of such attacks can be the leakage of usernames, passwords and personal data, or phones, calls and SMS can be intercepted, which also provide a great platform for social engineering attacks.
Although this subsection was mainly about Wi-Fi, it is worth mentioning that Bluetooth connections also carry risks and are vulnerable. With the proliferation of smart watches and IoT (Internet of Things) in general, we are increasingly leaving this interface on, so we have to consider the benefits and dangers of it as well while doing so.

3.3. Mobile applications

An average user has 60 apps installed on their phone, which gives malicious actors great surface to attack. As it has become a part of our lives, a wealth of data is

---

16 M. ROUSE: Search Networking – VPN (virtual private network); Search Networking, 01 08 2019. https://searchnetworking.techtarget.com/definition/virtual-private-network. (downloaded: 30 September 2019)

17 KASPERSKY: Kaspersky – What is DNS Cache Poisoning or Spoofing?; 09 10 2019. https://www.kaspersky.com/resource-center/definitions/dns. (downloaded 09 October 2019)

18 Rapid7, "Rapid7-Man-in-the-Middle (MITM) Attacks; 08 10 2019. https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/. (downloaded: 08 October 2019)

accessible through our phones.[19] Using Check Point security provider's grouping, mobile threats can come from three main sources: network, applications, and the device itself.[20] The security of networks can be enhanced by the above. The latter two are described below.

Applications and mobile devices themselves are therefore a source of risk. Briefly, in the case of applications, the following risks may arise. [21]

Infected apps from Google Play Store or Apple Store. It may be surprising, but service providers do not have the capacity to thoroughly examine every app that has been uploaded, so there are examples where an app turns out to be infected years after it is published to stores (and after many downloads). Apple has stricter requirements for application developers than Google, but that does not guarantee security either. To reduce this attack surface, it's a good idea to look closely at the reliability of an application, or the provider. If it is a well-known brand's or major company's development that can give some sense of security, but that is not always true either. If we are the victim of such an attack, we can hope that the steps, suggested in other sections of this paper, can reduce the damage.

Sideloaded applications: sideloading means file transfers between two local devices (via Wi-Fi, Bluetooth or memory card). For Android, this usually means installing an app package in APK format on an Android device. [22] Such packages are usually downloaded from sites other than Google Play, usually via a computer. For Android users, downloading apps is only possible if the user has enabled "Unknown sources" in their security settings. For iOS, it means installing an IPA file on an Apple device, usually using a computer program such as Cydia Impactor or Xcode on the actual device, not through the Apple Store. For modern (not jailbroke) versions of iOS, application sources must be trusted by both Apple and the user.[23] The simplest way to reduce the risk is to avoid sideloading and hacked, misconfigured devices, which carry dangers and are much less secure than factory-configured devices.

Zero day application malware: A zero-day attack exploits a vulnerability that has not yet been discovered, so there is no security patch for it yet. This can appear in any category, there are many malicious programs targeting applications that for example can take control of the device.
According to McAfee Mobil Threat Report, in 2018 the number one in this threat category were hidden applications, which then get access to our personal data

---

19 R. SAMANI – G. DAVIS: McAfee Mobile Threat Report Q1, 2019; 01 01 2019. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf. (downloaded: 27 October 2019)

20 Check Point: Checkpoint – CHECK POINT SANDBLAST MOBILE; 25 11 2018. https://www.checkpoint.com/downloads/products/sandblast-mobile-datasheet.pdf. (downloaded: 20 September 2019)

21 Ibid.

22 J. HILDENBRAND: Android Central- What is sideloading; 02 02 2012. https://www.androidcentral.com/what-sideloading-android-z. (downloaded: 20 September 2019)

23 N. STATT: The Verge- This illicit iPhone app store has been hiding in plain sight; 20 February 2019. https://www.theverge.com/2019/2/20/18232140/apple-tutuapp-piracy-ios-apps-developer-enterprise-program-misuse. (downloaded: 30 September 2019)

unnoticed. These can get to phones in different ways. There can be apps which have built in backdoors. For example TimpDoor is a malware for Android, it tricks the user to download app via SMS (it is visible as a voice message which requires the user to download an app to be played) from outside the official store. It can ensure access to the device and as its icon is hidden, it is hard to notice and it runs in the background. Then the device can also be used as entry-point to internal networks of companies. We might also remember the similar Guerrilla, DressCode, Rootnik and MilkyDoor, which are typically hidden in games or customization tools. These malwares naturally are handled by Google as best as possible, but attackers always find newer ways to get to their targets.[24] Another dangerous form are FakeAPPs, which are apps posing as something known. They mimic popular applications and often are very convincing copies. For example there was a fake version of Fortnite app (said beta, invitation only version, tutorials). Attackers also set up targeted ads, which contributed to the success of spreading these. These were downloadable from unknown sources and users had to allow admin access and other rights to these apps. Then they start sending messages, downloading hidden apps and allowing ads. They can also be spyware or start cryptomining. Obviously this model of publishing apps outside of Google Play brings great risk (and also normalizes this, which makes users less suspicious against these attacks). Banking is also a popular area for this kind of attack, also with Trojans (for example looks and functions as a valid app, but after a while, decrypts the malicious code, after the app is already out of the sandbox). This can be noticed by unexpected popups and behaviours and overlays which are asking for personal information. In my opinion banks' communication is also key in this area, to make customers aware and ensure them about valid application versions. As we can already see, these categories are overlapping, but I would like to add a few thoughts to cryptomining applications. They are not restricted to stay only on the users' phone, but they can also jump to other home devices (such as smart TVs). They are not only using processing capacity, but harm to the hardware as well (for example the battery can swell and crack the case). Just like for other threats, provides are starting to ban these kind of applications as well. [25]

Users may also be a source of danger if they do not update their installed applications and operating system. The main purpose of each update is to address the discovered vulnerabilities, so in theory, every time we update, we need to get more secure applications. It can be manual or automated, users can decide on the settings. Users must also review the default settings of the applications. For many apps the default is to share the location, photos, etc. on the phone, which comes with risks, so users should only allow the most necessary ones to take advantage of the app's features.

As they can be used as applications, firewalls for mobile devices are also going to be mentioned in this section. Although their usage is not typical outside the corporate environment, firewalls can be a very effective way to protect mobile devices. There are many service providers to choose from, with some features available free of charge and higher-end ones available for purchase. Their strength is tackling zero-day attacks, because at the enterprise level they can merge data from operating firewalls, come up with responses, and then they can push down the updates

[24] SAMANI – DAVIS op. cit.
[25] Ibid.

to other operating firewalls under their control. They can also scan networks, help web browsing make safer, create secure vaults for photos and videos and so on. They are important because they can detect those risks which humans are not able to, so they can be a good addition next to practices enhancing safety.

3.4. Mailing, Social Media

Email and social media are one of the biggest attack platforms nowadays, through which for example **social engineering** and **phishing** attacks appear. "Social engineering, by means of influence and persuasion, deceives, manipulates or persuades people that the social engineer is really what they say they are. As a result, the social engineer, with or without technology, can use people to gain information."[26] According to surveys, more than 90% of successful hacks and data breaches come from phishing scams, emails that make recipients to click on a link, open a document, or pass information to people whom they should not.[27] Training employees, users to recognize and respond to these threats can therefore be critical for companies, but we also see the importance of this as an individual.

In order to filter out scams and malicious emails received through the mail system, we need to carefully examine the email. First the user has to look at the sender by hovering the cursor over it, which shows the real email address where it came from. If it doesn't match the displayed address, the suspicious email is likely malicious. Note that emails can often appear to be from a trusted source, but only small details indicate that they are not true senders, such as @ gooogle.com, one character more, or switching o to zero, and similar changes. It is customary to add extensions to names of trusted providers, such as @ amazoon.helpdesk.com, which should also be treated with care. Hovering the cursor over a hyperlink can also help to make the real destination visible, so if it does not look the same as the displayed, it possibly is a fraudulent or suspicious page. Another reason for suspicion is if there is an urgency in the email, such as short-term offers or sudden calls to action. These all serve the purpose of tricking the reader to act immediately without thinking as the attacker wishes. Even strange or too generic addressing, or if the letter is written with bad grammar can be a sign of false intent. These emails are often sent with non-native unusual wording (these are usually generated using Google translate). It is also suspicious if the sender asks us for data, or data confirmation via a link, or if they offer prizes, but ask for sensitive information such as credit card details in return. Even if these requests sound and look valid, it is worth visiting for example the bank's own website rather than using the link provided, or calling the service provider to confirm the request verbally. However, the general policy of businesses is to never ask for personal data via email. Attachments can also be a source of risk. It is worth considering whether the recipient is waiting for the sender to send an email with attachment, and whether the email is addressed to them. These are trivial questions, but human curiosity sometimes makes the recipient to open up content that contains attacks. If malwares pass through the simple rules above, firewalls can still help. It is important to keep private and corporate correspondence strictly separated to protect employers. Although this is generally not allowed by company policies either, it is

[26] K. MITNICK – W. SIMON: A legendás hacker – A megtévesztés művészete; Budapest, Perfact-Pro, 2002.

[27] MORGAN op. cit.

strongly recommended not to use a private mail account to share company files. It is also possible that we access our private social media or mailing accounts from corporate laptops, which has to be done with caution as well. According to the already quoted ENISA report, phishing attacks on mobile devices have grown on average by 85% per year since 2011, compared to the same period in the previous year. Phishing has been observed to increase through SMS, mobile messaging (WhatsApp, Facebook Messenger, etc.) and social media applications (such as Instagram).[28] Trends show that these attacks are increasingly personalized, making it increasingly difficult to detect them. Social media can be a great source of personalization for attackers. Phishers take advantage of the trusting relationship between users and social media platforms and the information they contain and they can easily guess for example personal passwords (like year of birth, children's name, etc.). It is recommended not to make the profiles public and to keep and show as little information as possible on these sites. Disclosing our phone number also allows social engineers to access online banking services (by phishing an SMS ID code). Image sharing can give hints about where we are going, which can give burglars a chance, but we can also share our interests through social media which can help social engineers to attack us in person or in other ways. For a hacker who is knowledgeable in influencing, people, and communications, this is enough to acquire sensitive information from its owner. Here, I would like to point out that people's fundamental compassion plays a big role, which is why they do not immediately assume the intention of abuse from someone who is kind to them. There are countless stunning videos on Youtube where reporters, after asking a few kind questions, are able to tell the subject's passwords as they share it themselves (in a few steps). As I mentioned earlier, the threat does not necessarily come from bad intentions, it is enough to let down our guard and answer questions that seem harmless or sincere. The books of Kevin Mitnick and Christopher Hadnagy have many more astonishing examples of how easy it is to trick people. Last but not least: LinkedIn. It can be used for example to understand corporate structure, which provides a good attack surface for corporate fraudsters, and a good reference for using social engineering (for example, the attacker can pretend to be a colleague). Lastly, for this point, it is advisable to delete existing user accounts on old or unused pages, as they can act as an unattended attack surfaces as well.

One final point worth noting is charging smartphones from corporate laptops. In this case, the charger cable is also capable of transferring data, so the phone acts as a storage medium, which is generally prohibited by corporate policy because it can enable the penetration of malicious attacks into the corporate network. Therefore, it is recommended to avoid this as well, just like connecting other media of unknown origin. (There is also an infamous form of attack during which attackers leave infected media, for example USB stick or CD on the street in front of the company and employees look at what them to find out what they are on a corporate machine, infecting the entire network.)

4. Research

To understand the current attitude and practices regarding security, I conducted an online survey with the same chain of thoughts as above. There were several

[28] ENISA (2018) op. cit.

questions about everyday security. I managed to gather 124 answers, 35% from males, 65% from females. Almost half of the respondents (45%) are from Budapest, and 41% are from other Hungarian cities. The rest of them lives elsewhere (villages etc.). More than half of them are generation Y, born between 1980-1996, 31% are generation Z (born between) 1997-2010, 11 are generation X (born 1965-1979), 2% are baby boomers (1946-1964), and only 1% of the respondents were born before 1945 (veteran generation). 43% of them are students from universities, 32% of them work. 30% of them have education or work experience in IT security field, which can affect their familiarity. In summary, the sample is quite young, which means that they should be more aware of the risks, but might mean that they do not consider the employers' point of view in their everyday life.

In the first question I provided a list of threats and asked the respondents to select those which they know the meaning of. Here they could mark multiple answers. The threats in the below diagram are listed from the bottom following the order in the first section of the article, which referred to the ENISA list. That list was based on prevalence. Interestingly there are kinds of attacks in the list which are less known by the respondents, but are still a top source of risk. This means that there is still room for improvement in identifying the source of threats, which would help reducing the possibility of attackers' success.

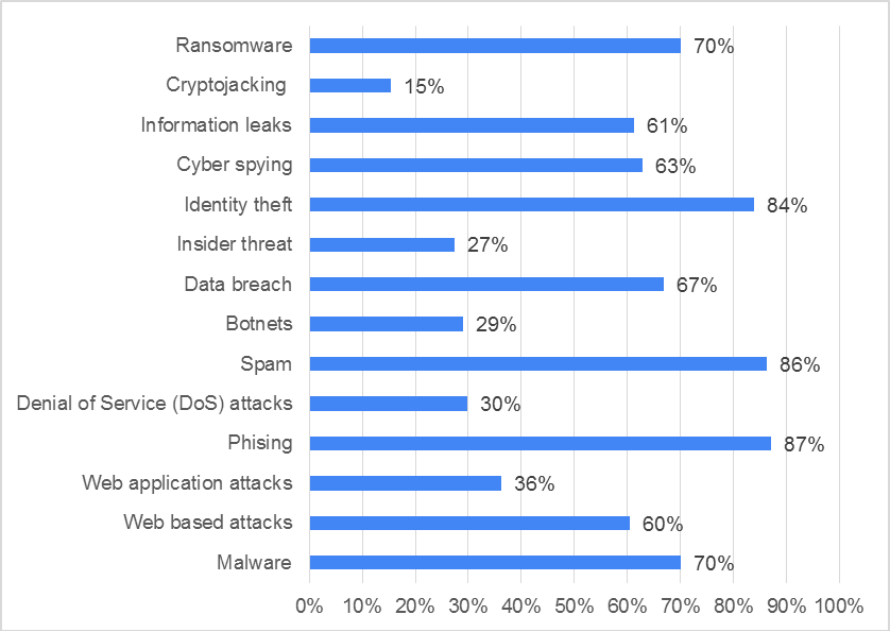


Figure 1: Which of the following threats do you know?, own edition, n=124

The next section of the questionnaire was about password habits with more than one questions. Respondents were asked to share the number of characters of their passwords, which they use to access their emails. The minimum was 6, the maximum was 32 characters, with the average of 12, median of 11. The first quartile is 9, the second is 11 and the third is 14. This means that most of them use quite short

passwords, which is not advisable because it makes attacks easier. I also queried how often they change their passwords. The answers are visible on the below frequency analysis figure compared to gender. In summary we can see that the habits are diverse in this regard (the question was open ended), but most commonly, respondents change their passwords rarely or almost never. This is followed by every less than six month and yearly. We can observe that based on the sample, males are more careful with their passwords in general.

Prevalence	Total	Male	Female
Every less than 6 months	21%	34%	13%
Twice a year	5%	5%	5%
Yearly	20%	22%	18%
Every 1-2 years	3%	7%	0%
Every 3+ years	3%	5%	3%
When the former password expires	9%	5%	12%
When I forget it	2%	0%	3%
When I am notified that it is compromised	3%	0%	4%
Rarely, almost never	35%	22%	42%
Total	**100%**	**100%**	**100%**

Figure 2: How often do you change your passwords?, own edition, n=124

This same password can be personally linked to 28% of the respondents, which means that the depersonalizing criteria to increase security is fulfilled in two third of the cases. 81% of the respondents reported to use this same password for more than one account, but only 25% of the interviewees said to apply the same password for work and private life. This is fortunate, because it could be a huge risk for employers. Respondents who have IT related education or experience are accountable for a higher ratio of separated password usage, but the relation is not significant. The last related question was if they use password manager programs. Only 30% of them use this kind of programs, and again in line with the previous answers, those who are more familiar with IT tend to use these programs more often, but not significantly. Hence this section of answers suggests that most of the respondents who are working are aware of the risk of using the same password for work and personal accounts at the same time. They are also quite good at protecting themselves with this method, if we do not consider the length of passwords.

Regarding wireless connections, 67% of the respondents keep their Wi-Fi turned on all the time, but only 15% do this with Bluetooth, as apparently it is less used or considered to be more dangerous. Only 17% reported to use VPN, and 16% said they do not know the answer to this question, which suggest that they are not familiar with the term. So there is definite need to improve in this area to enhance safety.

Almost half of the respondents rely on automatic operating system updates (45%), and automatic application updates (41%). Around two third of them reported to periodically check default settings of apps (67%) and validate which apps can access their camera, location, microphone, files etc. (66%). This shows that this part of everyday security is better known among respondents and that around half of them

are familiar with the advised measures. 44% of the answers confirmed the usage of firewalls and antivirus, which is higher than expected in my opinion. My previous assumption was that those who are experienced in IT are more likely to use these kind of support, but the distribution of answers was steady and they didn't suggest any kind of relation. I also examined if any of the above responses can be linked to age, but surprisingly, from this survey at least, age differences could not be shown, and older respondents were just as up to date and informed as their younger counterparts.

To the last section of the proposed countermeasures I demonstrate three questions. The first was about if the respondents' social media profile is public. In total, 31% said yes to the question, interestingly, a higher proportion of male respondents share their profile publically. This is probably due to attempted courtship initiations from unsolicited sources via social media. Remarkably, 8% of the respondents said that they think banks and other service providers can ask them to provide their personal data through emails (with links for example), and further 2% is unsure about the answer. 3% confirmed that they would also open attachment from unknown sources, further 6% reported that they are not sure if they would do that. This is an important attack surface and these answers show that there is always room for improvement is this area, but generally people are aware of this kind of threat.

5. Summary

This article's aim was to point out that corporate security is in the hands of the employees' as well, not just employers'. The weakest link in corporate security may be the person, but we could see that risk can be reduced in countless smaller ways. The first step towards prevention and risk reduction is identifying possible attacks, which I introduced at the beginning of this article. This was followed by a series of practice-oriented recommendations aimed at tackling different areas of threats, which can be followed to improve individual and corporate security. They can help us to stop attackers with malicious intent to get to our personal data, or through us, to our company and its data as well. I also introduced an online survey which aimed to examine the current situation and attitude towards practical security among peers. In summary, it is visible that there are points which are more known than others, but from the open ended questions and comment section, I was able to see that generally respondents are well informed and educated in this field and that they consider it as part of their normal, everyday life. There always will be room for improvement, but this can be filled for example from employers' part with education and awareness raising programs. Large companies usually provide high quality education in these areas to their employees, but sometimes they do not emphasize that their personal, out-of-work life can have a major impact on the life of the company.

Bibliography:

- ANDÓ, G.: Minden, amit a GDPR-ról tudni érdemes; kozlekedesvilag.hu, 30 04 2019. https://www.kozlekedesvilag.hu/2018/08/24/minden-amit-gdpr-rol-tudni-erdemes/ (downloaded: 06 October 2019)
- ANDRE, L.: 51 Important Cybercrime Statistics: 2019 Data Analysis & Projections; FinancesOnline, 02 01 2019. https://financesonline.com/cybercrime-statistics/. (downloaded: 07 October 2019)
- Check Point: Checkpoint – CHECK POINT SANDBLAST MOBILE; 25 11 2018. https://www.checkpoint.com/downloads/products/sandblast-mobile-datasheet.pdf. (downloaded: 20 September 2019)
- GDPR Key Changes; 21 04 2019. https://eugdpr.org/the-regulation/ (downloaded: 10 July October 2019)
- ENISA: ENISA Threat Landscape Report 2018- 15 Top Cyberthreats and Trends; European Union Agency for Network and Information Security (ENISA), Athens, 2018.
- HILDENBRAND, J.: Android Central- What is sideloading; 02 02 2012. https://www.androidcentral.com/what-sideloading-android-z. (downloaded: 20 September 2019)
- HIGHFIELD, V.: The top ten password-cracking techniques used by hackers," 26 06 2018. https://www.alphr.com/features/371158/top-ten-password-cracking-techniques. (downloaded 06 October 2019)
- KASPERSKY: Kaspersky – What is DNS Cache Poisoning or Spoofing?; 09 10 2019. https://www.kaspersky.com/resource-center/definitions/dns. (downloaded 09 October 2019)
- KOVÁCS, L.: Kiberbiztonság és -stratégia, Budapest: Dialóg Campus Kiadó, 2018.
- KOVÁCS, T. –MILÁK, I.– OTTI, C.: A biztonságtudomány biometriai aspektusa; Pécs, 2012.
- MITNICK, K.– VAMOSI, R.: The art of invisibility, New York: Hachette Book Group, 2017., p. 19
- MITNICK, K. – SIMON, W.: A legendás hacker – A megtévesztés művészete; Budapest, Perfact-Pro, 2002.
- MORGAN, S.: Cyber Security Ventures- 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics; Cyber Security Ventures, 06 02 2019. https://cybersecurityventures.com/cybersecurity-almanac-2019/ (downloaded: 30 September 2019)
- Rapid7, "Rapid7-Man-in-the-Middle (MITM) Attacks; 08 10 2019. https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/. (downloaded: 08 October 2019)

- ROUSE, M.: Search Networking – VPN (virtual private network); Search Networking, 01 08 2019. https://searchnetworking.techtarget.com/definition/virtual-private-network. (downloaded: 30 September 2019)
- SAMANI, R. –DAVIS, G.: McAfee Mobile Threat Report Q1, 2019; 01 01 2019. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf. (downloaded: 27 October 2019)
- STATT, N.: The Verge- This illicit iPhone app store has been hiding in plain sight; 20 February 2019. https://www.theverge.com/2019/2/20/18232140/apple-tutuapp-piracy-ios-apps-developer-enterprise-program-misuse. (downloaded: 30 September 2019)
- TechJury – 33 Eye-Opening Cybercrime Statistics to Help You Protect Your Business in 2019; TechJury, 07 06 2019. https://techjury.net/stats-about/cybercrime/. (downloaded: 01 October 2019)

SÁNDOR MAGYAR PhD

THE INTERFACES OF IT OPERATION, DEVELOPMENT AND CYBER SECURITY, APPROACHED FROM THE POINT OF VIEW OF TECHNICAL TOOLSETS

Abstract

The world is increasingly moving in the direction of digitalization. The increased number of IT tools poses an increased threat both in operation and in cybersecurity. It is indispensable to comply with the rules set by cyber defense, and to serve the areas of operation, development in an appropriate way. The study of the topic shows that the set of tasks of developers and operators in the IT area as well as in the cyber defense mission systems, in many cases overlap each other. The domestic and international literature does not contain sufficient recommendations; therefore, looking at this from the point of view of cyber defense, it is appropriate to define the boundaries of the areas precisely.

***Keywords*:** IT operation, IT development, cyber defense, cyber security, IT task delineation

Our daily life is increasingly connected to the world of the Internet, where we can handle our correspondence, banking operations, shopping, and social relationships. The Internet of Things[1] provides us opportunities to have access to many services, which can increase our efficiency, both at individual and company level. Nowadays, society is moving more and more dynamically towards digitalization and relying on computer technology.[2] One of the drivers of the development has been the increased efficiency of the support services of ICS (Info-Communication Systems).

It is a technical feature that more and more devices are connected and communicating with manufacturers and operators over the World Wide Web to improve the products, learn about user habits, organize and store them. The increased number of IT assets poses an increased threat as well, both for the operation and the cyber defense alike. The higher the number of IT devices in commerce and the more data they contain, the more interested the attacker will be.

The malicious codes, the proliferation of other threats, their consequences are gradually increasing the threat for the continuous availability of ICS.[3]

---

1 Internet of Things – IoT

2 Government Resolution No. 1035/2012. (II. 21.) on the National Security Strategy of Hungary, paragraph 31.

3 Government Resolution No. 1139/2013. (III. 21.) on the National Cyber Security Strategy of Hungary, paragraph 4.

Compliance with cybersecurity policies, and maintaining a high quality of support for areas of operation and development are essential if information security risks are properly managed within the organization.

The market sector and also the areas of state administration and public administration are increasingly reliant on IT development, on the ongoing services provided by operation. However, in recent decades, in the case of the systems created by IT developments, the main focus is on security, in addition to their operating and purpose functions.

For an organization, information and its knowledge base are considered to be one of the most important assets. Therefore, a breach of the confidentiality, integrity and availability of data can result in significant material, reputational, operational, and other organization-specific damage. In order to avoid this, and in order to achieve efficient operation, it is important to coordinate both technological and administrative information security measures, and to design, develop and operate the three areas mentioned in the title in a coherent, complex system.

The above is also formulated by the National Cyber Security Strategy of Hungary[4], which states: *"In addition to external damage, there is also the risk that the operational security regulations of information and communication systems that are components of cyberspace are not well organized."*

The areas of IT operation and development often exhibit overlaps with cyber defense activities. In the various organizations, this may possibly be due to the fact that cyber defense grew out of IT operation, keeping the operator's mindset. An in-depth study of the topic points out the fact that the tasks of developers and testers of IT area often overlap each other. The domestic and international literature does not contain sufficiently appropriate recommendations; therefore, examining these, from cyber defense aspects, is justified to define the exact boundaries of the area.

Legal regulations[5] specify the information security requirements in detail, but do not provide an exact requirement, only guidance on the delineation of tasks. They do not make specific recommendations on conflicts of interest, either. As an example, Act L of 2013 on the electronic information security of state and local government agencies (hereinafter: IS Law) does not include the resolution of the conflict of interest of an official in charge of electronic information security being subordinate to the IT operating organization.

There are only minor recommendations for standards, but those working in the field would need to have more robust task delineation.

Naturally, in this paper I look at IT, development, operating and cyber defense activities of organizations, where these areas are assigned to separate organizational

4 Government Resolution No. 1139/2013. (III. 21.) on the National Cyber Security Strategy of Hungary, paragraph 4.

5 Act L of 2013 on the on the security of electronic information of state and local government agencies and its implementing regulations, Act CLV of 2009 on the Protection of Classified Information and its Implementing Regulations.

components. In the case of small organizations where the three areas belong to one server unit – possibly with a serving staff of a couple of employees – it is impossible to define task delineation, since in many cases, the same person performs the administrative, development and, in addition, cyber defense tasks well.

For each of the three different areas, a specific set of procedures should support the activities. It is important that although all three areas are involved in close cooperation their resources differ, in addition to their document systems. These include regulatory environments, hardware and software environments, human resources, or financial resources. For example, it is not worth comparing a developer software with a system management solution.

The development - which also includes modernization, the creation of new capabilities - needs to be supported by substantial planning and risk analysis.[66] The PDCA[7] cycle, in which the process approach is a basic expectation. Government Resolution No. 1838/2018 (XII. 28.) on the Network and Information Security Strategy of Hungary also includes *"a fundamental precondition of the effective protection against cyber-attacks is that the development of quality assurance processes is given a marked role in the planning of IT developments, as well as the definition and measurement of cyber security criteria".*

During operation, accurate knowledge of system status, configuration, and change tracking are essential. "*Operation covers the whole system. It includes maintenance of hardware, software, communication devices, data storage devices and configuration management procedures for these devices. "*[8] In case of IT system received from development, documented and tested, it is expedient to think along the appropriate standards such as the ISO 29119 standard[9] which facilitates creating a common language.[10]

Continuous operation and availability are the responsibility of the operator and are always accountable for them. If a person who is not a member of the development organizational unit is capable of implementing system-wide interventions – for example someone who is a developer whose earlier authorizations survived – may often result in problems due to lack of an appropriate level of administrative thinking, lack of up-to-date documentation. Without centralized change management, finding the source of the incident (possibly, problem) and restoring the original status is slow and difficult.

The legal background is more elaborated in the area of information security and cyber defense, but it is not regulated in the delineation of IT operation, development and cyber defense. For want of "rigorous" legal regulations, the area of operation and development depends on the attitude of the organizational leaders. Organizational

---

6 András HOLTAI, Sándor MAGYAR, Béla PUSKÁS: The Boundaries of IT Development and Operations, Reconnaissance Review 2016/1. pp. 191-203.

7 PDCA – Plan-Do-Check-Act.

8 Lajos MUHA – Csaba KRASZNAY: Security Management of Electronic Information Systems, Curriculum, NKE, 2018.

9 ISO/IEC/IEEE 29119 Software Testing Standard

10 András HOLTAI, Sándor MAGYAR, Béla PUSKÁS: General Issues in IT Operations, Reconnaissance Review 2015/4. pp. 91-102.

culture in certain organizations, the individuals' ability to assert their own interests can greatly influence the hierarchy of the areas and often generate duplication of tasks or irresolvable conflicts.

The areas of IT operation, development and cyber defense interact with each other. In case of vulnerabilities that occur in ICT systems, problems are hard to resolve for want of accurate documentation. It presents a major risk if knowledge of the system only exists in the mind of one particular IT expert, without appropriate documentation, whether we are talking about development, operation or security areas, there is a high risk once that particular person quits his job or is off sick.

However, the task system of the three areas may, in some cases, conflict. The main task of the operation is to ensure the availability of the electronic information system to the users. Cyber defense and information security must ensure confidentiality and integrity. However, there may be extreme cases where the two are in complete conflict with the other, in which the manager above them has to decide which area's proposal to implement. This is very rarely the case, but in an extreme case, when for example the mail server is under virus attack, a possible decision of cyber defense would be to shut down and reinstall the server from a backup to stop the further spread of viral infection as soon as possible, while the operation area is responsible for the continuous maintenance of operation, service in support of an operation where human life could be on the line. Thus, the leader, considering the done damage and the risks, will have to make his decision.

Among the areas of operation and cyber defense, it must be clarified in the SLA[11] which party provides what to the other party. This is important in the procedural framework for troubleshooting the earliest possible error event.

The data stored in the info-communication system can be protected with technical tools, solutions, software, regulations against external threats. Most of the technical solutions are installed at the access points, hence the term "border protection".

In case we use our devices for protection at home or in a SOHO[12] environment we still need to protect them. The personal computers, laptops, tablets, and mobile phones may contain (in fact, in most cases they do contain) personal data (such as images, user name and password combinations, banking data etc.) and therefore, it is mandatory to install anti-virus software on them that already includes firewall features. Just as in the case of managing operation systems, it is advisable to set the download of the security updates to automatic update in the appropriate virus protection systems, in order to keep the antivirus definitions up to date.

Systemic thinking is of paramount importance in the field of information technology. Devices communicate within a network, interacting with one another. Many IT devices have security features. Port security in the switches, ACLs[13] in the

[11] SLA – Service Level Agreement
[12] SOHO – Small Office-Home Office - Home (Small Business) Use
[13] ACL – Access Control List

routers, encryption and SSID[14] concealment, etc. in the WIFI[15] networks can be mentioned as examples.

In the rest of this paper, I look at IT devices performing major IT and IT security, or even multiple functions to explore the issue of interfaces. While describing the functions of the devices, I will be exploring functions as possible areas of overlaps. It is important to emphasize that the issue of responsibility in case of joint operation may result in the area-specific experts mutually pointing their fingers at each other, which must be avoided, highlighting cases where system administrator level access is granted to several areas at the same time.

The following devices, sub systems are always part of a complex system, understood as a whole, where their impact on the security of the system is strong.

Firewall tools

In order to connect our electronic information system with other systems, it is necessary to install interface protection devices, such as a firewall, at the connection points.

Traffic passing through firewalls is scanned and the data packets coming through the port from the appropriate IP[16] address may be allowed to pass through or may be banned. In many cases, the internal regulation of data traffic may be justified, therefore we can distinguish between internal and external firewalls. Firewalls can have software and hardware solutions, and manufacturing companies in the IT security market offer numerous products for both.

Routers can also be used as a firewall, where by using ACLs you can enable or disable IP addresses. Routers are typically part of IT operation, and their firewall rules on them are set by network (routing-switching) professionals.

There are a number of issues that can arise from the delineation of tasks. If, for example, we speak about a software firewall, the firewall software runs on an IT device that needs to be serviced by IT operation. That is, operation ensures the following throughout the life cycle of the device:

– updating the basic operating systems;
– updating virus definition databases;
– making backups for required resets and digital forensics[17] activities.

The situation in which the white and black lists on the firewall are not, or not only, set up by the operation, the following question arises: which organizational unit will be responsible for checking the proper settings?

14 SSID – Service Set Identifier
15 WIFI – WIFI Wireless Communication
16 IP – Internet Protocol
17 Digital Forensics – investigation of computer-related crimes

Proxy servers

A special kind of firewall is the proxy server that makes communication between the external and the internal network possible, by communicating on behalf of the internal workstations.

Its useful feature is that it can include content caching that helps clients perceive network traffic faster.

Proxies may be able to regulate their own network traffic by filtering content based on a set of rules and protecting the network, in which case the IP address of the proxy is displayed on WAN[18] side.

There are several types of proxy servers. The anonymous proxy, as its name suggests, provides the user with anonymity. Anonymity on the Internet is achieved by using TOR[19], for example, which also hides the computer behind a different IP address.

The operation of proxies mainly belongs to area of responsibility of IT, but cyber defense also plays a part in working out the best proposal in the area of securing information.

New generation firewalls

IT attacks have undergone significant development. The firewall protection mechanisms mentioned above, which check the data packages and enable or disable them no longer provide adequate protection in themselves these days, so it has become necessary to extend their features. There are an increasing number of applications employed by users that use different, often variable, ports. Encrypted channels have become a part of everyday life, and this is why there is a need for real-time application-level monitoring, with real-time intervention, even automatically.

Intrusion detection systems[20]

Intrusion detection systems also respond to the threats of today. In the case of firewalls, traffic filtering is implemented, but operators, cyber defense experts do not receive notifications of harmful content being blocked or content deemed harmful. In the event of intrusion detection, an alarm is triggered, which can trigger event-management if necessary.

For efficiency, you run a database containing a large number of rules and samples to filter out harmful content.

---

18 WAN – Wide Area Network

19 TOR – The Onion Router. This system allows an anonymous presence on the Internet and provides a connection to the hidden Internet

20 Intrusion Detection System – IDS - intrusion detection system

Intrusion prevention systems[21]

Today's challenge is protecting corporate, personal, classified information. Like IDS, IPS also detects harmful content, but in addition to its alert function it also has a preemptive and preventive function. IPS also performs a deep level analysis of traffic at the data packet level, but is able to block unwanted traffic. In addition to firewall functions, it can filter out threats using signatures and rules in your database, like an antivirus software, for example.

Bait systems[22]

One of the questionable tools in the interface between cyber defense and IT operation is the bait system (hereinafter referred to as "honey pot").

The device is actually a trap, which is a sensor system that appears to be an important device in the electronic information system and generates an alarm for a monitoring terminal. As the honey pot has no user end function in the network any requests, queries addressed to it suggest malicious intent.

They can be used on any wired or wireless network. Even phones with cellular Internet traffic, with some pre-installed sensor systems, can perform a honey pot function, which can be used to filter out malicious IP addresses, for example.

Uniform protection against threats[23]

The objective of the UTM systems is, beyond the traditional firewall function, to perform virus - and intrusion protection tasks as well. The devices also include VPN[24] support options. It has the advantage of being able to perform WEB filtering at the application level and also support the protection against data leakage.

Complex servicing of the above functions can provide more effective protection against threats, when enforcing the interface protection tasks of electronic information systems.

Log collecting systems

The IT area and the area of cyber defense operations cannot do without the collection and analysis of log files.

The IT devices, whether they are clients, servers, network devices, interface protection devices, and the services running on them, store their activity assigned to logging.

---

21 Intrusion Prevention System – IPS - system to prevent intrusion
22 Honey Pot – bait systems
23 Unified Threat Management – UTM - Unified protection against threats
24 VPN – Virtual Private Network – VPN

The availability of real-time log entries in the IT infrastructure is essential for efficient IT operation and event handling.

As required by applicable law: *"The security configuration of the system includes the logging features that enable security breaches to be investigated when security incidents are suspected and when a breach of security is suspected."*[25]

The operation of log collection systems also raises issues of delineation of functions. Logging, log analysis is done on some IT device (it can be a workstation, a server, a network active device). The basic operation tasks, whereby I mean the updates (firmware, operating system, and virus-definition database) must always be done by the IT service organization. However, the issue of who shall manage the special log collection and analysis software at administrator level may be agreed between the cyber defense and operations. There are two possible solutions:

- cyber defense tells operation what kind of log data is needed and must be provided by the operation;
- cyber defense sets the log collection data that it can retrieve independently from the system.

Both solutions require organization-specific, multi-step fine-tuning.

The issue of saving and deleting log data is always a particularly sensitive area. However, this is the basis of the activity in event-management and these data will serve as evidence of subsequent risk analyses and accountability requests.

Virus protection systems

There are many virus filtering and antivirus software programs on the market. In order to protect our system from malicious code, we need to run an antivirus system. Unfortunately, antivirus systems alone are not suitable for protection against the more sophisticated APTs.[26]

Examining the antivirus systems in terms of interfaces, it can be stated that it is a very important area. In the electronic information system, a virus hit is an event that both the operation and the cyber defense organization must respond to.

For the operational side, the responsibility is countering malicious attacks through prevention, disinfection, providing evidence and support for cyber-defense, and the responsibility of cyber defense is to identify the attack vector, which can be:

- incident occurring via external media/data storage device;
- malicious code from a malicious website;
- accessed by email;
- connecting an unauthorized device to the system;
- intentional attack by an authorized user.

---

[25] Subsection (1) of Section 35 of Government Decree 161/2010 (V.6.) on the Electronic Security of Classified Information and on the Authorization and Regulatory Oversight of Encryption Activities

[26] APT – Advanced Persistent Threat

Virus protection systems are increasingly advanced. They are capable of automatic responses, which include the automatic deletion, quarantining and identification of suspected malicious intruder. They send reports and alarms about their activities, so 24/7 monitoring centers are required for event management.

They can be updated manually, automatically, which can be classified rather as operating activities. Also, for antivirus systems, the principle that the operator performs day-to-day operations, according to the regulatory activities defined by the cyber defense organization, must be adhered to. The results will be notified to the cyber defense team. It is important to determine that updates are downloaded automatically, when online and the procedure of "take on board all updates blindly", when offline is asserted within the organization, or updates are tested after installation and verified, ("fixing bugs") and a more secure version be used locally, in the Rules of Procedure.

For example, if the cyber defense area were to set and operate, with full administrator rights, the virus protection system, in the case of the audit, the official performance of the tasks of the event would stay within the organizational unit.

Within an organizational unit – which can be at Department or Board of Directors level – for example, the parallel presence of both areas may cause conflicts of interest. In case of an incident, the cyber defense and the operation areas would report to the same supervisor/leader, so in many cases the problem – because of own interests – would stay within the organizational unit and would not be escalated to the appropriate level.

Endpoint protection solutions[27]

The endpoint protection systems in an enterprise environment are becoming more common. In many cases, they are an integral part of virus protection systems. The main task of the virus and firewall functions in addition to external peripherals (external storage devices, printers, etc.) is to monitor access rights and to control them based on authentication. The company systems more and more often prohibit the use of private data storage devices (USB devices) as a possible source of the spread of viruses. For example, in some systems USB devices will be added to the endpoint protection system based on their hardware serial numbers and only these registered (authorized) devices can be used in the electronic information system. When unregistered devices are connected, the port is shut down, no data is generated, or an alarm is generated in the system, which must be treated as an event until it is investigated. This could prevent mobile phones, MP3 players, from being connected to the system, even with the intention of charging their batteries. Furthermore, authorized devices can be linked to the user, which means that only the authorized user can use the devices linked to them. Even though the device is registered in the system, if it is not connected by its owner, it will be blocked and an alert will be issued.

On the operational side, the situation is similar to that of antivirus systems. In order to avoid conflicts of interest, it is advisable to ensure the IT operation the right

[27] Endpoint Protection System

to run the system, however, the system and / or operation should immediately notify the cyber defense of all incidents.

Vulnerability testing tools

An important phase of development is testing, which examines function and analyses security at the same time. Only reliable, proven hardware and software should be installed and used in IT systems.

When testing electronic information systems, many software programs can support security testing functions.

When delineating interfaces, logically new questions arise:

- Should vulnerability testing tools be used to protect the availability of system operation, or is it a typical cyber defense exercise that ethical h EQF be used for production?
- Can you use the vulnerability testing tools in both areas in a predefined way, because in both cases the goal is to make the system more secure?

In my opinion, operation should run the approved and already tested system and is not responsible for vulnerability testing, which is typically a cyber-defense task.

With regard to the development of systems, Károly Kassai has already outlined that*: "In the field of event-management, a technical change requiring development and organization is a widening of the topic of vulnerability investigations, and a central technical requirement with a strict field of data protection."*[28]

Harmful code[29] **Analytical Laboratory**

Signature-based anti-virus protection solutions do not provide complete security. More and more viruses are appearing, which means an increase in the size of antivirus databases, and more targeted attacks come to the forefront. In many cases, malicious codes that can appear on any physical infrastructure, such as mobile phones, laptops, etc. can only be found by analyzing their conduct, with the so-called "sandbox" technology.[30]

From the perspective of the delineation of responsibilities, the activity covers a cyber-defense task in the field of malware analysis; however, the system mostly operates in a virtual infrastructure, for which operating experience is also required, but it's not the task of IT operation, but of the cyber defense specialists who have the operator's knowledge and experience.

---

[28] Károly KASSAI: Cyberspace - Current Changes; PROFESSIONAL REVIEW, 2019 (1), pp. 116-134.

[29] Malware – harmful code

[30] Sandbox: An IT environment in which programs can be executed securely to test code and detect malicious software

New-generation attacks are now protected against sandbox technology, which means they don't work and run in a test environment. It is therefore a challenge to create a test environment that simulates the conditions of real life.

Source code analysis software

Source code analysis software allows detection of vulnerabilities, in addition to the functional area. The method is a static procedure. Source code analysis can also detect bugs that would only occur much later during operation and pose security risks. The activity should be classified in the field of cyber defense, which can advance the work of developers and operators.

Mobile device management[31]

Mobile device management is a set of security capabilities, security policies that can provide organizations or companies with adequate security to protect the data they protect on their mobile phones. MDM not only provides secure access to the corporate environment, enterprise data, but also to the management of a secure device.

It has basic security features, but it needs to be set up for operation. Here it should assert the principle that the cyber defense policy provides the required policies to operators, who implement the appropriate settings. which are validated from time to time by the cyber security area.

The above toolsets are in a constant state of change. The emerging technologies, such as machine learning, artificial intelligence, constantly shape the opportunities of the offensive and defensive sides. Artificial intelligence can make a significant difference by analyzing user interactions and network behavior.

The advancement of quantum computing brings with it an acceleration of computing capacity, which will also affect the defense and attack tools. In particular, encoding and encryption will be threatened by the development and penetration of quantum computing.

Conclusions

We must remember that our tools – that are parts of our daily life – are connected to a network, which can be used for purposes of attacks perpetrated in order to do harm, or achieve gains. The security methods must always be used (virus protection, firewall, passwords, etc.). Throughout the examples of many IT tools, this chapter shows that the interfaces are often blurred. However, you must always be aware of the areas of responsibility, control and accountability.

System administrator passwords for systems, devices, services are always the most protected pieces of information in systems. System-level access is provided to

[31] MDM – Mobile Device Management

the operator. It is worth considering how effective an electronic information system is if more than one organization has the highest access.

Another problem is that the purpose of the operation is to eliminate the incident and restore the normal operation as soon as possible, to record any clues for cyber defense. The cyber defense – by using its tools – reveals the story, makes recommendations to the risks elimination, in order to make sure that similar information security incidents do not happen again in the future, and restoring business as usual as soon as possible is not its primary concern. It is important to have the right control in all cases and not to have the double role of controller and controlled role within an organizational unit, because in this case, for example, incidents – resulting from malfunctioning that make the same leader look bad – will not be elevated to the appropriate level.

The basic element of efficient operation is the delineation of appropriate tasks and responsibilities, which must be included in the internal regulation of the organizations. There should be a clear delineation of functions and scopes of authority in IT operation, development and cyber defense.

It sometimes happens that the shortcomings of regulations are not recognized as a problem by the leaders responsible for an area.

Bibliography:

- Act L of 2013 on electronic information security of state and local government agencies.
- Act CLV of 2009 on the Protection of Classified Information.
- Government Resolution No. 1035/2012. (II. 21.) on the National Security Strategy of Hungary. Point 31.
- Government Resolution No. 1139/2013. (III. 21.) on the National Cyber Security Strategy of Hungary, paragraph 4.
- Government Resolution No 1838/2018. (XII. 28.) on the Strategy for the security of networks and information systems of Hungary.
- András HOLTAI – Sándor MAGYAR – Béla PUSKÁS: General Issues in IT Operations, RECONNAISSANCE REVIEW 2015/4. pp. 91-102.
- Andrew HOLTAI, Sándor MAGYAR, Béla PUSKÁS: IT development and operation interfaces, Intelligence Review, 2016/1. pp. 191-203.
- ISO IEC 27000 Standards
- ISO/IEC/IEEE 29119 Software Testing Standard
- Károly KASSAI: Cyberspace – Current Changes, PROFESSIONAL REVIEW, 2019 (1), pp. 116-134.

- Lajos MUHA – Csaba KRASZNAY: Security Management of Electronic Information Systems, Curriculum, NKE, 2018.
- Subsection Section Government Decree No. 161/2010 (V.6 :) on Electronic Security of Classified Information and on the Authorization and Supervision of Cryptographic Activity

SÁNDOR KISS – LAJOS ZÁHONYI

EXAMINATION OF THE HISTORY OF INFORMATION SECURITY - THE BEGINNINGS[1]

Abstract

Information security is based on three principles. One of the principles is that information should be intact, it should remain accurate, and should not be distorted. Second, the authorized user should always have access to the information and related values. The third principle is the question of authorization or confidentiality, meaning that only the eligible or authorized person should have access to the information.

The situation of information Security and its Relationship Tool Kits have changed a lot since the beginning of the 20th century to the present day and it can be stated that the culture of IT systems that has been gradually spreading from the end of the 20th century, has really brought to the forefront the need for stronger organization of information security. Yet, based on the above three principles, it is possible to follow this change taking place along evolutionary milestones and events.

In this study, I turn back to the beginning of the 20th century and along the three principles of information security, I would like to present one episode of World War I, the first really great global conflict, from a security science perspective. Due to the interdisciplinary nature of the study, it also covers areas of history and law, starting from a security science footing.

Keywords**:** information security, World War I., principles of information security, history of information security

[1] Special thanks to László VARGA for the pigeon!

Picture 1: In a war, the value of information can be measured in human lives[2]

History of Science Foundations

No discipline can exist without antecedents. All science is on the move, every science is looking for answers and thus evolving. These answers are built on each other and this raises new questions. Development is unstoppable. To better understand the problems of the present age, we must look back and learn from these answers. This is no different in the field of security science, either.

"The purpose of security science is to analyze the security functions of systems from the outset, and implement the security planning of the systems with as much detail as possible."[3] As technology advances over time, new and emerging information security challenges are emerging. It was a little over a decade ago that the ISO27001 information security system set of standards was published, which was then an appropriate regulatory response to the challenges of the age. In Hungary, the legislative system is also trying to pick up the pace that this development is causing. Regulatory forms, regulations and laws are constantly evolving throughout the world, including the European Union and Hungary.[4] If we examine the causal relationships, we can see that the safety device systems are constantly changing and adapting. The challenges of a given age are answered by the tools and technical standards of that age.

---

2 https://worldwar1historyfacts.weebly.com/ (downloaded 11 November 2019.)

3 KISS, Sándor: Óbuda University, Introduction to Security Technology 2019 p. 13.

4 See Act L. of 2013 on Electronic Information Security of State and Local Government Bodies; https://net.jogtar.hu/getpdf?docid=a1300050.tv&targetdate=&printTitle = (downloaded 14 November 2019)
The Directive on NIS Directive https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (downloaded 14 November 2019.)

Historically, the process of learning about security can be divided into four stages. These are:

- The first phase is the "age of innocence"[5] which preceded the industrial revolution; it denotes the 17th-18th centuries. A characteristic of this era is that man had not yet consciously addressed, measured or analyzed security problems in the today's sense. Natural disasters, catastrophes, and epidemics, but also the presence of war itself, was considered an accepted part of life. Although the conflicts of the age also forced answers to be given, but the answers, the devices and device systems could be considered more instinctive than conscious.This instinctive response is already evident in case of early man's "security tool", the dog, or in the response given to the spread of medieval epidemics.[6]
- The second phase is the "age of discovery "[7], which is the period between the arrival of the industrial revolution and the turn of the 19th and 20th of centuries. By this time, the importance of security had been recognized and theoretical foundations had already been developed. The technical sciences or medicine already had some tools on the basis of which the theoretical foundations were recorded and used. During this period, social development brought with it the need for security. With the use of new tools and technologies, people discovered security issues around themselves and took some initial steps toward resolving dangerous situations.
- The third phase is the age of "system security"[8], which can be recorded as a response to the explosive development starting from the beginning of the 20th century. It is characterized by a high degree of industrial development, the development of defense industry, the new technical achievements such as the evolution and spreading of the airplane, or later by the development of the space industry.
- The fourth phase is the age of "security science"[9], which already provides precise and meaningful answers to the advances in science and technology. One already recognizes the principles and contexts of security, develops one's own systems of tools, and uses these tools to develop answers, without regard to the fact whether they are different techniques or systems.

In terms of the historicity of science, this study represents the era of "system security" in the 20th century. One of the most significant conflicts of the first century - and its consequences - is the information security challenges of the World War I. At this age, there was a sharp leap forward in social terms, including industrial development, weapons and technical equipment. And looking at information security within security science, it can be considered a milestone in the evolution of information security. The tools of the old days are still present, but the advances of the modern age are on the doorstep, which also carry the risks of information security. The answers are still

---

5 Sándor KISS: On the History of the Development of Security Technology; Military Engineer X. Volume 4 - December 2015. p. 26.

6 Endre SZŰCS: The "security tools" of the caveman; Military Engineer XI. Issue 4 - December 2016. pp. 216-221.

7 KISS op. cit. p.26.

8 Ibid. p. 27.

9 Ibid. pp. 27-28.

rudimentary, and can be understood rather from a social and legal point of view. This is the "dawn" of information security, from which we will, in almost 100 years, reach the establishment of the National Cyber Security Institute.

Introduction

"The information security situation is peculiar, present at the same time in every area of the organization, and even the proper design and operation of its conditions goes well beyond the safe management of information. It means the regulation, conduct, utilization and control of all resources, staff, assets, information systems, and other assets of an organization. Its management is the responsibility of senior management."[10]

Information security is based on three pillars. The first is to keep the information intact, accurate and not distorted, the second is for authorized users to always have access to the information and related values, and the third is to have authority for access or confidentiality, i.e. that the given piece of information should be accessible to the person cleared for access or authorized to have access to it.

Picture 2: Complexity of information security. You can learn from the past[11]

In light of these basic pillars I look at the tools and tool kits of about 100 years ago, and what responses were made with regard to the challenges and technological possibilities of the age when dealing with or preventing an information security "incident". In this study I consider an undesirable or unexpected unique or repeated

[10] Krisztián Gergely HORVÁTH: Understanding IT Security; CISA CISM Budapest, 2013 p. 13.

[11] https://www.tylercybersecurity.com/blog/fundamental-objectives-of-information-security-the-cia-triad (downloaded 11 November 2019)

event to be an information security incident[12] that jeopardizes operational activities and threaten the security of information.

"Pathology of Information" or incident in integrity

On 31 May 1916, the German Imperial Naval Fleet (*Kaiserliche Marine* in German) and the British Royal Navy (Royal Navy) fought in the North Sea the greatest naval battle in world history that posterity calls the Jutland Sea Battle.[13] [14] [15] The battle involved 151 vessels from the British side and 99 from the German side.

We are at the beginning of the 20th century. Although the military industrial achievements show a modern and advanced image, there are no cell phones, networks yet, and even the use of radio signals was not widespread or considered reliable.[16] Morse codes are already in use, but they are often not trusted given the war conditions. In the midst of this battle, David Beatty, the commander of the British Royal Navy, communicated with signaling flags that he believed to be the safest means of communication. This appearance of communication, on the other hand, was born in an earlier age and was part of its tool kit. This way of transmitting information should have covered a distance of 15-25 km at sea during battle. You can imagine how great a dysfunctional source of threat it was. In reality, it was virtually impossible to clearly identify the signals. This situation presented a clear possibility of information damage.

---

12 [ISO / IEC TR 18044: 2004] * MSZ ISO / IEC 27001: 2006 (3.6)

13 https://www.telegraph.co.uk/news/2016/05/31/the-battle-of-jutland-is-still-sending-signals-now/ (downloaded 10 November 2019)

14 http://www.rubicon.com/english/pages/1916_junius_1_veget_er_a_jutlandi_csata/ (downloaded 10 November 2019)

15 https://ng.hu/kultura/2016/06/01/jutland-1916/ (downloaded 10 November 2019)

16 http://jproc.ca/rrp/nro_his.html (downloaded 10 November 2019)

Picture 3: Failure to ensure information integrity gives rise to a series of misunderstandings

As a result, a series of errors, misunderstandings or "incidents" occur. The wrongly interpreted flag signals between the British fleet commander and his subordinates[17] resulted in the temporary separation of the fleet and thus the weakening of it and the appearance of salvos fired at the wrong time and at the wrong target.[18] [19] Due to information damage, inaccuracy and incompleteness, approximately 2000 people died on the British side. It is not without reason that the serial information problems typical of the Battle, are referred to by posterity - on the British side - only as “pathology of information.”

"For heaven's sake, stop it!" - Incident of availability

Availability is to ensure that a given and authorized or intended recipient of a piece of information purpose has access to that information and its added value when needed.

The way of delivering information and the protection of information greatly depends on the efficiency of the typical assets of the age. If one writes an e-mail

[17] https://www.history.navy.mil/our-collections/photography/technology/communications/flag-signals-and-semaphore.html (dowloaded 14 November 2019)

[18] https://www.iwm.org.uk/history/battle-of-jutland-timeline (downloaded 14 November 2019)

[19] https://www.iwm.org.uk/history/what-was-the-battle-of-jutland (downloaded 14 November 2019)

nowadays and assigns a clear and real recipient to it, the message will be delivered. Seen through our eyes today, it may seem strange to read that 100 years ago the homing pigeons, considered part of the tool kit, performed the function of delivery.[20]

"Post pigeon communication is based on the ability of some pigeon species, if properly flown, to fly home instinctively over long distances and after long periods of absence," writes a contemporary service regulation issued to the mail pigeon service.[21]

During World War I, mail pigeons were widely used by both the Entente and the Central Powers. Pigeons were one of the safest information tools in the age to ensure that the right piece of information is available. According to contemporary observations, 95% of messages sent by mail pigeons reached their destination. Even today, this is a serious achievement.

The United States entered World War I in 1917 and its troops were already involved in specific combat activities on the Entente's side in 1918. In October 1918 a battalion of the American army entered the Argonne forest, where the attack stalled because they were surrounded by the Germans. The fact of encirclement reached the US Army Headquarters, which ordered artillery bombardment to help the US attacks.

However, during the massive cannonade the artillery bombarded the positions of friendly troops because accurate information on the coordinates or location of their own troops is not available. This is the time when their last messenger pigeon will be launched with the following message:
"We are along the road parallel to 276.4. Our own artillery is dropping a barrage directly on us. For heaven's sake, stop it."[22]

---

20 Hungarian National Archives Military Pigeons in World War I http://mnl.gov.hu/mnl/nml/csak_a_legritkabb_esetben tagadja meg a szolgalatot (downloaded 08 November 2019)

21 Gábor KISS: Pigeons in the Austro-Hungarian Armed Forces during World War I, 26. 10. 2011. (downloaded 11 November 2019)

22 https://www.worldwar1centennial.org/index.php/communicate/press-media/wwi-centennial-news/1210-cher-ami-the-pigeon-that-saved-the-lost-battalion.html (downloaded: 08 Nobember 2018)

Picture 4: The availability cannot be regarded as self-evident – the homing pigeon is part of the contemporary tool kit, which made it possible for the information to become available.[23]

This messenger pigeon, called "Cher Ami" (Dear Friend), flew 25 miles in 25 minutes and delivered the message to US headquarters and after receipt of the message the cannonade was immediately stopped, saving the lives of some 200 American soldiers. Cher Ami was hit several times during her flight, losing one of her eyes and one leg. However, the message was delivered and became available. After recovery, the heroic messenger pigeon was awarded the French War Order, the Croix de Guerre. His stuffed body can still be seen at the Smithsonian Institute in the US.

Confidentiality - the disclosure of information

Ever since there is confidential information, all those who are not part of the confidentiality surrounding it have been trying to obtain it. Nowadays, in the world of IT systems, the issue of confidentiality can be interpreted in a complex way. On the one hand, it means the dedication of the rights of the information data asset, its protection, and the fact that this information shall only be accessible to authorized persons. In the days of World War I[24], the issue of confidentiality of information is also a very sharp point because when it comes to investigating actions to obtain information, it is not only a bad decision or the resulting human omission, not even a mistake or a defect in the tools or systems, but deliberate human behavior, a deliberate

[23] The Smithsonian, National Museum of American History https://www.si.edu/object/nmah_425415 (downloaded: 12 December 2019)

[24] BODA, József – REGÉNYI, Kund: History of Intelligence from Antiquity to the Present - Dialogue Campus Publisher Budapest, 2019. pp. 111-116.

violation of a rule, and a deliberate breach of a system of tools that results in a violation of the confidentiality of information.

Obtaining useful and relevant information in times of war is a key issue. Possession of this relevant information can affect the lives of thousands of soldiers. Today, wars are conducted in a quieter fashion. It takes no more than a company of well-trained hackers and they can virtually interfere in the lives of countries, societies and communities to have a lasting impact on posterity. One hundred years ago, there were also similar groups exerting influence, they were intelligence agencies.
At the outbreak of World War I, all major states already had military intelligence organizations which in the Austro-Hungarian Monarchy[25] was simply called the *Registry Office,* then known as *Evidenzbureau*.

Picture 5: Colonel Alfred Redl, „the Mole" – He was trusted for a long time due to his reliability and good ideas

By the end of World War I, the staffing level of the *Evidenzbureau* reached approximately 2,000 and Colonel Alfred Redl was Deputy Head of this organization from 1908 to 1912.[26] Redl himself, as a professional career officer, was, talented and full of good ideas at work. Ha earned enduring merits in the area of organization, wire-tapping (eavesdropping) and fingerprint identification.[27]

Colonel Redl worked in the Austro-Hungarian Military Intelligence for more than a decade and during this period he continued to provide sensitive information, especially to Tsarist Russia. Based on his actions, we can surely regard him as an

---

25 Szilárd SZABÓ: Central Military Reconnaissance and Defense Organization of the Austro-Hungarian Monarchy during the World War I; National Security Review 2018/Special issue pp.7-12.

26 ASZTALOS, Aladár: Spies in World War I, Anno Publishers, 2000. pp 18-33.

27 PAPP, Gábor: What We Didn't Know About Colonel Redl's Treason 22/07/2013. https://kulturpart.hu/2013/07/22/amit_eddig_nem_tudtunk_redl_ezredes_arulasarol (downloaded: 17 November 2019)

insider informant (mole) who was also made (in)famous by the media at the time. After a decade of organizational work, he was unveiled as a double agent in 1913. After he was caught out[28], Redl was given the opportunity to end his life with his own hands. The authorities, however, couldn't prevent "strictly confidential" key wartime operational information from getting into unauthorized hands. At the outbreak of the war, the Russian, Serbian and Italian parties all had relevant information on the operational deployment plans of the Monarchy. Redl did an effective job and as a result indirectly influenced the lives of hundreds of thousands of Hungarian soldiers.

One answer of the age: legal regulation

Nowadays, it is natural for us to install different security software when using our computers and to accept the privacy policies of software manufacturers and various websites in order to comply with information security rules. However, the use of information protection standards as a self-evident precaution was not the case in the beginning of the 20th century. Perhaps it can also be said that a complex interpretation of information security has not yet been called for. However, incidents in the modern sense did occur, so they seized the opportunities offered by the systems of the era to respond to incidents that had emerged. A universally widespread contemporary instrument was the introduction of written regulations. Standardization was still very rudimentary.[29] It is true that the establishment of the German Deutsches Institut für Normung (1917), the American National Standards Institute in the US (1918) and the French Commission Permanente de Standardisation (1918) can be considered to have taken place during World War I, but at the time it might have mostly affected areas of military and technical origin.

The tool of the age is literacy, which could formulate the problem and respond to a regulatory proposal. In most cases this was the legal regulation itself.

In the area of the monarchy, after the Great Compromise of 1867, a slow process was begun to extend the level of regulatedness of the state's operating order to ever greater areas. Laws and regulations were issued for all areas of life. In today's terms, we would look in vain for information security "keywords" in the regulations of the era, yet indirectly we can find significant regulatory requirements established in the light of the challenges of the age.

For example, the contemporary legal regulation, "Act V of 1878 on the Hungarian Criminal Code, the criminal acts and offenses"[30] provides guidance on how to deal with a breach of confidentiality as a principle of information security. Section 142

---

28 DRUSZA, Tamás – REGÉNYI, Kund – Addenda to the case of Colonel Redl, or the lessons of the Empire's most treacherous traitor still having an impact today; National Security Review 2018 Special Issue http://epa.oszk.hu/02500/02538/00026/pdf/EPA02538_nemzetbiztonsagi_szemle_2018_ksz_1_036-045.pdf (downloaded: 17 ovember 2019.)

29 ZELTWANGER Holger: A short history of standardization and CAN February 16, 2015 https://www.controleng.com/articles/a-short-history-of-standardization-and-can (downloaded 14 November 2019)

30 https://net.jogtar.hu/jogszabaly?docid=87800005.TV&txtreferer=94500007.TV (downloaded 14 November 2019)

describes the issue of infidelity and Subsection (5) of Section 144 and Sections 146 and 147 provide a clear definition of confidentiality. At these points, with the emergence of 'infidelity' as a concept, it defines a longer procedure in response to the then challenges of information security. Another noteworthy legal instrument considered as part of the contemporary tool kit is the “Act LXIII of 1912 on Exceptional Measures in times of War".[31]

The uniqueness of this law lies in the fact that it can be considered a sort of Business Continuity Plan (BCP) with the difference that in this case the level of organizational regulation is a state level regulation.

Contemporary auditors

As part of this study, I would like to briefly address who were the ones who reviewed these contemporaneous tool kits and who had the authority and relevant tools to respond to these information security incidents. Who were those who had the appropriate professional background in the field, were sufficiently independent to make objective proposals, and had sufficient evidence, solid information to give meaningful answers and proposals. Who can we call contemporary auditors.

The word "auditor" had a completely different meaning 100 years ago. Yet what we now know as auditor qualities had already existed. To our current knowledge, auditors were required to know[32] [33] [34] principles, procedures and techniques to be applied. They had to be clear about the correctness, accuracy, and reliability of the information they received. They had to be familiar with the regulatory environment, make comments based on evidence, be of the highest professional standards and be independent.

Considering all these qualities, we can consider the monarchs and rulers, the responsible statesmen of the era to be the leading auditors of World War I who are acting in their executive capacity. They were the ones who had all the qualities and privileges to influence the contemporary asset systems. Emperor Franz Joseph, as sovereign of the Austro-Hungarian Empire held regular meetings with the representative of the Evidenzbureau and the representatives of the states forming the Monarchy.

Although, as a ruler, he was directly involved in the affairs of his empire, yet the distanced "ruler" perspective from which he viewed matters was so far from the investigated areas that this aloofness alone ensured sufficient independence and he

---

31 https://net.jogtar.hu/getpdf?docid=91200063.TV&targetdate=&printTitle=1912.+%CA9vi+LXIII.+t%C3%B6rv%C3%A9nycikk&referer=1000ev (downloaded 14 November 2019)

32 Dr. Attila GUTASSY – Ferenc Nimród GUTASSY: Quality Management for Everyone; Raabe Klett Education Consulting and Publishing Ltd. 2018. pp. 274-276.

33 https://www.poligont.hu/searchbase/security/az-audittal-connection-seconds/ (downloaded 14 November 2019)

34 https://www.tankonyvtar.hu/en/content/tamop412A/2011-0089_11_kornyezetiauditalas/ch17s04.html (downloaded 11/14/2019)

was well aware of the regulatory environment, he could act with professionally due care and diligence.[35]

Conclusion

Like all sciences, the field of security science is constantly evolving. This is especially true in the field of information security within security science. This study, with some peculiar examples, made an attempt to present the events of this period in history during World War I and the incidents that occurred in that period of time that had a major impact on the development of information security. This effect can also be considered as a kind of milestone in terms of the information security situation and its systems of relationship tools.

Examining the three principles of information security, we have seen that responses to the challenges of that age have produced the potential of the tools of the age, which subsequently forced an actual future development in the field of information security.

Respect for the heroes, respect for our great-grandfathers and great-great-grandfathers!

Bibliography:

- ASZTALOS, Aladár: Spies in World War I, Anno Publishers, 2000. pp 18-33.
- BODA, József – REGÉNYI, Kund: History of Intelligence from Antiquity to the Present - Dialogue Campus Publisher Budapest, 2019. pp. 111-116.
- DRUSZA, Tamás – REGÉNYI, Kund – Addenda to the case of Colonel Redl, or the lessons of the Empire's most treacherous traitor still having an impact today; National Security Review 2018 Special Issue http://epa.oszk.hu/02500/02538/00026/pdf/EPA02538_nemzetbiztonsagi_szemle_2018_ksz_1_036-045.pdf (downloaded: 17 ovember 2019.)
- GUTASSY, Attila Dr. – GUTASSY, Ferenc Nimród: Quality Management for Everyone; Raabe Klett Education Consulting and Publishing Ltd. 2018. pp. 274-276.
- HORVÁTH, Krisztián Gergely: Understanding IT Security; CISA CISM Budapest, 2013 p. 13.
- KISS, Sándor: On the History of the Development of Security Technology; Military Engineer X. Volume 4 - December 2015 pp. 26-28.

[35] Szilárd SZABÓ: The Evidenzbureau. Reconnaissance organization of the Austro-Hungarian Monarchy 1850-1919. Law Enforcement History Booklets XXV.f. (2015) Issue No. 43-46. p. 130 https://www.researchgate.net/publication/329789362_Az_Evidenzbureau_Az_Ostrak-Hungarian_Monarchy_First_Organisation_1850-1919 (downloaded: 17 November 2019)

- KISS, Sándor: Óbuda University, Introduction to Security Technology 2019. p. 13.
- KISS, Gábor: Pigeons in the Austro-Hungarian Armed Forces during World War I, 26. 10. 2011. (downloaded 11 November 2019)
- PAPP, Gábor: What We Didn't Know About Colonel Redl's Treason 22/07/2013. https://kulturpart.hu/2013/07/22/amit_eddig_nem_tudtunk_redl_ezredes_arulasarol (downloaded: 17 November 2019)
- SZABÓ, Szilárd: Central Military Reconnaissance and Defense Organization of the Austro-Hungarian Monarchy during the World War I; National Security Review 2018/Special issue pp.7-12.
- SZABÓ, Szilárd: The Evidenzbureau. Reconnaissance organization of the Austro-Hungarian Monarchy 1850-1919. Law Enforcement History Booklets XXV.f. (2015) Issue No. 43-46. p. 130 http://jproc.ca/rrp/nro_his.html (downloaded 10 November 2019)
- SZŰCS, Endre: The "security tools" of the caveman; Military Engineer XI. Issue 4 - December 2016. pp. 216-221.
- ZELTWANGER, Holger: A short history of standardization and CAN February 16, 2015 https://www.controleng.com/articles/a-short-history-of-standardization-and-can (downloaded 14 November 2019)
- https://www.researchgate.net/publication/329789362_Az_Evidenzbureau_Az_Ostrak-Hungarian_Monarchy_First_Organisation_1850-1919 (downloaded: 17 November 2019)
- https://net.jogtar.hu/jogszabaly?docid=87800005.TV&txtreferer=94500007.TV (downloaded 14 November 2019)
- https://net.jogtar.hu/getpdf?docid=91200063.TV&targetdate=&printTitle=1912.+%CA9 vi+LXIII.+t%C3%B6rv%C3%A9nycikk&referer=1000ev (downloaded 14 November 2019)
- https://www.history.navy.mil/our-collections/photography/technology/communications/flag-signals-and-semaphore.html (dowloaded 14 November 2019)
- https://www.iwm.org.uk/history/battle-of-jutland-timeline (downloaded 14 November 2019)
- https://www.iwm.org.uk/history/what-was-the-battle-of-jutland (downloaded 14 November 2019)
- https://www.tylercybersecurity.com/blog/fundamental-objectives-of-information-security-the-cia-triad (downloaded 11 November 2019)
- https://worldwar1historyfacts.weebly.com/ (downloaded 11 November 2019.)
- https://www.telegraph.co.uk/news/2016/05/31/the-battle-of-jutland-is-still-sending-signals-now/ (downloaded 10 November 2019)

- http://www.rubicon.com/english/pages/1916_junius_1_veget_er_a_jutlandi_csata/ (downloaded 10 November 2019)
- https://ng.hu/kultura/2016/06/01/jutland-1916/ (downloaded 10 November 2019)
- https://www.worldwar1centennial.org/index.php/communicate/press-media/wwi-centennial-news/1210-cher-ami-the-pigeon-that-saved-the-lost-battalion.html (downloaded: 08 Nobember 2018)
- https://www.poligont.hu/searchbase/security/az-audittal-connection-seconds/ (downloaded 14 November 2019)
- https://www.tankonyvtar.hu/en/content/tamop412A/2011-0089_11_kornyezetiauditalas /ch17s04.html (downloaded 11/14/2019)
- The Directive on NIS Directive https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (downloaded 14 November 2019.)

Legislation:

- Act V of 1878 Hungarian Criminal Code on Crimes and Offenses
- Act L of 2013 on Electronic Information Security of State and Local Government Bodies
- Act LXIII of 1912 Article on exceptional measures in the event of war

AUTHORS OF THIS ISSUE

- **ÉVA BEKE** is a PhD student at the Óbuda University Doctoral School on Safety and Security Sciences, Budapest;
- **SÁNDOR BABOS** is a PhD student at the Public Service University, Budapest;
- **DÓRA DÉVAI** is a PhD student at the Public Service University, Budapest;
- **SÁNDOR KISS** is a Colonel (R) and a university docent at Óbuda University Doctoral School on Safety and Security Sciences, Budapest;
- **SÁNDOR MAGYAR** is an IT and cyber security expert;
- **LÁSZLÓ SIMON** is a PhD student at the Public Service University, Budapest;
- **KATA REBEKA SZŰCS** is a PhD student at Óbuda University Doctoral School, Budapest;
- **LAJOS ZÁHONYI** is a PhD student at Óbuda University Doctoral School on Safety and Security Sciences, Budapest.

EDITORS OF THIS ISSUE

- **KÁROLY KASSAI** is working at MNSS;
- **JÓZSEF KIS-BENEDEK** is an independent terrorism and security policy expert;
- **BÉLA PUSKÁS** is a cyber security expert.

CONDITIONS FOR PUBLISHING IN THE NATIONAL SECURITY REVIEW

Requirements to be met by the writings

Ethical requirements:

- the writing has not been published yet elsewhere in its present form;
- it represents the author(s)' exclusive literary property, which is verified by the author(s), through his signing an author's declaration;
- it must be annotated with correct references that can be easily checked up;
- as well as with appropriate bibliographical information (including the literatures referred to, the list of Internet material, together with the date of downloading);
- it can reflect the author(s)' own opinion, which does not need to necessarily coincide with the Service's standpoint.

Content requisites:

- we publish in our reviews – in conformity with their nature – those scholarly writings (studies, essays and articles) that relate to home defense, first of all to military science, national security, intelligence, reconnaissance, military security and security policy;
- the writing must be logically worded, easy to survey, coherent, relevant and well-arranged;
- the formulation of the author(s) own concept needs to be clear, his (their) conclusions have to be well-founded, supported by clear arguments and data.

Formal requisites:

- the size of the manuscripts cannot possibly exceed the space of one author's sheet (40,000 characters or 20-21 pages); written by Times New Roman 12 letters, 1.5 spacing; the pictures and graphics prepared in an easy to be processed format (.jpg or .tif), on electronic data carrier (CD), accompanied by a printed hardcopy. All this has to be taken into account when the author(s) sends his (their) writing to our address;
- however, the manuscript can be sent also by Internet to the following E-mail addresses: natsecreview@gmail.com (National Security Review). It is necessary to attach to the manuscript the author(s)' name, rank, position, sphere of activity, permanent address, phone number and Internet address;
- we pay royalty for the accepted and published writings, based on the contract of agency, in harmony with the relevant HDF regulations and according to our available financial resources;
- the Editorial Board has the manuscript revised in every case by the Service's competent, officers (with academic degree) or other experts;

- the Editorial Board preserves the right – taking into consideration the advisers' recommendations – to deny (without justification) the publication of those works that have proved to be ill-qualified to appear. However, it does not send back such writings and does not hold them either;
- everyone is entitled to publish in our periodicals, if the Editorial Board assesses his writing – on the basis of ethical, content and formal requirements – to be suitable for being published in our reviews and on the Internet. The Board holds until the end of the given year those writings that have been accepted, but not published. If the author wishes, we are ready to return his writing to him;
- the author has to enclose in his work an "Abstract/Résumé" maximum in 10-12 lines, in Hungarian and also in English;
- he also has to provide at least 3-5 keywords in Hungarian and English;
- we kindly ask the author to send us also the correct English title of his writing.

Formal requirements of academic communications

Our periodical publishes exclusively such studies that are provided with appropriate references and are prepared on the basis of the MSZ ISO 690 design standard.

The author has to attach to his communication:
- NAME OF THE AUTHOR, (his rank);
- TITLE OF HIS WRITING (in Hungarian and English);
- ABSTRACT/RESUME (in Hungarian and English);
- KEYWORDS (in Hungarian and English);
- AUTHOR'S DECLARATION.

Bibliographical reference

We kindly request the author to apply the usual numbered references, with the method to be found in "the Bibliographical references, (Bibliográfiai hivatkozások) MSZ ISO 690. p. 19-20".

If the author fails to use this method, we send back his writing for re-elaboration.

Citations

If the author has citations within the text, he has to mark them with raised numbers (superscripts) in the order of their appearance, immediately following a passage of research information. At the foot of that same page, a note beginning with the corresponding number identifies the source of information.

First citations

If we have a list of citations (bibliography), the first citation has to comprise at least: the author's name, his full address, the page-numbers of the citation, in such a way to be easily identified in the list of biographical references.

Examples:

1. Jenő KOVÁCS: Roots of the Hungarian Military Science, ideological problems of its development. p. 6.
2. Tibor ÁCS: Military culture in the reform era. p. 34.
3. Lajos BEREK: Basic elements of research work in Military Science. p. 33.
4. www.globalsecurity.org/army/iraq (downloaded: 19 04 2012)

List of biographical references (biography):

We have to fill the list by arranging the authors' name in alphabetical order.

Examples:

1. Tibor ÁCS: Military culture in the reform era. Budapest, 2005, Zrinyi Publishing House. ISBN 963 9276 45 6
2. Lajos BEREK: Basic elements of research work in Military Science. In: Tivadar SZILÁGYI (editor): Excerptions. Budapest, 1944 Zrínyi Miklós Military Academy. pp. 31-50.
3. Jenő KOVÁCS: Roots of the Hungarian Military Science, ideological problems of its development. In: New Defense Review, 2993. 47. vol. no. 6. pp. 1-7, ISSN 1216-7436
4. www.Globalsecurity.org/army/iraq (downloaded: 19 04 2012)

Requirements for pictures, sketches, illustrations, diagrams and other appendixes:

- title of the picture or illustration;
- source of the picture or illustration (or its drafter);
- serial number of the picture or illustration, (e.g. 1. picture);
- if it is possible, a Hungarian legend should be provided when the caption of the picture or illustration is given in a foreign language.

Requirements for abbreviations and foreign terms:

- foreignisms and abbreviations should be explained – at their first appearance – in the footnote, in Hungarian and in the original foreign language;
- e. g. WFP – World Food Program – ENSZ Világélelmezési Programja.

Points of Contact of the MNSS Scientific Board:

Postal address:
Katonai Nemzetbiztonsági Szolgálat Tudományos Tanácsa
1502 Budapest, Pf. 117

E-mail: natsecreview@gmail.com

Editor in chief: Colonel István Talián
E-mail: talian.istvan@knbsz. gov.hu