AARMS

Academic and Applied Research in Military and Public Management Science

Volume 17
Issue 3
2018

SCIENTIFIC JOURNAL OF THE NATIONAL UNIVERSITY OF PUBLIC SERVICE, HUNGARY

AARMS is a peer-reviewed international scientific journal devoted to reporting original research articles and comprehensive reviews within its scope that encompasses the military, political, economic, environmental and social dimensions of security and public management

AARMS is published in one volume of four issues per year by the National University of Public Service, Budapest, Hungary, under the auspices of the Rector of the University.

All correspondence should be addressed to Prof. Dr. PADÁNYI József, Editor-in-Chief
National University of Public Service
P. O. Box 15, H-1581 Budapest 146 Hungary

aarms@uni-nke hu
aarms uni-nke hu

AARMS

Academic and Applied Research in Military and Public Management Science

Volume 17 Issue 3 2018

An International Journal of Security, Strategy, Defense Studies, Military Technology and Public Management
Published by the National University of Public Service

Publisher:

NORDEX Non-Profit Ltd. – Dialóg Campus
Responsible for Publishing:
PETRÓ Ildikó, Managing Director

Proofreader:

GERGELY Zsuzsanna

Typeset and print by NORDEX Non-Profit Ltd. – Dialóg Campus

ISSN 2498-5392

Contents

AARMS Vol. 17, No. 3 (2018) 5–18.

The Politics of Oil in the Kurdistan Region of Iraq

Paiman Ramazan AHMAD[1]

This research is aimed at identifying the role of petroleum revenues in the Kurdistan Region for better economic efficiency and sovereignty of the Kurdistan Region in the future. This study identifies some root causes of deficiency of revenue usage generally, as well as specific causes in the Kurdistan Region. Further, the study looks at the various factors that affect oil production in the Kurdistan Region and compares it to the Federal Government. This study seeks to show how the Kurdistan Region generates the oil reserves regionally, despite the difficulties it encounters with the Federal Government due to the constitutional ambiguity. The research analysis concludes the importance of energy efficiency for the Kurdistan Region both economically and politically.

Keywords: *Kurdistan Region, Federal Government (Iraq), oil production, international legacy, constitutional dispute*

Introduction to the Petro-Region of Kurdistan (2007)

According to Nawshirwan Mustafa, leader of the Change Party in the Kurdistan Region, "Iraqi government never wanted the Kurdistan Region to be independent economically, because that will give the chance for the Kurdistan Regional Government to become independent". [43] The rise of oil production in recent years, typically in 2007, has dramatically transformed the economy of the Kurdistan Region. Many international oil companies (IOCs) poured into the region to extract cheap oil and get high profit out of the business; Sardar stated that "at the beginning the oil companies that invested in Kurdistan were small and not effective, but now there are globally known companies and very competitive". [1] Notably, the Kurdistan Region became an important economic agent in Iraq. Its presence in the economy grew with the oil control and regionalization of revenues. Although, it might be counted as the aim for the Kurdistan Regional Government (KRG) to expand the power of the local government on the economic base, but on the other hand, generating the oil revenues was extremely needed for the KRG to re-build the region. Additionally, the Federal Government's policy towards the region, urged the KRG to sow the oil in the region for better economic developments, the oil boom appeared to be a tremendous blessing for the Kurdistan Region. Hence, the KRG passes its own hydrocarbons law, "the Oil and Gas Law of the Kurdistan Region in 2007". [45]

The Prime Minister, Nechirvan Barzani, highlighted that this move is a "Historic moment", which "together with Iraq, the Constitution, will be the foundation of our economic development", [2] and will allow the Kurdistan Regional Government to "choose the best,

[1] Ph.D. in Public Administration, University of Raparin, Lecturer in Law and Administration departments, Rafia-Sulaimania-Kurdistan Region-Iraq. Teaching in Tishk International University-Erbil- previously "Ishik University" at Faculty of Administrative Sciences & Economics, Department of International Relations & Diplomacy, Erbil- Kurdistan Region -Iraq; e-mails: paiman.ramazan@gmail.com and paiman@raparinuni.org

most experienced, the most committed investors" for the Region. The most important thing about the Kurdistan Region is the fact that the oil fields are untapped; the only good thing Saddam Hussein did was: he was late in generating the oil resources in the Kurdistan Region. In this view, Kurdistan is the youngest region that exports oil, and its capacity is increasing rapidly. Conversely, Guy pointed out that "Iraq is the toughest environment we operate in", says the Chief Executive of a big Western oil company." [3] While, the stability and security of the Kurdistan Region are the immensely important factors for attracting foreign direct investors.

How Oil Economically Shaped KRG as a Petro-Region?

The economic growth of the region is the evidence of the oil revenues effectively generated recently by the regional government. The priority in the constitution of the KRG is given to the Investment Law, [4] and this is to be considered as the key driver of the foreign investment initiatives in the KRG. Since 2006, the KRG has managed to think about Investment Law, [4] and as well as the establishment of a separate institution which deals with investment in the KRG. Thus, in 2006 "the Kurdistan Board of Investment (BOI) was established, the main objective of BOI was to create new opportunities, and this was done by the legacy of the KRG Investment Law Article 5 which states that "a project shall be exempt from all non-custom taxes and duties for 10 years, starting from the date of providing service by the project, or the date of actual production", [4] this law was passed by the Kurdistan National Assembly and was ratified by Masoud Barzani, the President of the Kurdistan Regional Government. Apparently, this law is the most essential factor for the dramatic growth in the economy of the Kurdistan Region. Moreover, the tax incentives and benefits were both attractive for the foreign investors, together with enjoying the same equal rights like the local companies were helpful for attracting foreign investors towards the region for building a sustainable and efficient economic system. In addition to that, the BOI law is the main factor for privatization of the petroleum revenues in the KRG as a developing market; and this has boosted the KRG position as a sovereign region in Iraq. The petroleum policy efficiency is driven from the investment policy of the KRG, which is different from the Federal Government. As it is acknowledged by Luis Martinez "the Kurdistan Region has a weak economic policy except for its oil sector policy. The more its oil sector grows, the more the region develops. It is a good idea for the Kurdistan Region to give more profit to the oil companies". [5] The core deficiency is that the domestic products of the region cannot meet the demand. Besides, the KRG is entitled to deliver the service to the public, and the demand for service is also increasing. The actual symptoms of the "Dutch Disease" in the KRG economy are observable factors. The KRG Minister of Agriculture, Abdul Star, Majid announced that "the government focus will be on boosting domestic agricultural products to decrease exports from outside; according to him this is the future policy of the KRG in the agriculture sector." [6] The agricultural production shrank to less than what it was producing before the oil production; the dramatic decline in the domestic production had a general negative effect on the region. Perhaps, the most visible consequence of the Kurdistan Region's reliance on oil is that it was the only thing to depend on for the time being to build the economic infrastructure of the region from scratch. In fact, this had

a political reason behind, which was the Iraqi Regime, which had devastated the agriculture sector in the Kurdistan Region. Although, currently the agriculture sector is not sufficient, historically agriculture played a significant role in the national economy of Kurdistan." The KRG contribution to Iraqi agriculture production share is 50% of the nation's wheat, 40% of its barley, 98% of its tobacco, 30% of its cotton and 50% of its fruit. This means the KRG is doing better than the Federal Government, regardless of having lots of concerns in the agriculture sector, based on the data of the Ministry of Agriculture Profile, Directorate General of Planning and Follow-Up, Directorate of Statistics, Kurdistan Region, 2007. Kurdistan Development Corporation, Industry Sectors: Agriculture. [46]

Politics of the Kurdistan Oil Market

The Iraqi constitution guarantees that the Kurdistan Region is a federal region under Article 117/1: "First: This Constitution, upon coming into force, shall recognize the region of Kurdistan, along with its existing authorities, as a federal region." [7: Art. 117/1] The Iraqi Constitution, Article 117/1 within this debate, the Kurdistan Region has dramatically exercised its monopoly over the regional reserves after the collapse of the Baath Regime. It is estimated that the majority of the public is employed in the formal economy, government sector. In line with this, the KRG needs sustainable financial resources to constantly support the population of the Kurdistan Region. To a great extent the Kurdistan Region's oil wealth has had a positive consequence for its political system, which might be turned into what political scientist Terry Lynn Karl stated as a "Pacted Democracy" in which the political parties agree on sharing the wealth of the country according to their voting, but what was in the KRG was different since the two main parties had control over the oil until 2007; the Kurdistan Region in many ways resembled a two-party regime, though it was governed by an alternating multi-party system. [8] At the most overt level, the conflict between the KRG and the Federal Government is about who controls the reserves. Beyond that, the dispute is: from where and how the KRG is shipping the oil, since the KRG is not a member state of the Organization of the Petroleum Exporting Countries (OPEC) and the International Monetary Fund (IMF) formally and the Federal Government wants to export all Iraqi oil from the State Oil Marketing Organization (SOMO). Hence, "SOMO is deemed by the federal government to be the sole body invested with the authority to organise the sale and export of Iraqi oil." [9] Broadly speaking, the oil dependent states suffer during the oil crisis, and particularly when the oil price tumbles down, since this economic phenomenon leads to a severe crisis for the KRG. Because the KRG uses the oil wealth and redistributes it for the benefit of the community in different terms and programs, and it has created a social economy for the region. Unsurprisingly, the KRG has absolute control of the oil companies, and almost all of the foreign companies. Although, the economic sovereignty of the KRG is still an oil export driven economy, but the KRG has planted the seeds of oil to grow and transform the region gradually. Perhaps the most important key elements that the KRG has sought to solve were first and foremost reforms and bringing new foreign oil companies to invest in Kurdistan.

Boosting the efficiency of oil production in terms of internationalization balanced the role of the KRG the same as the Iraqi Government for the foreign oil import countries.

The process of the refinery of the KRG oil is not sophisticated; hence the companies can handle it properly, because many oil revenues had been newly explored; therefore, it needs new construction and drilling, the risk of drilling for crude oil in the KRG is also low. The disagreement with the Federal Government and the KRG is accompanied by the natural resource distribution and sharing the capital. Moreover, the power of the KRG as a region shifted the Iraqi oil policy of centralization to a more decentralized dimension. Which is contradicting the notion of nationalism, "the oil market power transferred to state owned enterprises in the late 1970s, oil companies have been largely overpowered by the tide of nationalization?" [10] More prominently, [11] stated that "on 26th February 2007, the Iraqi Cabinet passed and recommended for parliamentary approval a new law governing the country's immense and largely untapped supplies of oil and natural gas". The ultimate goal of this law was first to control energy reserves all over Iraq and in particular those in the Kurdistan Region, besides that, it was what the United Stated wanted after the Iraqi invasion, to promote the role of foreign private companies to have a say in Iraqi energy industry. Furthermore, there was a significant potential in terms of the Production Sharing Agreements (PSAs), the ownership system of oil in the Federal Government, which since the 2003 invasion has become the nightmare for Iraqi politicians, as Muttitt highlighted that "straight after the war, was guided less by firm principles than by an ideological presumption that the oil industry's future lay in the IOCs' hands." [12] They "could not accept that there might be a legitimate political position that opposed transferring control [to the IOCs]." In an interview with the Minister of Natural Resources of the KRG, Ashti Hawrami stressed "the importance of regional management of the oil sector in which the benefit goes to the KRG residents, Iraq and the future generation." [13]

Crucially, Hawrami added that the federal constitution of 2005, has fundamental concepts of power sharing and revenue sharing, it decentralizes the management of new oil and gas reserves in the country to the regions and governorates, it calls for joint rights in the old fields, though the Federal Government denies these rights by the regions to practise. From an early stage, the KRG thought strategically of efficient management of oil reserves; however, that contradicts the federal interest in oil production mainly. In fact, sharing oil profit with the private international companies who invest in oil production in Kurdistan brought key development into the oil field since 2005. The Kurdish approach "was to move swiftly to develop an investor-friendly legal regime for petroleum exploration and development, based on a model production sharing contract and a framework Petroleum law." [14] It can hardly be doubted that this formed part of a wider agenda by the authorities to lay down a long-term economic basis for an independent Kurdish state. In fact, this effort has attracted more than two dozen of the International Oil Companies (IOCs). [14] The strategy that the KRG follows is in contradiction with the Federal Government, as the Federal Government avoids any "PSAs" and prefers the Technical Service Contracts (TSCs), in which it avoids the influence of the international oil companies in oil production; this is yet the best practise for the Federal Government. Although, according to the *International Energy Agency* figures, "PSAs are only used in respect of about 12% of world oil reserves, in countries where oilfields are small (and often offshore), production costs are high, and exploration prospects are uncertain. None of these conditions applies to Iraq". It can be said that the Kurdistan Regional Government petroleum industry is based on the PSAs, which is considered to be a radical change in the oil and gas field management compared

to the Federal Government regulations and system of energy management. “Investors use their capitals but share the profit, and the KRG believes such agreements provide vital encouragement for companies to increase their production in the region.” [15] The KRG Ministry of Natural Resource is seeking oil efficiency for better growth in the energy sector, though Baghdad bargained to stop the KRG from exporting oil, but this was not successful. As many multinational oil companies, such as “ExxonMobil, Chevro Total, and Gazprom,” accepted to enter into the market production based on production sharing agreements. [16] The root of the dispute with the Iraqi Federal Government is dated back to 2004 when “the KRG independently signed a contract with the Norwegian Oil Company (NOC)”, [10] in reaction to what the KRG did, the Federal Government decided to warn all foreign companies to avoid signing contracts with the KRG, since the company’s federal contracts would be terminated.

Further, the action of the Federal Government was threatening and it was waging sanctions against any foreign company investing or even buying oil from the KRG, “SOMO, on behalf of the Iraqi federal ministry of oil, is hereby warning all companies, individuals and bodies from buying the Iraqi crude oil cargo that is loaded on the vessel”, [17] International oil companies are increasingly drawn to the region, as contracts to re-develop old oil fields and explore for new ones in southern Iraq turn out to be less attractive than anticipated.” [18] However, for some well-known oil companies, it was not easy to defy Baghdad and move to Kurdistan including Shell, which has a strong presence in three major oil and gas fields in Iraq, Shell has come close to securing contracts with the region twice before, but pulled back so as not to antagonise the central government in Baghdad, which regards all deals signed by the Kurdistan Regional Government as illegal. [19] Importantly, Shell has no interest to lose its interest in the federal contracts, but started to explore interest in Iraq as one entirety and wants to engage with the KRG oil market, too. The central government claims the illegality of oil export from the Kurdistan Region. But according to the Iraqi Constitution, Kurdistan is a Federal Autonomous Region and it has its own constitution, and the Petroleum law is well addressed by the regional constitution and it is in line with the federal constitution. Hence, it gives the right to generate and export oil. The ambiguous Iraqi Constitution, Article 109/1 highlights: “the federal government with the regions and governments shall undertake the management of oil and gas extracted from current fields provided that it distributes oil and gas revenues in a fair manner in proportion to the population distribution in all parts of the country with a set allotment for a set time for the damaged regions that were unjustly deprived by the former regime and the regions that were damaged later, as well in a way that assures balanced development in different areas of the country, and this will be regulated by law.” [7: Art. 109 para. 1]

Adding to this, the second part of Article 109 explains that “the central government with regional governments should work to formulate necessary policies and strategies for developing the oil and gas fields for achieving highest benefits for the Iraqi people.” [7: Art. 109 para. 2] According to the first part of Article 109 that states “current” which does not mean the future oil fields, but the current explored revenues before the 2005 constitution, not to mention that the Iraqi government never shows willingness in returning the capital that the Kurdistan Region deserves. And this made the KRG hesitate in returning the profit share to the central government. Since there is no trust and Baghdad has not shown willingness in providing the Kurdistan Region with the needs that the region needs. Despite the fact

that Baghdad has always triggered the problem in the Kurdistan Region Oil development, and the successful economical experiences of Kurdistan were never welcomed by Baghdad, instead Baghdad always accused the Kurdistan Region over its independent oil production. This mistrust has historical and logical roots for the Kurdistan Region. Even though, Article 108 mentioned that "oil and gas are the property of the nation (people) of all the Regions and Governorates." [7: Art. 108] On the ground, the government of Iraq is the owner of the oil wealth and the people of Iraq have never enjoyed the energy wealth. On the other hand, it is obvious that the Iraqi Constitution has no implication of "future revenues", it just mentions the oil resources without indicating them, as Article 111 says: "All powers not stipulated in the exclusive authorities of the federal government shall be the powers of the regions and governorates that are not organized in a region. The priority goes to the regional law in case of conflict between other powers shared between the federal government and regional governments." [7: Art. 111]

According to Article 111, the power of the Kurdistan Region is to be taken into consideration legally and seriously. While the first paragraph of Article 117 states that "the regional powers shall have the right to exercise executive, legislative, and judicial powers in accordance with this Constitution, except for those authorities stipulated in the exclusive authorities of the federal government." [7: Art. 117 para. 1] This completes what is missing in Article 111. In fact, a bilateral agreement between Erbil and Baghdad looks impossible; the Iraqi government has always practiced abusing its power over the KRG budget. Precisely, as alleged by the Kurdistan President's Chief of Staff, Fuad Hussien "Baghdad rejects mentioning the KRG as an oil producer in the official constitution, since Iraqi exports 3.4 million barrels of oil daily, and out of that almost 400,000 barrels (bbl) of it is exported by Kurdistan Region." [44] This constitutionally jeopardizes the KRG to be an independent region as mentioned by the Iraqi Constitution. Additionally, Baghdad's latest ace was to nearly cut the Kurds out of the federal budget. The $119 million budget for 2013 was passed on 7 March. The Kurds only got $646 million of the $3.5 billion they requested. [20] As a result, the KRG passed its regional Financial Rights Law on 23 April 2013: "Law of identifying and obtaining financial dues to the Kurdistan Region – Iraq from federal revenue. (The 'Financial Rights Law'.) The Financial Rights Law allows the KRG to independently export crude oil produced in the Kurdistan Region if the Federal Government fails to pay the KRG its share of revenues (including oil revenues), budget items, other national allocations and reparations." [21]

In spite of all this, in January 2014 "the federal government practised suspending the KRG budget for almost one year." [22] A serious perspective for the KRG reaction was to get prepared for the financial crisis and to have a strategic mechanism for determining what the KRG was getting from the Federal Government, and also, what was to do if the Federal Government would not pay. Then the KRG government would be able to export oil to provide its population with the needs, which in practise meant getting ready to practising the economic efficiency for the region. Accordingly, the Iraqi government has tried to revise and amend the constitution according to oil and revenue sharing, the first attempt was made during 2010–2011 and was twice failed, since the Prime Minister, Nuri Al-Maliki and his followers had tried to restrict the regional authority of the KRG and as the main purpose was to enact the new law for oil and gas, "in spite of having the Ministry of Oil, the Federal government also intended to create new entities in oil field such as the Iraqi National

Oil Company (INOC) and, the Federal Oil and Gas Council (FOGC) besides the Bureau of Independent Advisors (BIA).” [23] A controversial issue is the incentives created by the Federal Government in increasing its monopoly through FOGC to review and control oil contracts both in the central government and in the KRG. In the new constitution, the FOGC got high authority in oil control as well “Article 18 of Iraq Oil Law of 17 August 2011, gives the right to BIA to review all new petroleum contracts.” [24]

The intention is clear that the Federal Government excludes the old petroleum contracts, since most newly signed contracts are in the Kurdistan Region, though another concern is that the BIA members ought to be foreign experts in which the Federal Government does not want foreign influence over oil. Ultimately, the Iraqi government wants to secure the guarantee of oil production under its authority. The core problem is the vagueness of the constitution, in addition to another very sensitive issue, the geographical location of the oil reserves in Iraq, in which “Iraq’s oil reserves are mainly concentrated in Shiite areas of the south and Kurdish region in the north. Some reserves are also located in central Iraq.” [25] Therefore, the Sunni Arabs would never accept the de-Baathification of oil reserves and oil policy, because the zeal for autonomy of the Basra province had been a concern for the Shia population of the province too, as mentioned by Mohammed al-Taie, an MP representing Basra, who told Al-Akhbar: “Establishing a semi-autonomous region is necessary to organize the wealth and power in any country whose federal government has failed in its performance and management of the state.” [26] As a consequence, the decentralization is highly accepted by the Kurds and Shia Leaders, whereas, it has been rejected by Sunnis; at this point KRG is the only efficient region for having untapped petroleum reserves.

Production Capacity of the Kurdistan Region in the Iraqi Oil Market

To be noted, the Kurdistan Region was devastated by the thirteen years of Baath Regime’s policy, thus the Kurdistan Region has worked hard to develop the energy sector, and the KRG’s capacity of oil production is progressing consistently. As mentioned by Prime Minister Barham Salih (2011) “the days when Kurdistan was an economic backwater are over”. [27] Kurdistan Oil production is featured as the so-called easy oil, which does not require deep drilling. Being poorly reported, the data on the Iraq oil reserves are different but, “the Department of Energy (DOE) Energy Information Administration (EIA) figures claiming that the territory of Iraq contains over 112 billion barrels of proven reserves—oil that has been definitively discovered and is expected to be economically producible. Since, Iraq is the least explored of the oil-rich countries.” [28] Therefore, there is a possibility that most of all those unexplored fields are in the Kurdistan Region since the Iraqi Baath regime neglected the revenues in the Region. “Almost 43 B/b are in Kurdistan region out of the 115/Bb of the Iraqi Crude Oil.” [29]

Additionally, the European Centre for Energy and Resource Security (EUCERS) stated that “natural gas reserves of Kurdistan are estimated at 100–200 trillion cubic feet—alternatively, 2.8–5.6 billion cubic meters—which is more than countries like Norway or Kazakhstan.” [30] Despite the fact that the Federal Government claims that it has an incentive in motivating investment in Iraqi, as mentioned in Article 26: “The state

guarantees the encouragement of investments in the various sectors; this will be organized by law." [7: Art. 26] But this is not the real picture for Kurdistan since the Federal Government restrains regional capacity in developing the energy sector. The disputes over oil production had affected the efficient regional and federal income usages in the country. The Federal Government's objection was yet not influential enough to stop all international investors to the Kurdistan Region, as the motto of the KRG was different from the central government. The production-sharing contracts (PSCs) have helped the KRG to attract many international oil companies to the Kurdistan Region since the early 2009. Acknowledged by Denise Natali, "the central government may also fear that paying the IOCs in the Kurdish north a greater profit margin than companies working in the south." [31] The international perception in case of the KRG has been positive since; the Iraqi government avoids foreign control over oil while the KRG has better relations with the foreign companies. If energy security is a real concern for the international energy markets, then supporting the KRG to produce oil is needed. The two most significant concerns in Iraqi oil production are always taken into account seriously: the first is that the largest oil fields are in Southern Iraq and in Northern Iraq, in the Kurdistan Region, typically in "Kirkuk" over which the KRG and the Federal Government still have a territorial dispute.

Yet a deeper look into the situation and politics reveals a more complex scenario with uncertain outcomes. The political arena is volatile, with the emergence of different perspectives on losing sovereignty, the rejection of privatization of oil according to many Iraqi specialists results in the long term future economic drawbacks based on the interpretation of the fact that the company will have the right in sharing of the revenues for a long period, i.e. at least for 30 years. However, comparing the Kurdistan Region as an oil rich "virgin region" to other countries is not fair, since the discovery of oil in the Kurdistan Region is quite novel; so its case is different. Overall, the Federal Government wants to have the benefit and share return of oil exports to the central government to control the cash flow in the country. In explaining the importance of the Kurdistan Region in terms of geological location, which is part of the Zagros Fold Belt that is a prolific oil province in Iran and Iraq to the south and west. (Figure 1)

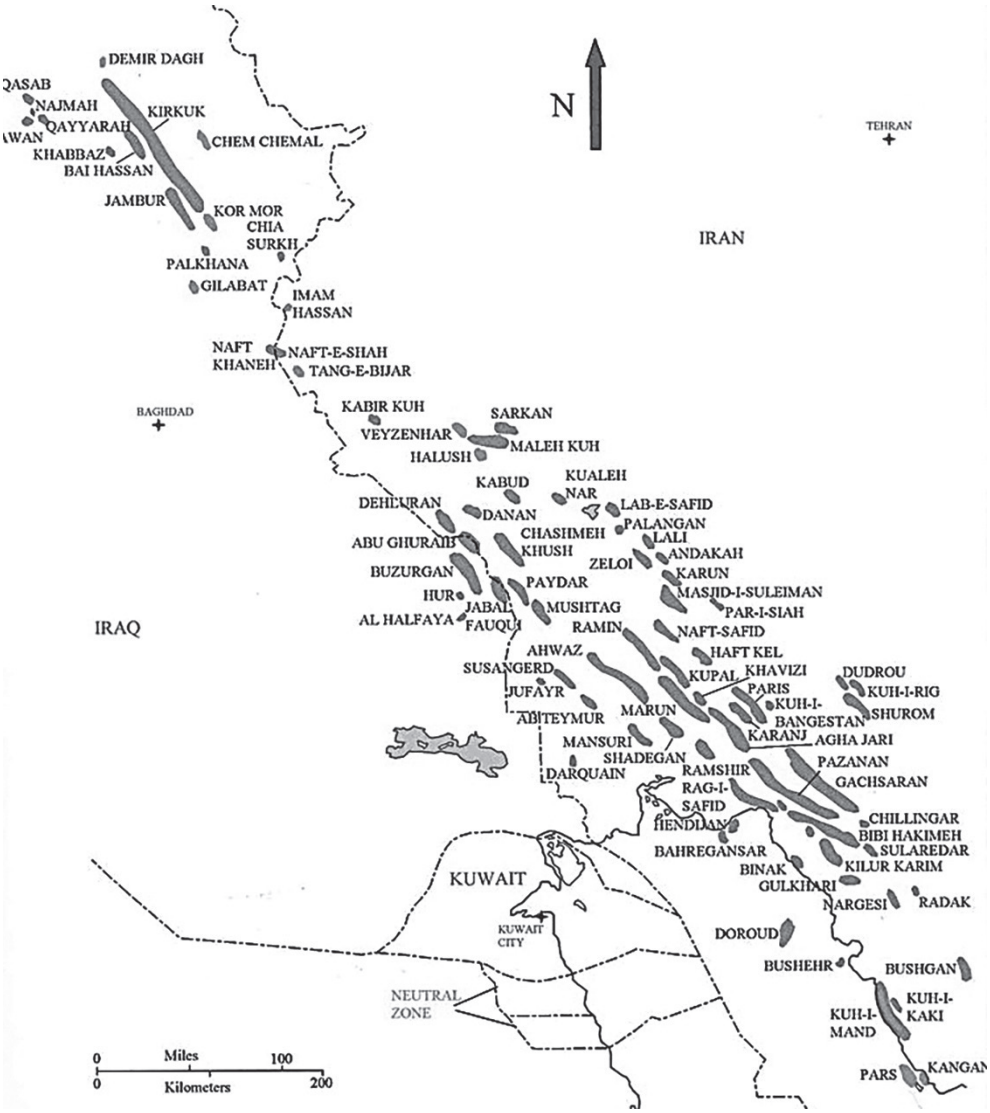


Figure 1. *Iran oil fields.* [47]

The Lack of International Legacy in the KRG Status as an Autonomous Rich Energy Region

The Kurdistan Region as an autonomous region is a geographically landlocked region; the region started the extraction of oil recently and typically after the 2007 disagreement with the Federal Government. In fact, the geographical role of the Kurdistan Region is critical, and the role of the Federal Government is stronger according to the constitution as well as according to the international status, Iraq is a sovereign state, while the KRG

is a federal region in Iraq. Hence, Kurdistan has no sovereign power in any decision making according to international regulations, thus the Kurdistan Region does not have a say in the international energy markets yet, as a sovereign state or region. Certainly, the KRG practice of a more business-friendly approach is driven from the "good neighbour policy". [16] The KRG's foreign energy policy is mainly dependent on Turkey as a neighbour country for the region at the present time. Although Iraq had a historical long-term relation with Turkey, recently, the Ankara–Baghdad relations had changed due to the KRG–Ankara ties. To put these results in context, according to the national interest both the KRG and Turkey have their own objectives to obtain. To begin with, the KRG–Federal Government relations are not certain and the issue of oil control is the main problem for both sides. A better explanation lies in the fact of federal sovereignty, whereas for the KRG, territorial claims and revenue control rights are important. The KRG energy ties with foreign countries are forbidden according to the Iraqi Federal Government and are illegal, besides the Federal Government has warned the foreign oil companies and countries for being involved in the KRG oil production and export. Interestingly, Ankara managed to work with both the Federal Government on the one hand, and the KRG, on the other hand. "We cannot ignore the energy resource next door to us", [32] as a result of the Turkish motive towards the KRG, the Iraqi–Turkish foreign relations were tensed, while Turkey started looking for better economic relations with the KRG. There is a significant potential in the Turkey–KRG energy partnership, since recently, Turkey's attitude had changed towards the Kurdistan Region, and the strategic relations are based on the economic contribution for both sides.

The interest lies in two dimensions, most importantly, in Turkey's energy security, where the "domestic energy consumption rises by 6–8 percent annually." [33] Meanwhile, for energy, Turkey depends on Iran and Russia mainly, thus the emergence of the KRG is an alternative for decreasing the Russian and Iranian influence on Turkey's energy security. "It is being concluded that energy imported to Turkey in 2013 reached $55.9 billion, almost about 22.2 percent of the total imports and about 56 percent of the total trade deficit of the country." [34] In this analysis, the KRG is a stable energy supplier for the Turkish energy security. In the meantime, the Kurdistan Region needs a partner for supporting the exporting of its oil to the international energy markets. The KRG realized this weakness at the very beginning of the oil development; therefore, the energy policy with Turkey was a major concern for the KRG to take it into account seriously. The reality of the KRG energy foreign policy and economic development as a dependent region fits the model study which was conducted by Pal Kolsto and Helge Balkkisrud, whom revealed that "the unrecognized de facto states have tended to stress in their interaction with the international community their economic viability and prospects for economic survival." [35] Although, having enough resources for the KRG means being sovereign, though the challenge is how to control them for domestic economic sovereignty and progress.

It bears emphasizing that the emergence of Kurdistan as an efficient de facto oil exporter relays on having free pipeline export to the international markets, which now the Kurdistan Region does not have, thus the diplomatic relations of the Kurdistan Region is fragile. Considering, the blooming economic cooperation with Turkey strengthens the role of the KRG in the region regardless of being a federal region. Within this context, the economic relations are remarkable for Turkey to diversify the domestic energy consumption, import via the KRG, as "Turkey's domestic resources are not sufficient to meet the energy demand." [36: 61]

Besides, the KRG's economy is also depending on the Turkish products mainly, including the entire market needs, acknowledged by the Kurdish officials, "Turkey is the KRG's main business partner—trade volume is $7.7 billion, 5 and 80 percent of Kurdish consumer imports come from Turkey." [37] In this equation, the KRG's energy reserves are important for feeding the European energy market, particularly the present initiative of the KRG for gas export to Europe. Tony Hayward, Chairman of Genel Energy, said that "gas export will be far more strategic than oil export for the KRG, my expectation is that by the early 2020s, more than 20 billion cubic metres of gas a year will flow from the Kurdistan Region of Iraq into the Turkish market and into Europe." [38] Apparently, international oil companies (IOCs) stayed in KRG even during the ISIS war, which gives credibility to the Kurdistan Region as an important offshore energy hub. Regarding recent updates in November 2015, "KRG's crude oil was sold for the first time the crude markets in North-Western Europe, this was the first oil barrels of KRG in the Baltic ports." [39] Remarkably, exporting oil independently to almost 10 countries complicate the tension with the central government further. However, the Minister of Natural Resources of the KRG reckoned that "it is premature to disclose the names of traders, shippers and buyers of Kurdish oil." [40] In fact, many countries are involved, yet it is elusive, as Stuart et al. mentioned, "with the federal government in Baghdad threatening to sue any buyer of Kurdish crude." [41] In line with this, in a commentary in the European Council on Foreign Relations, [42] the role of the Kurdistan Region is mentioned among the reliable sources of secure energy for the European Union, "Iraq—and in particular, Kurdistan—is another potential supply option for Europe: it has massive oil and gas resources and international exploration and production companies are present and active". Kurdistan, as mentioned, can be a sustainable energy supplier for the European Continent in the future, therefore, the dispute between the KRG and the Iraqi government is to be settled.

Concluding Remarks

To conclude, the role of oil revenues in the strengthening economic independence for the Kurdistan Region is extremely important. Moreover, the Kurdistan Region cannot be economically efficient, unless it finalizes the disputes with the Federal Government of Iraq, especially the constitutional disagreements on oil share and the territorial disputes, as well. A key ending of this analysis is the conclusion that the Kurdistan Regional Government seems to have yet a deeper concern about the regional petroleum revenues, since the regional politics reveals a more complex scenario with uncertain outcomes due to the federal–regional disputes on the one hand and the instability of Iraq on the other hand. The political arena is volatile, with the emergence of new threats that may affect the oil production. In spite of that, the success of the Kurdistan Region as a key oil producer depends on Turkey and the international oil companies. Eventually, the KRG can perform well by following different policies, especially such as the Production Sharing Agreements with International Oil Companies and good neighbour policy with Turkey. Causally, the KRG needs to focus on diversifying the chance for oil and gas transport via different channels and other countries to decrease the exclusive Turkish influence on the energy production of the Kurdistan Region.

References

[1] SARDAR, A.: *International oil companies and public right.* December 2, 2013. www.payik.net/all-details.aspx?jimare=258 (Downloaded: 22.11.2015), (Translated from Kurdish language.)

[2] BARZANI, N., (PM): *Kurdistan Oil and Gas Law approved by Kurdistan Parliament.* krg.org, August 6, 2007. http://cabinet.gov.krd/a/d.aspx?s=010000&l=12&a=19507 (Downloaded: 11.11.2015)

[3] GUY, C.: Iraq's appeal wanes for oil majors. *Financial Times*, March 17, 2013. http://pictorial-guide-to-energy.blogspot.hu/2013_03_01_archive.html (Downloaded: 13.11.2015)

[4] *The Investment Law.* (Official English translation of the investment law.) http://belkib.com/in-english.html. (Downloaded: 13.11.2015)

[5] Interview with Luis Martinez. In. *French Oil Expert: Kurdistan Oil Deals Are Transparent and Standard Contracts.* London, Erbil, Baghdaf: Iraq Energy Institute, November 12, 2012.

[6] *Interview with, KRG, Agriculture Minister, Abdul-Star Majid.* 2014. http://hawlati.co/%D8%A6%DB%95%D8%B1%D8%B4%DB%8C%DA%A4%D-B%95%DA%A9%D8%A7%D9%86/49649 (Downloaded: 22.11.2015)

[7] *Iraqi Constitution, 2005.* (English version.) www.washingtonpost.com/wp-dyn/content/article/2005/10/12/AR2005101201450.html (Downloaded: 21.11.2015)

[8] KARL, T. L.: *The Paradox of plenty: oil booms and petro-states*. Oakland: University of California Press, 1997.

[9] *State Oil Marketing Organisation, (SOMO).* http://somooil.gov.iq/en/ (Downloaded: 04.11.2015)

[10] LEUBA, K.: *Exxon's role in Iraq-Kurdistan relations.* Cairo: The American University in Cairo, 2014. http://schools.aucegypt.edu/huss/pols/Khamasin/Pages/article.aspx?eid=15 (Downloaded: 25.11.2015)

[11] BADER-BLAU, S.: Iraqi unions vs. big oil. In. *Middle East Research and Information project*. MER 275, Vol. 45 (2015). www.merip.org/author/shawna-bader-blau (Downloaded: 25.11.2015)

[12] MUTTITT, G.: Fuel on the Fire: Oil and Politics in Occupied Iraq. *Energy Policy*, 39 (2011), 7482–7483.

[13] ABO: *Blessed with resources.* Interview with Ashti Hawrami, Kurdistan's Minister for Natural Resources. June, 2013. www.abo.net/oilportal/interview/view.do?contentId=2122237 (Downloaded: 22.11.2015)

[14] CAMERON, P. D.: Managing the Politics of Oil Reforms: Lessons from Iraq. Washington D.C.: Center for Energy, Petroleum & Mineral Law and Policy, 2010.

[15] SHIVAN, F.: What Brings Oil Giants to Kurdistan? *Kurdish Globe*, July 22, 2013. www.kurdishglobe.net/article/851D1BB96C51323F04FBC7CBBC14A20E/What-Brings-Oil-Giants-to-Kurdistan-.html (Downloaded: 13.11.2015)

[16] IIG: Overview: Kurdistan Region of Iraq. *Diplomacy & Politics*, July 30, 2013. www.investingroup.org/publications/kurdistan/overview/diplomacy-politics (Downloaded: 22.11.2015)

[17] Iraq threatens legal action against any buyer of Kurdistan oil. *EKurd Daily* (online), June 1, 2015. http://ekurd.net/mismas/articles/misc2014/6/state8043.htm (Downloaded: 23.11.2015)

[18] Total investing in Kurdistan oil despite threats. *Market Watch* (online), August 21, 2012. accessed on November 21, 2015, available online at: www.marketwatch.com/story/total-investing-in-kurdistan-oil-despite-threats-2012-08-21 (Downloaded: 23.11.2015)

[19] PEG, M.: Sell again weighs energy openings in Iraqi Kurdistan. *Reuters* (online), September 21, 2012. http://uk.reuters.com/article/2012/09/21/uk-shell-iraq-kurdistan-idUKBRE88K0YC20120921 (Downloaded: 21.11.2015)

[20] OGIB RESEARCH TEAM: Iraq – Kurdistan's Billion-Barrel Oil Investment. *Oil and Gas Investment Bulletin* (online), March 27, 2013. http://oilandgas-investments.com/2013/investing/iraq-kurdistan-oil-investment (Downloaded: 21.11.2015)

[21] KORNEY, S., GOLDEN, G. J., AMIRI, A.: Moving towards direct oil exports from the Kurdistan region of Iraq. *Lexology* (online), June 11, 2013. www.lexology.com/library/detail.aspx?g=fa8e7f9c-6f37-4ad8-b052-a72a542e9cbc (Downloaded: 10.11.2015)

[22] KAYAKIRAN, F.: Iraqi Kurds to pay oil exporters $75 million with more to follow. *Bloomberg* (online), November 7, 2014. www.bloomberg.com/news/2014-11-07/iraqi-kurds-to-pay-oil-exporters-75-million-with-more-to-follow.html (Downloaded: 21.11.2015)

[23] KORNEY, S., SATTAROVA, S., AL-MALIK, M.: Two are not always better than one: Iraq is competing oil and gas laws. *Lexology* (online), October 14, 2011. www.lexology.com/library/detail.aspx?g=546ce703-21a9-4163-b5cc-b7c8e67c3101 (Downloaded: 10.11.2015)

[24] AHMED, A. M.: *Preliminary remarks on the new version of oil law.* Norway: Iraq/Development Consultancy and Research, 2011. www.iraq-businessnews.com/wp-content/uploads/2011/08/Ahmed-Mousa-Jiyad-Preliminary-Remarks-on-the-Parliament-New-Version-of-the-Oil-Law2.doc (Downloaded: 10.11.2015)

[25] GUPTA, A.: *Countries with the biggest oil reserves.* October 30, 2013. www.hydrocarbons-technology.com/features/feature-countries-with-the-biggest-oil-reserves (Downloaded: 20.11.2015)

[26] AL-MASHHADANI, M.: Can Iraq's Basra province become the Kurdistan of the south? *Al-Akhbar English* (online), December 4, 2014. http://english.al-akhbar.com/node/22755 (Downloaded: 23.11.2015)

[27] UPI: *As Iraq smoulders, Kurds sit on oil riches.* December 22, 2011. www.upi.com/Business_News/Energy-Industry/2011/12/22/As-Iraq-smolders-Kurds-sit-on-oil-riches/97641324580189 (Downloaded: 20.11.2015)

[28] LUFT, G.: *How Much Oil Does Iraq Have?* Washington D.C.: Brookings Institution, 2003. www.brookings.edu/research/papers/2003/05/12globalenvironment-luft (Downloaded: 25.11.2015)

[29] BARZNJI, N.: *Oil in Kurdistan region.* April 3, 2014. http://bzavpress.com/Detail.aspx-?id=2962&LinkID=2 (Downloaded: 23.11.2015)

[30] PFLÜGER, F., DUERO, A.: New stability and prospects for Kurdish oil and gas. *Elektor* (online), December 5, 2011. www.elektormagazine.com/news/New-Stability-and-Prospects-for-Kurdish-Oil-and-Gas (Downloaded: 23.11.2015)

[31] NATALI, D.: The politics of Kurdish crude. *Middle East Policy Council, Journal Essay,* XIX 1 (2012). www.mepc.org/journal/middle-east-policy-archives/politics-kurdish-crude?print (Downloaded: 27.11.2015)

[32] CETINGULEC, M.: Turkey pivots to Baghdad to close deal on Kurdish oil. *Al-Monitor* (online), May 19, 2013. www.al-monitor.com/pulse/originals/2014/05/turkey-needs-baghdad-permission-sell-kurdish-oil.html# (Downloaded: 23.11.2015)

[33] TOCCI, N.: Turkey's Kurdish Gamble. *IAI Working Papers* (online), 13 10 (2013). www.iai.it/sites/default/files/iaiwp1310.pdf (Downloaded: 20.11.2015)

[34] YEREVAN, S.: Kurdistan's energy resources could be a defining point of Turkey's foreign policy. *Diplomatic Courier: A Global Affairs Magazine* (online), July 24, 2014. www.diplomaticourier.com/2014/07/24/kurdistan-s-energy-resources-could-be-defining-point-of-turkey-s-foreign-policy/ (Downloaded: 24.11.2015)

[35] VOLLER, Y.: *From rebellion to de facto statehood: international and transnational sources of the transformation of the Kurdish national liberation movement in Iraq into the Kurdistan regional government.* (Ph.D. dissertation) London: University of London, London School of Economics and Political Science, 2012.

[36] ERENSU, S.: Abundance and scarcity amidst the crisis of 'modern water'. In. HARRIS, L. M., GOLDIN, J. A., SNEDDON, C. (eds.): *Contemporary Water Governance in the Global South. Scarcity, Marketization and Participation.* London and New York: Routledge, 2013. Part II/6.

[37] SONER, C., TYLER, E. (2012). *Turkey's changing relations with Iraq: Kurdistan up, Baghdad down.* Washington D.C.: Washington Institute for Near East Policy, 2012.

[38] *Minister of Natural Resources Speech.* Ashti Hawtami on the website of the Ministry of Natural Resources of KRG. http://mnr.krg.org/index.php/en/press-releases/513-minister-hawrami-says-kurdistan-makes-progress-on-gas-export-to-turkey-and-europe-krg-s-direct-oil-sales-fund-war-against-isis (Downloaded: 23.11.2015)

[39] GORODYANKIN, G.: Kurdish oil reaches Baltic, targets Russian markets. *Reuters* (online), November 8, 2015. www.reuters.com/article/2015/11/18/us-kurdistan-oil-europe-idUSKCN0T72LP20151118#m829xQucS49PMs8o.97 (Downloaded: 27.11.2015)

[40] ZHDANNIKOV, D.: Exclusive: How Kurdistan bypassed Baghdad and sold oil on global markets. *Reuters* (online), November 17, 2015. www.reuters.com/article/2015/11/17/us-iraq-kurdistan-oil-idUSKCN0T61HH20151117#3qr5VG1QCr4tbZ34.97 (Downloaded: 26.11.2015)

[41] STUART, E., LANINGHAM, P. van, MORLEY, J.: Iraqi Kurdish crude oil exports win favour in Europe. *Middle East Energy Focus* (online), August 27, 2015. www.platts.com/news-feature/2015/oil/middle-east-energy-focus/kurdish-crude-exports-082815 (Downloaded: 26.11.2015)

[42] CHYONG, C., SLAVKOVA, L., TCHERNEVA, V.: *Europe's alternative to Russian gas.* London: European Council on Foreign Relations, 2015. www.ecfr.eu/article/commentary_europes_alternatives_to_russian_gas311666 (Downloaded: 22.11.2015)

[43] MUSTAFA, N.: Oil Dispute between KRG and Federal government. *Sbeiy.com,* November 28, 2007. www.sbeiy.com/(X(1)S(3m4f40sf4m4h12jtb3pd40ed))/ku/article_detail.aspx?ArticleID=278&AuthorID=36 (Downloaded: 20.11.2015)

[44] RUDAW: *Erbil says no breakthrough in energy, budget talks with Iraqi team.* April 15, 2014. http://rudaw.net/english/kurdistan/15042014 (Downloaded: 21.11.2015)

[45] *Oil and Gas Law of the Kurdistan Region – Iraq, 2007.* http://cabinet.gov.krd/uploads/documents/Kurdistan%20Oil%20and%20Gas%20Law%20English__2007_09_06_h14m0s42.pdf (Downloaded: 20.11.2015)

[46] *Kurdistan Development Corporation, Industry Sectors: Agriculture.* Erbil, Kurdistan Region: Ministry of Agriculture and Water Resources, Directorate General of Planning and Follow-Up, Directorate of Statistics, 2007.

[47] Iran: 14 new oil and gas fields to be put up for tender. *energy-pedia.news,* s.d. www.energy-pedia.com/news/iran/14-new-oil-and-gas-fields-to-be-put-up-for-tender (Downloaded: 20.11.2018)

AARMS Vol. 17, No. 3 (2018) 19–46.

Combating Cyber Crime[1]

Krunoslav ANTOLIŠ,[2] Ivančica VARJAČIĆ,[3] Mario JELENSKI[4]

Life in a modern society is determined by strategic drivers, the most important of which are the Internet and Information and Communication Technology (ICT). Their use is one that contributes to global development and enables it to be balanced globally. The sustainability of this development is directly dependent on the degree of Internet misuse and the misuse of ICT. That is why we are discussing computer criminality through the example of Croatia. In the second part, we analyse the misuse of new ICT and the ways and possibilities of legitimate opposition to ICT abuses.

Keywords: *Internet, ICT, abuse, misuse, cyber crime*

Introduction

New information technologies are unavoidable factors in the modern world changing it in technological but also in communicological sense. According to Antoliš: "both aspects of the changes, apart from new possibilities, bring along vulnerabilities, which must not be disregarded." [3: 121] The mentioned vulnerabilities open the doors wide to computer crime characterized by fast-spreading, a variety of forms aimed at material and non-material benefits, with perpetrators having technical knowledge, going global and by a high "dark figure of crime". An inseparable term related to computer crime is digital evidence which combines text, images, audio and video recordings. Information vulnerabilities have a direct impact on the security of modern economic systems where ICT is becoming a dominating information and communication platform. It is not only terrorists that we should be concerned about when thinking of the security of economic entities but also organized and economic crime, competitive states and companies, different hackers and even those who, due to various social and economic reasons, live on the margins of modern society. Of course, none of the mentioned categories is immune to committing terrorist acts and that is why, for prevention reasons, all of them should be observed and prevented in accordance with security estimates according to the views of Antoliš and Varjačić. [2: 231]

This paper also deals with the reasons why Darknet has become a safe haven for all those who want to protect their activities from the eyes of others. We are primarily interested in those who use this Darknet protection to deal with illegal activities such as organized crime, violent extremism, terrorism, radicalization, etc. But, to be able to devote this analysis to the abuses

---

1 All statements made in this article are solely those of the author and in no way reflect the official position or policies of the Republic of Croatia, the Croat Parliament, the Croat Government or Ministry of the Interior.

2 Ph.D., assistant professor, Ministry of the Interior of the Republic of Croatia, Police Academy, Police College in Zagreb; e-mail: kantolis@fkz.hr

3 Crime Investigation Specialist, Ministry of the Interior of the Republic of Croatia; e-mail: ivarjacic@mup.hr

4 Professional Bachelor of Criminal Investigation, Ministry of the Interior of the Republic of Croatia; e-mail: mario.jelenski@gmail.com

of Darknet, we must first understand how Darknet works for which this article should serve as a guidance. After that, we will point out the problems related to the control of the Darknet's work, especially those that are technology-related. Then we will analyse the existing legal norms available to members of the security system for legitimate monitoring, interception and analysis of Darknet. The conclusion of the paper deals with the collection and processing of digital evidence in order to prevent and prosecute perpetrators of criminal offenses.

The evolving strategic environment and strategic drivers of change determine the life of the contemporary man of the 21st century. Strategic drivers need to identify the most prominent ones, such as globalization, political geometry, demographic changes, climate change and the impact of new bio and nanotechnologies, as well as ICT and the Internet.

In September 2017 the European Cybercrime Centre (EC3) at Europol conducted Internet Organized Crime Threat Assessment (IOCTA) to inform the governmental bodies of the European police to shift its focus to cybercrime. They have set four top crime priorities:

- cyber-dependent crime;
- child sexual exploitation online;
- payment frauds;
- online criminal markets.

A cyber-dependent crime includes crimes that can only be committed using communication and information infrastructure (computers, servers, networks) and poses a real threat to the survival of modern society. Cyber-dependent crimes represent any threat to the loss of availability and integrity of the communication and information infrastructure, as well as any threat to the loss of integrity, availability and confidentiality of data in the cyber space. Cyber-dependent crimes can be divided into either negligent or malicious action of a user. In addition to these critical threats to cybernetic security, there are various other threats that affect human rights, identity of a person, intellectual property rights and other criminal offenses that pose a threat to the normal behaviour of users in cyberspace.

For conducting cyber-dependent crimes, most commonly, malicious computer content is used that expands through the existing communication and information infrastructure. Malicious content can be divided into four categories:

- spam;
- hoax;
- phishing;
- malware.

Spam is a malicious e-mail that aims to promote advertising content (mostly pornographic) or is a means of spreading malicious links. For his dissemination, he uses a variety of web sites, chat rooms, or blogs to collect email addresses and ultimately send malicious content. Unlike spam, hoax is a form of e-mail that does not cause harm, but only serves to spread untruthful content via e-mail or the Internet.

Phishing is a real criminal product through exploiting the vagueness and thoughtlessness of the user to collect key and secret personal information (such as username, password and other personal information) for financial gain. In phishing, the perpetrator uses a false identity by presenting itself as a financial institution that the user is a member of and asks him to update his security accreditation after which the perpetrator gains access to the victim's

financial services. There are a variety of types of phishing e-mails, from the simplest of which e-mails require access to the data, to the complicated approaches that send e-mails to sites that are fake as financial institutions sites.

Malware is a collective name for all types of malicious content whose purpose is to gain access to the computer system and data of users without their knowledge. Various viruses, worms, Trojan horses, ransomware programs, rootkits, spyware are included in the malware. Malware is closely related to the cybernetic crime itself because it is through it that it is realized. Once the perpetrator gets access to the desired computer system, he uses it further to blackmail the user or for further attacks to the real target.

A subcategory of Malware called Ransomware is today in common use. It is a malicious content that consists of two types of malware: Trojan and cryptolocker. The Trojan uses different holes in the system to make it noticeably plugged into the cybernetic system and spread to other computers on the network. After the "insert" into the cybernetic system, a cryptolocker is triggered that encrypts the user's file and asks for the ransom to restore the file to the previous state.

The 21st Century Information Environment

The world of the 21st century is a world where the use of information communication technologies determines the lives of people and creates their perceptions of events at the global, regional and local level. The power of media has multiple implications for the conclusion and creation of images of the world we are living in. Many of these facts are ready to be used to create an acceptable view of the world to their particular interest on the public interest account to the benefit of others. Manipulation enabled by the wide availability of information communication technologies is visible on a daily basis and is present in the most influential media infrastructure of today's Internet. The Internet is full of misinformation, conspiracy theories, gossip, which are unstoppable and with great speed of dissemination currently available to the modern people. In this overload with Internet information, it is difficult to distinguish truth from lies, good from evil, because creators of constant information attack on modern people are skilful and determined in their own way. [15]

The influence of media on contemplating of contemporary people is based on the principle: "Almost by definition […] a war waged on live television is a war in which political and public relations considerations become inextricably bound up with military tactics and strategy […] how victory is won is almost as important as victory itself." [23]

The modern world is facing a number of risks, such as the abuse of new technologies, especially ICT and the Internet, Cyberwars, Cyberterrorism and Cyber riot, Security of Critical National Infrastructure, Intellectual Property in Cyber Space, Networks and Networked Information Thinking, Censorship in Cyber Environment, Neutrality in Cyber Space, Privacy (GDPR) and Anonymity in Cyber Space.

The use and abuse of the Internet resource, for example, occurs at every moment, at all levels: surface web, deep web and especially the Darknet. Each of the above levels of the Internet is recognized from the point of view of its opportunities that are targeted, used and/or abused. Of course, in the further development of technology and also in the development of the legal system and legal norms, it is necessary to work on the opening of the space of use

and the closure of the space for abuse. It is important and unambiguous that internationally recognized socially unacceptable forms of behaviour on the Internet should be punished, no matter what its level is.

Abuse on the Surface Web

The reasons why the surface Internet is interesting are numerous: decentralization of infrastructures, easy access and anonymity, globalization of the world public, fast communication, cheap maintenance and web application development, news making…

Abuse on the surface web has many forms, especially those committed by violent extremists and terrorists with goals such as:

- publicity and propaganda in the form of psychological war in the service of networking as well as recruiting and mobilization of violent extremists and terrorists through the Internet forums;
- data mining of the targets and the information exchange—for instance on IED i.e. improvised explosive devices and possibilities to provide needed equipment;
- fund raising and donations for violent extremists and terrorists, etc.;
- planning and coordination of violent extremist and terrorist activities—along with preserving secrecy by coding the messages and communications.

Evidence of these is a number of websites such as: *Islamist Website, Jihadi Website, Terrorist Blog, Terrorist Forum*, Jihadists use mobiles as propaganda tools, *A Jihadist's Course in the Art of Recruitment,* Abu 'Amr's handbook.

FBI Director James B. Comey said that terrorist groups are turning to encrypted communications. He also said that the Islamic State has attracted at least 21,000 English-speaking followers on the Twitter social media platform, bombarding them with incitements to violence.

When the Islamic State operatives encounter a potential recruit, Comey said, "we see them giving directions" to move to a mobile messaging app that is encrypted, he said. "And they disappear." [10]

Terrorists Abuse WhatsApp

London terror suspect Khalid Masood sent a WhatsApp message to an unknown person just before Sunday's attack that killed four people and injured dozens. The message's contents—and its intended recipient—cannot be accessed by police because the popular, Facebook-owned messaging service encoded them. [8]

It is the burgeoning of these secret, inaccessible corners of the Internet that worries law enforcement agencies, which have been talking for several years about the dangers posed by criminals and terrorists who can now "go dark" by using strong encryption.

FBI Director James Comey said "That is a shadow falling across our work." "The darkness is spreading through the whole room", he also said last week at a security conference at the University of Texas at Austin. [14]

Amber Rudd, Secretary of State for the Home Department of the UK said: "We need to make sure that organizations like WhatsApp—and there are plenty of others like that—don't provide a secret place for terrorists to communicate with each other." [14]

Terrorists' Love for Telegram

Terrorism and intelligence experts have known for years that the encrypted messaging application Telegram is now the "app of choice" for terrorists and specifically for ISIS. [12] The ISIS members behind the 2015 Paris attacks used Telegram to spread propaganda. ISIS also used the app to recruit the perpetrators of the Christmas market attack in Berlin last year and claim credit for the massacre. More recently, a Turkish prosecutor found that the shooter behind the New Year's Eve attack at the Reina nightclub in Istanbul used Telegram to receive directions for it from an ISIS leader in Raqqa.

The Croatian Legal Framework for Information Security

The National Security Council and the Office of the National Security Council is on the first place. We can say that the Office of the National Security Council is like a "National Security Authority" and it performs administrative and professional staffs for the National Security Council. The Office of the NSC is a central state-level information security body that coordinates the adoption and monitoring of the application of measures and standards of information security in Croatia. [21]

The next important agency is the Computer Emergency Response Team (CERT). It is a national body for prevention and protection against computer threats to the security of public systems in Croatia. CERT deals with incidents if one of the parties is in Croatian or in the .hr domain or in the Croatian IP area. It is a member of the Forum of Incident Response and Security Teams (FIRST) and working group TF-CSIRT. [22]

The Information Systems Security Bureau (ISSB; Croatian acronym is ZSIS) is the Office for Security of Information Systems, the central state body for performing tasks in the technical areas of information security of the state bodies of Croatia, which include information security systems standards, security accreditation of information systems, cryptomatic management used in the exchange of classified information and coordination of prevention answers to computer threats to security of information systems. Also, it is responsible for regulating the technical areas of security information system safety regulations and their ongoing alignment with international standards and recommendations, and participates in national standardization of information system security areas. Standards of technical information security systems apply to all state bodies, units of local and regional self-government and to legal entities with public authority that use classified and unclassified data within their scope.

Together with these bodies, internet investigations, information security protection and the fight against abuse and misuse of the internet is under the jurisdiction of the Ministry of the Interior and the Ministry of Defence, for which separate departments were established.

The operational body established in the Republic of Croatia for the purpose of supervising the telecommunications operators' services is the Telecommunications Surveillance Operative-

Technical Centre (OTC). The legislation enacted in 2006 which is still effective today determines two agencies: the Security-Intelligence Agency (Croatian acronym is SOA) and the Military Security-Intelligence Agency (VSOA), i.e. civilian and military with operations at home and abroad, and the Telecommunications Surveillance Operative-Technical Centre, which is in charge of activation and management of measures for the confidential surveillance of telecommunications services, activities and traffic.

The laws of the Republic of Croatia allow the surveillance and legitimate interception of the Internet by the security intelligence agencies (SOA and VSOA) and the police.

The legal basis for the handling of security intelligence agencies is the Law on Security and Intelligence System of the Republic of Croatia, July 5, 2006. [24]

For the application of secret data collection measures to security intelligence agencies, a warrant is required from a Supreme Court judge.

"Article 33.

First secret surveillance of telecommunication services, activities and traffic:

a) secret surveillance of communications facilities,
b) the surveillance of telecommunications traffic data,
c) the surveillance of international telecommunications connections, […]

Third secret surveillance and technical recording of interior facilities, closed spaces and objects." [24]

Despite the capabilities and powers of the security services, the data and information they collect are not digital evidence for court proceedings in the Republic of Croatia. Even when they are based on suspicion that they indicate the perpetration of criminal offences for which they are prosecuted ex officio, and when the law is obliged to collect the collected data and information to the State Attorney's Office.

Since the police action must be proportional to threats, it usually goes hand in hand with actions that less distort the constitutionally guaranteed human rights and freedoms.

Such is, for example, the authority in Article 68. (the Act about police duties and powers) which enables them: "To reduce the risk, violence, prevention and detection of crimes for which the public prosecution, the police officer may from telecommunications service providers seek to: verify identity, duration and frequency of contact of certain telecommunication address." [24]

But when such measures are not enough then the ones that can be more effective are taken. If in the police surveillance and legitimate interception of data on the Internet the police are acting, then its powers come from the Code of Criminal Procedure, from October 11, 2011. [25] Special Collection of Evidence (Investigating judge-warrant):

"Article 332.

1) surveillance and technical recording of telephone conversations and other communications to remote,
2) the interception, collection and recording of computer data,
3) enter the premises for the purpose of conducting surveillance and technical recording of premises,
4) secret surveillance and technical recording of individuals and objects in dealing with the work of police officers in cases where there are reasonable grounds for suspecting that the abuse of Darknet is important to deter a perpetrator of a criminal offence in

committing a criminal offence. For these reasons, the legislator freed the police officer or civil servant in civil suit from the obligation of presentation." [25]

Law on police businesses and officials, June 30, 2009. [26]

"Article 17.

(1) A civil servant in a civilian suit shall be presented before the beginning of the application of police authority by displaying the official badge and the official identity card.

(2) A police officer in the chamber shall be presented by displaying the official badge and the official identification card at the request of the person to whom the police authority shall apply.

(3) Exceptionally, a police officer shall not be represented in the manner prescribed in paragraphs 1 and 2 of this Article if the circumstances of the application of police powers indicate that it could jeopardize the attainment of its objective.

(4) As soon as the circumstances referred to in paragraph 3 of this Article cease, the police officer shall be presented in the manner prescribed in paragraphs 1 and 2 of this Article.

(5) The provisions of paragraphs 1 to 4 of this Article shall not apply to the conduct of a police officer who undertakes concealed police actions: observation, escort, trap or, which under special law undertakes special evidence actions: monitoring and technical recording of telephone conversations and other remote communications, interception, collection and recording of computer data, entrance to the premises for supervision, secretly tracing and technical recording of persons and subjects and technical recording of rooms, use covert investigators and dependents, simulated sale and purchase of items and simulated bidding and simulated receipt of bills, providing simulated business services or concluding simulated legal transactions, supervised transportation and delivery of criminal offences." [26]

As police powers end up within the borders of a national territory, i.e. state, police actions that cross the state border are always possible to be questioned from the point of view of legality. Since the vast majority of police researches in the virtual environment, i.e. on the Internet, are such that they cross the boundaries of the national territory, they are legitimate only if we can legitimize them by international police co-operation. It is, therefore, important to rely on cooperation with, for example, Europol and/or Interpol in all such police proceedings.

Analysis of Computer Crime – Case Study Republic of Croatia (2004–2013)

The investigation of computer crimes is complex and demands a wide knowledge of technical distinctions between new technologies, primarily due to seeking for different types of evidence in digital form. There is a number of different definitions for computer crime. According to Dragičević: "If the term crime represents totality of criminal behaviour in a particular area within a certain period of time, then computer crime can be defined as totality of criminal offences committed on a computer system or by exploiting it in a certain field within a certain period of time." [6: 112] But according to Bača computer crime is: "A form of criminal behaviour of exploiting computer and information technology by using a computer as a tool or target to perpetrate criminal offence with relevant consequences according to criminal legislation." [4: 22] An inseparable term related to computer crime is digital evidence defined by the Criminal

Procedure Act of the Republic of Croatia (OG no. 152/08, 76/09, 80/11,121/11, 91/12,143/12, 53/13,145/13) as follows: "…electronic (digital) evidence is a data which is, as evidence in electronic (digital) form, obtained as stipulated by this Act." Digital evidence can also be explained as "any computer data which can either prove that criminal offence is committed or indicate a connection between" a criminal offence and an injured party, or "connection between criminal offence and its perpetrator" according to Protrka. [11: 2] Digital evidence combines text, images, audio and video recordings. We can only say that the investigation of a computer crime is very complex to carry out and that requires better knowledge of technical distinctions than the investigation of any other criminal offence, primarily due to its seeking for different types of evidence (electronic, i.e. electromagnetic type of evidence) as it deals with electronic equipment. [4]

This paper deals with computer crime in the Republic of Croatia for the period between 2004–2013 and analyses statistical indicators of computer crime based on the reports of the Ministry of the Interior on criminal offences referring to computer crimes and its perpetrators for the period between 2010–2013, according to K. Antoliš, I. Varjačić. [2] [13] The assumption is that the "dark figure of crime" of the reported development of computer crime is not connected with the increase in all reported criminal offences in the Republic of Croatia and that the computer crime rate is outstandingly low in all criminal offences in the Republic of Croatia. With regard to computer crime perpetrators, the assumption is that they are mostly males, the citizens of the RC, with a wide age span, and that on average, one perpetrator commits several criminal offences. Data analysis in this paper first represents data for the period between 2004 and 2012 and then for the year 2013, while for the period between 2004 and 2013 the data are united. There are two reasons for such data presentation, first, on 1 October 2004 Amendments to the Criminal Code harmonized with the Convention on Cybercrime entered into force introducing criminal offences related to computer crimes, and the second reason is that on 1 January 2013 the new Criminal Code entered into force in the Republic of Croatia.

Also, the analysis is carried out of the sentences pronounced to the perpetrators of computer crime in the RC according to the data of the Central Bureau of Statistics for the period 2009–2013; the year 2013 is analysed separately due to the new Criminal Code enforcement. It is assumed that the number of pronounced sentences is smaller in relation to the number of criminal offences for which the perpetrators are reported.

Computer Crime

Regarding the criminal law framework, it should be stressed that on 1 October 2004, the Amendments and Supplements to the Criminal Code were enforced. (Act on Amending and Supplementing the Criminal Code of the RC, OG no. 105/04) and that the data for 2004 include the period from 1 October 2004 to 31 December 2004. The mentioned Amendments to the Criminal Code define the following criminal offences: "Offences against the confidentiality, integrity and availability of computer data, programs or systems", "Offences related to child pornography on computer system or network", "Computer-related fraud".[5] Following that,

[5] See the complete legal description of offenses Act on Amendments to the Criminal Code, OG no. 105/04.

as mentioned in the introduction to this paper, on 1 January 2013 a "new" Criminal Code in the RC came into force (OG no. 125/11) in which criminal offences of cybercrime are separated in Chapter XXV. "Criminal offences against computer systems, programs and data", Article 266, "Illegal access"; Art. 267, "Computer system interference"; Art. 268, "Data interference"; Art. 269, "Illegal Interception"; Art. 270, "Computer-related forgery"; Art. 271, "Computer-related fraud"; Art. 272, "Misuse of devices", Art. 273, "Serious criminal offences against computer systems, programs and data".[6]

Looking nearly ten years back, we can see a development of computer crime in the RC. In the analysed period of time, the biggest number of the total reported criminal offences was recorded in 2010, while the analysis shows noticeable increase in each criminal offence in 2008, except for the criminal offences against Computer-related fraud, the highest number of which was reported in 2010 (903 criminal offences) making the biggest number of reported criminal offences in 2010.

The percentage of resolved criminal offences in 2004 and 2005 was 100%, with the smallest number of reported criminal offences in which 14 and 72 criminal offences were reported in 2004 and 2005, respectively. With the exception of these two years, the highest percentage of resolved offences was 97.3% in 2010, with the biggest number of reported offences. The average percentage of the resolved criminal offences analysed for the whole period of time was 93.64%, shown in Table 2. The number of reported, resolved and percentage of resolved criminal offences against computer crime in the RC for the period between 2004−2013 is given in Table 1.

Table 1. *Reported, resolved and percentage of resolved criminal offences of computer crime in the Republic of Croatia for the period between 2004−2013 according to the data of the Ministry of the Interior.* [19]

	Year									
	2004	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**
Reported Criminal Offenses	14	72	109	174	653	367	1,002	863	631	707
Resolved Criminal Offenses	14	72	103	165	625	338	975	813	553	642
% Resolved	*100%*	*100%*	*94.5%*	*94.8%*	*95.7%*	*92.1%*	*97.3%*	*94.2%*	*87.6%*	*90.8%*

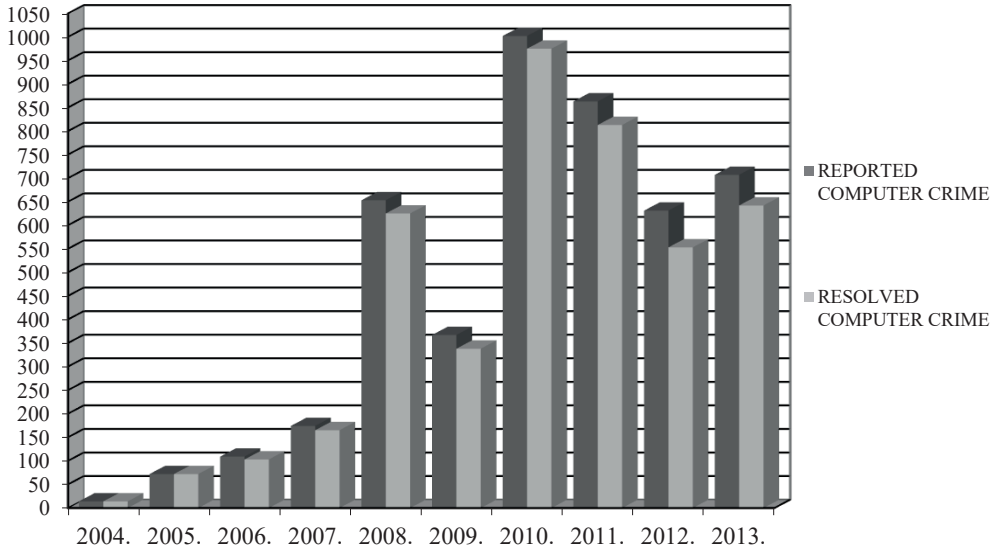
Table 2. *The total number of reported, resolved and percentage of resolved criminal offences of computer crime in the Republic of Croatia for the period between 2004−2013.* (According to the data from Table 1.)

	Reported	**Resolved**	**% Resolved**
Total Number	*4,592*	*4,300*	*93.64%*

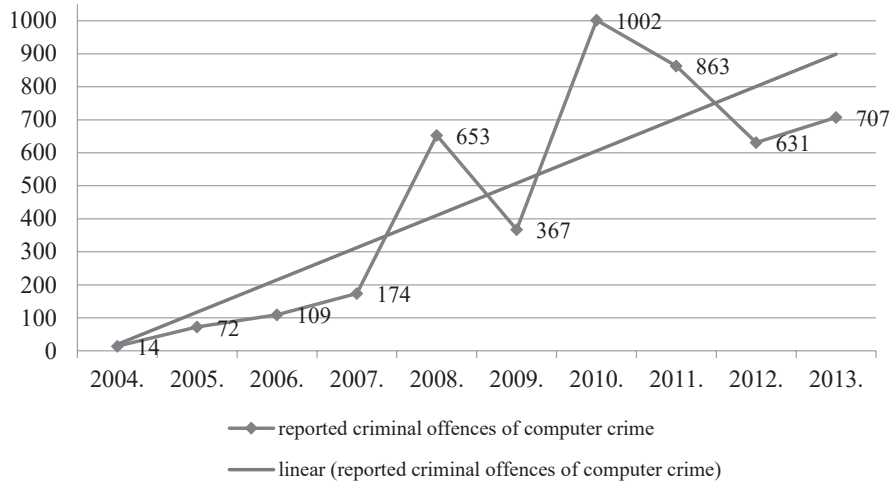
The conclusion is that the number of reported criminal offences had a linear trend of growth till 2008, followed by a decline after which the number of reported criminal

[6] See the complete legal description of offenses in Art. 266–273 in the Criminal Code OG no.125/11, 144/12.

offences increased; ultimately, it had the growth trend which is shown in Graph 2. Also, the ratio between the reported and resolved criminal offences shows a high percentage of the resolved criminal offences.

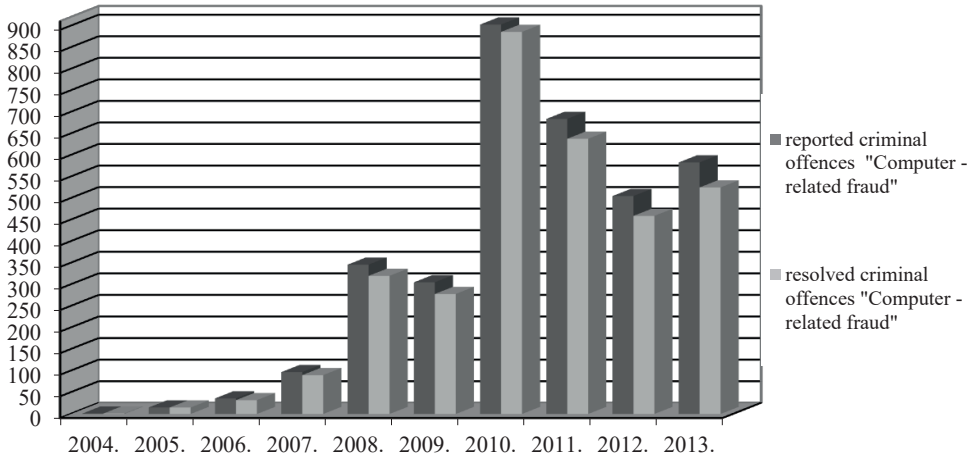


Graph 1. *Ratio of reported and resolved criminal offences of computer crime in Croatia for the period between 2004−2013.* (According to the data from Table 1.)



Graph 2. *Linear trend of growth in the number of criminal offences of computer crime reported in Croatia for the period between 2004–2013.* (According to the data from Table 1.)

The most numerous criminal offences in the analysed period of 10 years were "computer-related fraud", the total of reported offences were 3,475 and 3,244, i.e. 93.35% of them resolved. The percentage of criminal offences of computer crime in the RC is 75.67%. Also, it is apparent that the number of reported offences of computer crime had a linear trend of growth from 2004−2008, while in the period between 2009−2013 varied every year as shown in Graph 3.



Graph 3. *Ratio of reported and resolved criminal offences, "computer-related fraud" in Croatia for the period between 2004−2013 according to the data of the Ministry of the Interior.* [19]

Table 3. *Reported criminal offenses of computer crime, all reported criminal offenses and percentage of criminal offenses of computer crime in all reported criminal offenses in Croatia for the period between 2004−2013 according to the data of the Ministry of the Interior.* [19]

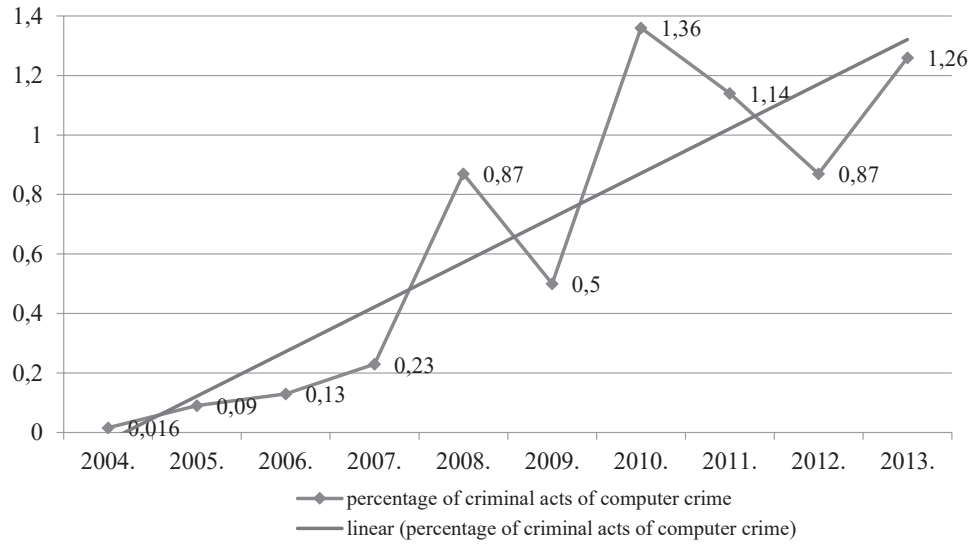
	2004	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**
"Computer crime"	14	72	109	174	653	367	1,002	863	631	707
All reported criminal offenses[7]	85,416	79,946	81,049	75,857	74,571	73,497	73,328	75,620	72,171	62,708
% Computer crime in all reported offenses	0.016%	0.09%	0.13%	0.23%	0.87%	0.50%	1.36%	1.14%	0.87%	1.26%

If we compare the number of reported criminal offences of computer crime with the total number of the reported criminal offences (for which criminal proceedings are instituted ex

[7] The data relating to criminal offenses for which the prosecution initiated ex officio.

officio), we can find out that the biggest number of the reported offences was in 2004, whereas the largest number of offences of cybercrime was in 2010. Comparing the development of all criminal offences of computer crime, we can see that computer crime does not follow the growth or decline of the reported criminal offences; the conclusion is that computer crime is not related to the total number of reported criminal offences.

Table 3 shows the data on the number of reported offences of computer crime, all reported criminal offences and percentage of computer crime in the period between 2004–2013. The percentage of computer crime in all criminal offences was 0.65%, if we exclude the year 2004, the average percentage was 0.72%. Graph 4 represents the percentage of computer crime in all criminal offences in the RC for the period between 2004 and 2013, showing its growing trend.



Graph 4. *The growth trend percentage share of criminal offenses of computer crime in all reported criminal offenses in Croatia for the period between 2004–2013.*
(According to the data from Table 3.)

Perpetrators of Computer Crime

To obtain information on perpetrators of computer crime, the data of the Ministry of the Interior reports on criminal offences of computer crime were analysed for the period 2010 to 2013. In that period the total of 3,203 criminal offences were reported which makes 69.75% of the total number of offences for the period between 2004 and 2013. Of 3,203 criminal offences, 2,983 were resolved, which is 93.13% including 401 physical persons and two legal entities reported, which represents a satisfactory sample for interpretation. According to the mean value, each perpetrator committed ≈ 7.4 criminal offences. Table 4 represents the analysis of perpetrators according to their age, divided into age groups

for each year of the analysed period. The age group of 29 to 39 years includes the greatest number of perpetrators, 115 of them. Distribution of perpetrators by age groups is shown in Graph 5, referring to the data in Table 4. By nationality, 85.5% of offenders i.e. 343 of them were Croatian citizens, while 58 of them were foreign citizens.

Most of them were males (330), i.e. 82%. 401 of them were physical persons (99.5%) and two legal entities. Data on gender of perpetrators and citizenship for the period 2010 to 2013 are shown in Table 5, while Graph 6 shows the percentage of perpetrators by their citizenship and Graph 7 by their gender.

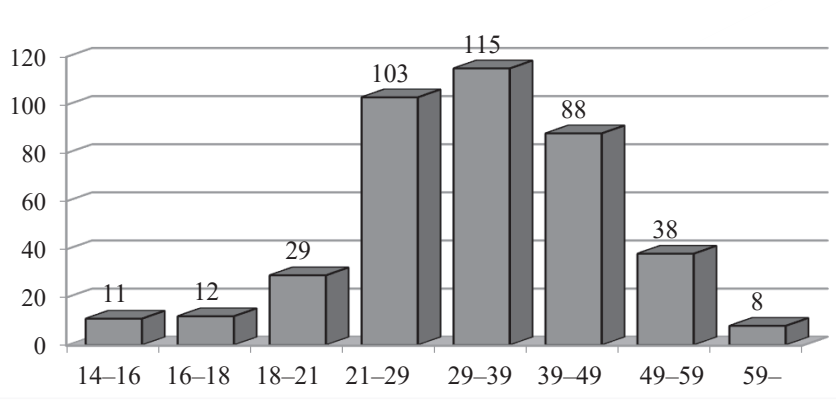
Comparison of data on the resolved number of computer crimes (Table 1) and data on the number of perpetrators (Table 4) shows that in 2010, the total of 83 perpetrators for 975 criminal offences were reported (≈ 11.75 criminal offences per a perpetrator), in 2011, the total of 142 perpetrators for 813 criminal offences (≈ 5.73 criminal offences per a perpetrator), in 2012, the total of 98 perpetrators for 553 criminal offences (≈ 5.65 criminal offences per a perpetrator) and in 2013, the total of 80 perpetrators for 642 criminal offences (≈ 8.02 criminal offences per a perpetrator) were reported.

Table 4. *Perpetrators of criminal offenses of computer crime according to age in Croatia for the period between 2010–2013 according to the data of the Ministry of the Interior.* [19]

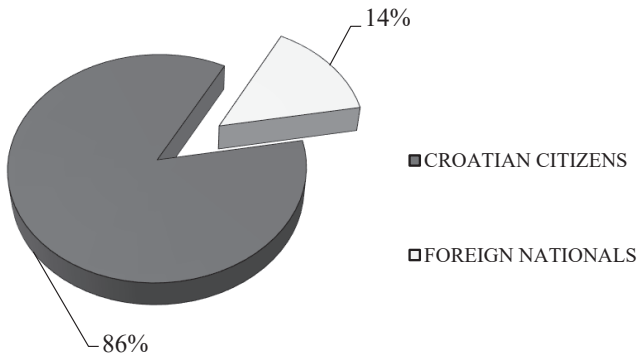
	Age							
	14–16	**16–18**	**18–21**	**21–29**	**29–39**	**39–49**	**49–59**	**59–**
2010	4	2	6	25	25	13	5	1
2011	4	5	12	32	39	37	10	3
2012	3	3	4	24	31	20	11	2
2013	/	2	7	22	20	18	9	2
Total	*11*	*12*	*29*	*103*	*115*	*88*	*35*	*8*
401								

Table 5. *Perpetrators of criminal offences by their gender and nationality in Croatia for the period between 2010–2013 according to the data of the Ministry of the Interior.* [19]

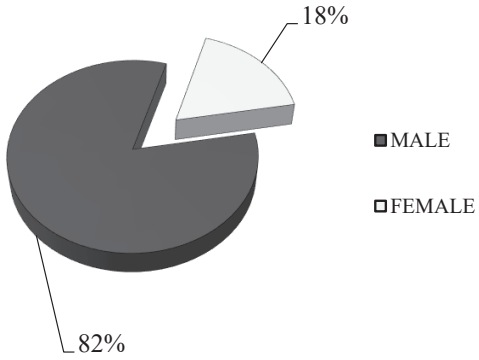
	Gender				**Nationality**	
	Female	**Male**	**Legal entity**	**Citizen**	**Foreign nationals**	**Croatian citizens**
2010	12	69	2	81	14	67
2011	30	112	/	142	19	123
2012	13	85	/	98	17	81
2013	16	64	/	80	8	71
Total	*71*	*330*	*2*	*401*	*58*	*343*



Graph 5. *Distribution of criminal offenders according to age groups in Croatia for the period between 2010–2013.* (According to the data from Table 4.)



Graph 6. *Criminal offenders according to nationality.* (Data from Table 5.)



Graph 7. *Criminal offenders according to gender.* (Data from Table 5.)

Sentences for Perpetrators in the Period 2009–2013

Analysis of the sentences pronounced over perpetrators of criminal offences of computer crime in the RC for the period 2009 to 2013 is based on the released data of the Croatian Bureau for Statistics. [20]

In the period from 2009 to 2012, 374 sentences were pronounced against perpetrators, the same period in which the perpetrators were discovered for 2,679 criminal offences shows a great disproportion between the number of sentences passed and the number of reports filed against the perpetrators of criminal offences. The growing number of sentences had a linear trend, from 51 to 125 sentences. Comparing the number of perpetrators reported in the period from 2010 to 2012 with the number of sentences pronounced, it was found that in 2010, 83 perpetrators were reported and 81 sentences were passed, in 2011, 142 perpetrators were reported and 117 sentences passed, and in 2012, 98 perpetrators were reported and 125 sentences pronounced and the total of reported perpetrators were 323 and 323 sentences pronounced. Table 6 shows the number of convictions against perpetrators for the period 2009–2012 according to years and criminal offences. Analysis found out that there were a total of 84 convictions for the criminal offence of child pornography on computer system or network, a total of 14 convictions for the offence against confidentiality, integrity and availability and 18 convictions for criminal offences of computer-related forgery and total of 258 convictions for criminal offences of computer-related fraud. It is evident that the most numerous convictions refer to computer-related fraud for which the biggest number of criminal offences were reported.

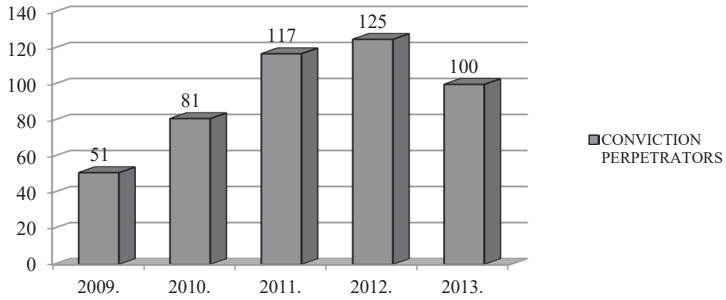
In 2013, a total of 100 sentences were pronounced (Table 7) and if that number is compared with the number of sentences from the years before, then a slight drop in the number of convictions can be seen. Most sentences (88) were passed for criminal offences of computer-related fraud, as expected. According to the data of the Ministry of the Interior in 2013, 80 perpetrators were reported for 642 criminal offences. If we compare the number of perpetrators which were police-reported with the number of convictions in 2013, the conclusion is that there were 25% more convictions than the number of the reported perpetrators which can mean that a number of offences were reported by the public prosecutor, not known to the police or, that during the procedure the criminal offence was classified differently or it was due to the completion of previous procedures. According to the data of the Ministry of the Interior, in 2013, three criminal offences of data interference were reported, four reports against criminal offences of illegal interception of data and ten reports against perpetrators committing criminal offence of misuse of device in 2013, for which there were no convictions.

Table 6. *Convictions of perpetrators for criminal offences of computer crime in Croatia for the period between 2009–2012 according to the data of the Croatian Bureau of Statistics.* [20]

	2009	**2010**	**2011**	**2012**	**Total**
Child pornography on a computer system or network					
Art. 197A para. 1	10	24	21	24	79
Art. 197A para. 2	3		1	1	5
Offences against confidentiality, integrity and availability of computer data, programs and systems					
Art. 223 para. 1		2		3	5
Art. 223 para. 2	2				2
Art. 223 para. 3		1	3	1	5
Art. 223 para. 4		1			1
Art. 223 para. 5		1			1
Computer-related forgery					
Art. 223A para. 1	2		3	2	7
Art. 223A para. 2			2		2
Art. 223A para. 3	5	1	1	2	9
Computer fraud					
Art. 224A para. 1	28	48	84	84	244
Art. 224A para. 2				2	2
Art. 224A para. 3	1	3	2	6	12
Total	*51*	*81*	*117*	*125*	*374*

Table 7. *Convictions of perpetrators for criminal offences of computer crime in Croatiafor the year 2013 according to the data of the Croatian Bureau of Statistics.* [20]

2013	
Unauthorized access	
Art. 266 para. 1	8
Art. 266 para. 2	1
Damage to computer data	
Art. 268 para. 1	1
Computer-related forgery	
Art. 270 para. 1	2
Computer fraud	
Art. 271 para. 1	82
Art. 271 para. 2	6
Total	*100*



Graph 8. *Convictions of perpetrators for the period between 2009–2013.* (According to the data from Tables 6 and 7.)

Table 8 shows the total of 115 prison sentences, 338 sentences of suspended prison, 4 fines for adults, 4 juvenile detentions, 11 juvenile warnings and 2 juvenile supervisions. Of 474 convicted perpetrators, 366 (77.21%) were males, which represent a smaller percentage than that of the police reported (82%). 13 sentences were pronounced for juveniles (2.74% of all sentences). The sentences pronounced over perpetrators according to age and gender for each year are shown in Table 9.

Table 8. *Pronounced sanctions by year for the period between 2009−2013.* (According to the data of the Croatian Bureau of Statistics.) [20]

Pronounced Sanctions						
	Prison	**Suspended Prison**	**Fine**	**Juvenile Prison-Suspension**	**Measures of Warning**	**Increased Supervision Measures**
2009	16	31	2	/	2	/
2010	25	52	/	3	1	/
2011	29	81	1	1	5	/
2012	26	96	1	/	/	2
2013	19	78	/	/	3	/
Total	*115*	*338*	*4*	*4*	*11*	*2*

Table 9. *Number of convicted perpetrators according to majority and sex in Croatia for the period between 2009−2013.* (According to the data of the Croatian Bureau of Statistics.) [20]

	Adult Perpetrators	**Juvenile Perpetrators**	**Total**	**Male**	**Female**	**Total**
2009	49	2	51	43	8	51
2010	80	1	81	65	16	81
2011	112	5	117	88	29	117
2012	123	2	125	95	30	125
2013	97	3	100	75	25	100
Total	*461*	*13*	*474*	*366*	*108*	*474*

Detailed presentation of the total of pronounced sanctions according to prison sentences ("P" in the table), suspended sentences ("S" in the table) and fines for every criminal offence for the period 2009−2013 is shown in Table 10. Analysis of the data on the mentioned sanctions[8] shows that the 6–12 month suspended prison sentences were pronounced in the greatest number (196)[9] followed by 3–6 month suspended prison sentences (111).

The greatest number of pronounced prison sentences (unconditional), were 3–6-month prison sentences (45), which makes 40% of prison sentences, they are followed by 6–12-month prison sentences (37). The strictest sentences were pronounced for the criminal offence of child pornography on computer system or network, 52 unconditional imprisonment (45% of all prison sentences) and 19 suspended prison sentences (17 sentences of 6–12 months in prison) and three sentences of 5–10 years in prison.[10]

This could be expected, as the strictest prescribed sentence is imprisonment. The lightest sentences were pronounced over perpetrators for the criminal offence of offences against the confidentiality, integrity and availability of computer data, programs or systems including 13 suspended sentences and one fine, five of them related to Item 1 for which the shortest sentence of all criminal offences is prescribed.[11]

For the most numerous criminal offences of computer-related fraud from Art. 224A para. 1, in the period 2009–2012, 243 sentences were pronounced, and 205 of them were suspended prison sentences (about 84%), mostly 6–12 month prison sentences (total 119), followed by 3–6 month prison sentences (total 70).[12]

Also, in 2013, computer-related fraud from Art. 271 para. 1, was the most numerous criminal offences for which 82 sentences were passed (82% of all sentences), 63 of them suspended prison sentences (about 77%), mostly 6–12-month prison terms (42 sentences) and 3–6-month prison terms (21 sentences).[13]

---

8 Compare with penalties prescribed in Articles 197A para. 1–2; 223 para. 1–5, 223A para. 1–3 and 224A para. 1–3. Criminal Code (OG no. 110/97, 129/00, 51/01, 111/03, 105/04, 84/05, 71/06, 110/07, 152/08) also and Art. 266 para. 1–2, Art. 268 para. 1, Art. 270 para. 1 and art. 271 para. 1–2. Criminal Code (OG no. 125/11, 144/12).

9 See detailed Art. 67 "suspended sentence" in Criminal Code (OG no. 110/97, 129/00, 51/01, 111/03, 105/04, 84/05, 71/06, 110/07, 152/08) and Art. 56 "suspended sentence" in Criminal Code (OG no. 125/11, 144/12).

10 Art. 197A para. 1 prescribes a punishment of imprisonment of 1–10 years, and paragraph 2 imprisonment for a term of six months to three years. Criminal Code (OG no. 110/97, 129/00, 51/01, 111/03, 105/04, 84/05, 71/06, 110/07, 152/08).

11 Art. 223 para. 1 punishable by a fine or imprisonment up to one year. Criminal Code (OG no. 110/97, 129/00, 51/01, 111/03, 105/04, 84/05, 71/06, 110/07, 152/08).

12 See detailed Art. 67 "suspended sentence" in Criminal Code (OG no. 110/97, 129/00, 51/01, 111/03, 105/04, 84/05, 71/06, 110/07, 152/08) in Art. 56 "suspended sentence" in Criminal Code (OG no. 125/11, 144/12).

13 Ibid.

Table 10. *Overview of pronounced sanctions according to prison sentences, sentences of suspended prison and fines to adult perpetrators for criminal offences of computer crime for the period between 2009–2013.* (According to the data of the Croatian Bureau of Statistics.) [20]

Pronounced Sanctions																	
	Prison																**Fine**
	Years								**Months**								
	5–10		**3–5**		**2–3**		**1–2**		**6–12**		**3–6**		**2–3**		**1–2**		
	P	**S**	**P**	**S**	**P**	**S**	**P**	**S**	**P**	**S**	**P**	**S**	**P**	**S**	**P**	**S**	
2009–2012																	
Art. 197a para. 1	3				2		5	1	11	13	30	1					
Art. 197a Para. 2										4	1						
Art. 223 para. 1										1		1		1		1	1
Art. 223 para. 2												1		1			
Art. 223 para. 3												3		2			
Art. 223 para. 4																1	
Art. 223 para. 5												1					
Art. 223a para. 1									1	4		2					
Art. 223a para. 2										2							
Art. 223a para. 3								2		2	1	2					2
Art. 224a para. 1			1		1		12	13	15	119	9	70		2		1	
Art. 224a para. 2												2					
Art. 224a para. 3							2	2	1	4		1	1				1
2013																	
Art. 266 para. 1										1	1	4		1			
Art. 266 para. 2										1							
Art. 268 para. 1												1					
Art. 270 para. 1										1		1					
Art. 271 para. 1							4	2	9	42	3	21				1	
Art. 271 para. 2							2			2							
Total	*3*	*/*	*1*	*/*	*3*	*/*	*25*	*20*	*37*	*196*	*45*	*111*	*1*	*7*	*/*	*4*	*4*

Conclusion for the Case Study of the Republic of Croatia

According to the research, a total of 4,592 criminal offences of computer crime were reported in the RC; for 4,300 of them the perpetrators were discovered (93.64% resolved). Their percentage in the number of criminal offences (instituted ex officio) was 0.72% on average (without data from the year 2004). In the analysed period, computer crime varied and was not dependent on fluctuations of other criminal offences. The most numerous criminal offences of computer-related fraud represent 75.67% of criminal offences (3,475).

In the period between 2010 and 2013, 403 perpetrators were reported for 2,983 criminal offences, which, according the mean value is ≈ 7.4 criminal offences per a perpetrator. Perpetrators are mostly Croatian citizens (85.5%) and males (82%). The age distribution of the perpetrators is wide and no significant data is obtained. A total of 474 sentences were pronounced, 346 of them (73%) for the criminal offence of computer-related fraud. According to the types of sanctions, most of them are suspended prison sentences (338), while the strictest sentences passed were for child pornography on computer system or network, 52 unconditional prison sentences (5–10-year imprisonment) and 19 suspended prison sentences. 461 adults were convicted and 13 juveniles (2.74%), mostly males (77.21%).

The results of the research proved the assumption that the development of computer crime in the RC is not related to the development of all other criminal offences and that the computer crime rate is very low.

Computer crimes in the RC are characterized by the "dark figure of crime" which can be explained by not reporting criminal offences by the injured party, disproportion is evident between the reported perpetrators, according to the data of the Ministry of the Interior and the number of pronounced sentences, which represents 2,983 reports in relation to 423 sentences.

This can be explained by a number of discarded reports by public prosecutors or by the court or by the court procedure changing the offence into extended criminal offence when filing the report on computer crime. [2] The results obtained in the research show that computer crimes in the RC are characterized by a prominent varying of the number of reported criminal offences, a high "dark figure of crime", high percentage of resolved offences and finally, a small number of convictions for perpetrators. [2] Characteristics of the perpetrators: they are physical persons, males, mostly citizens of the RC, while no particular result was obtained with regard to age.

Deep Web

The public information about the deep web is that it is currently 400 to 550 times the size of the World Wide Web. Deep Web contains 7,500 terabytes of data compared to 19 terabytes of data on the Web. The Deep Web contains almost 550 billion individual documents compared to 1 billion of the surface web. [9] Sixteen of the largest deep websites collectively contain about 750 terabytes of information—enough for yourself to exceed the size of the Web site forty-five times.

Deep Web is the largest growing category of new information on the Internet. The total content quality on Deep Web is 1,000 to 2,000 times the size of the Web. Deep Web content is very relevant to any information needs. More than half of the deep web content is contained in topic-specific databases. Full ninety-five percent of the deep web is publicly available (free).

Violent Extremists and Terrorists Abuse Darknet to Hide

Darknet is the hidden portion of the Internet that is only available through specialized browsers, Tor. It is not really a single entity but instead thousands of sites, most of them encrypted and all available only to those with information about how to find them and how to access them. [14]

"It's a place where all sorts of illicit activities can happen. It's the sort of place where you would go if you wanted to buy weapons," said Herb Lin, a senior research scholar for cyber policy at the Hoover Institution at Stanford University. [14]

The dark web also plays a key role in terrorists' overall communication strategy.

"One of the things they do is they train each other on how to run all the traffic on their Android mobile phones through the dark web so all their Internet and voice traffic is sent through encrypted channels and so unreadable by law enforcement," said Aaron Brantly, a Professor of cyber studies at the US Military Academy. [14]

Tor

Layered routing is one of the most widely used technologies by anonymization networks. The objective of the layered routing is to provide anonymous communication between the entities on the network. This analogy is called the onion. Each router, when receiving a message, "eats" one layer of such a "port". It works in a way that it uses its own encryption key, and thus provides the necessary data for routing the rest of the data structure. The remainder passed contains a message and routing instructions intended for all of the following routers. The last routing removes the last encryption layer. It also sends the original message to the destination.

The Tor Network functionality is based on the onion routing; speaking of pseudo anonymous (or anonymous) communication within a computer network developed by David Goldschlag, Michael Reed and Paul Syverson. [7] The onion routing is based on the mixed networks of David Chaum. In addition to mixed networks, it includes many modifications and upgrades of this technique. The most important is the introduction of the concept of the onion router. The goal of routing mail is to maintain the privacy of the sender's and recipient's message privacy while also protecting the content of the message while travelling through the network. That is exactly what we can do by using Chaum's mixed cascades.

So, the message travels through a network of proxy servers, and they call it the onion servers in this case and point the message unpredictably. It is being crypted before being transmitted between servers. This prevents unauthorized browsing of the message content, so-called eavesdropping. The basic advantage of the onion routing is the fact that for anonymous communication it is not necessary to work properly through all the servers with which the connection is made. It is important to emphasize that if an attacker still manages to access one or perhaps even a few servers, the user's animation is not compromised. Messages are in the Onion Routing (OR) network multiply encrypted, and this is precisely why the anonymity is not compromised. In order to gain control over all servers, it is possible to reconstruct the message path of the OR network.

Tor networking routers use special routing onions. They are used to establish a connection to send the message. The start-up router randomly selects a number of onion routers and sends a message to each. It contains a symmetric message decryption key, and the forwarding instructions

for the next router. These messages are encrypted with the public key of the appropriate router. Specifically, as the resulting layered data structure encrypted, it is first necessary to decrypt the outer layers in order to get inside.

VPN and IP Address

Provide users with the ability to send and receive data over public or shared networks as if their computers are locally connected. VPN allows: security, functionality, manageability, anonymity. The traffic between you and the VPN service you use is encrypted so it is impossible for someone to see what you are doing on the Internet. As long as you are connected to a VPN, you will have access to the entire Internet without any censorship that could affect you. You can access services and geographically limited web pages if you are using a VPN server located in the region where these services or websites are available. The servers you are connecting to will not see your IP address, they only see the VPN server address. You can surf the web, read your e-mails, or send important information on public networks, without the risk of someone spitting you.

For example, Netflix and YouTube may sometimes limit the display of content in a particular region. If you type the name in the search engine, you will get a response "Content not available in your region". Using VPN, you can hide your location. If a VPN has servers in the US, the services you use "think" that you are there, not in your home, wherever you are. VPN is also useful if you need to hide your identity when using peer-to-peer services, such as BitTorrent. Your Internet service providers can see data that travels through a VPN, but not where they are or where they come from. This is useful because it adds yet another level of privacy, but also because some operators are driving traffic through BitTorrent.

Special technological advances in communication have been achieved by a hybrid approach that integrates Tor and VPN communication techniques. There are two possibilities. The first possibility is that a user first connects to Tor, and then to the VPN. Another possibility is that a user first connects to the VPN, and then to Tor. Everywhere the two possibilities have their advantages and disadvantages, which are further explained in detail below.

Tor through VPN

In this configuration you connect first to your VPN server, and then to the Tor network before accessing the internet: your computer → VPN → Tor → internet; your apparent IP on the internet is that of the Tor exit node.[14]

[14] Crawford D. "Pros: Your ISP will not know that you are using Tor (although it can know that you are using a VPN), The Tor entry node will not see your true IP address, but the IP address of the VPN server, If you use a good no-logs provider this can provide a meaningful additional layer of security, Allows access to Tor hidden services. Cons: Your VPN provider knows your real IP address, No protection from malicious Tor exit nodes. Non-HTTPS traffic entering and leaving Tor exit nodes is unencrypted and could be monitored, Tor exit nodes are often blocked. We should note that using a Tor bridge can also be effective at hiding Tor use from your ISP (although a determined ISP could in theory use deep packet inspection to detect Tor traffic)." [5]

VPN through Tor

This involves connecting first to Tor, and then through a VPN server to the internet: your computer → encrypt with VPN → Tor → VPN → internet.

This setup requires you to configure your VPN client to work with Tor, and the only VPN providers we know of to support this are AirVPN and BolehVPN. Your apparent IP on the Internet is that of the VPN server.[15]

Some Challenges

When using Tor, the last exit node in the chain between your computer and the open internet is called an exit node. Traffic to or from the open internet exits and entries leaves this node unencrypted. Unless some additional form of encryption is used (such as HTTPS), this means that anyone running the exit node can spy on the users' internet traffic. SSL connections are encrypted, so if you connect to an SSL secured website (https://) your data will be secure, even if it passes through a malicious exit node.

End-to-end timing attacks is a technique used to de-anonymize VPN and Tor users by correlating the time they were connected, to the timing of otherwise anonymous behaviour on the Internet. An incident where a Harvard "bomb-threat idiot" got caught while using Tor is a great example of this form of de-anonymization attack in action, but it is worth noting that the culprit was only caught because he connected to Tor through the Harvard campus WiFi network. If such an attack (or other de-anonymization tactic) is made against you while using Tor, then using VPN as well will provide an additional layer of security.

Speed is a limiting factor in the use of communication techniques with a high level of anonymity, as evidenced by the concrete outcomes of the communication analysis presented in the following illustrations.

---

[15] Crawford D. "Pros. Because you are connected to the VPN server through Tor, the VPN provider cannot 'see' your real IP address – only that of the Tor exit node. When combined with an anonymous payment method (such as properly mixed Bitcoins) made anonymously over Tor, this means the VPN provider has no way of identifying you, even if it did keep logs, Protection from malicious Tor exit nodes, as data is encrypted by the VPN client before entering (and exiting) the Tor network (although the data is encrypted, your ISP will be able to see that it is heading towards a Tor node), Bypasses any blocks on Tor exit nodes, Allows you to choose server location (great for geo-spoofing). All internet traffic is routed through Tor (even by programs that do not usually support it). Cons. Your VPN provider can see your internet traffic (but has no way to connect it to you). Slightly more vulnerable to global end-to-end timing attack as a fixed point in the chain exists (the VPN provider)." [5]

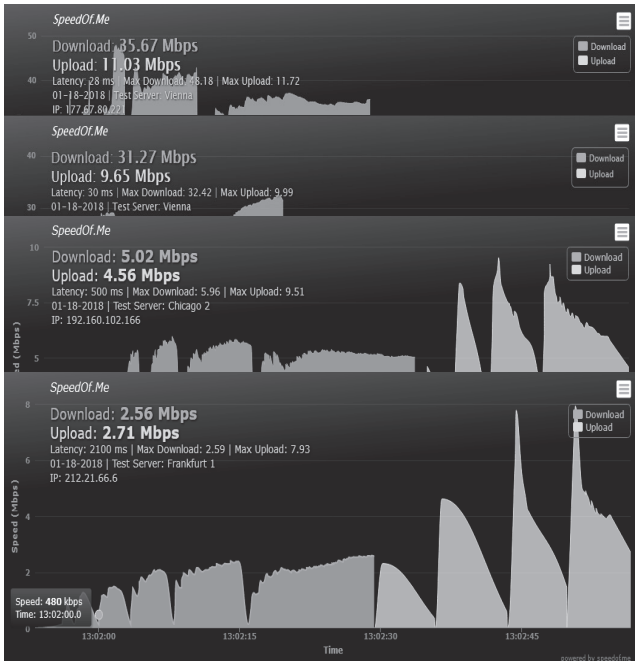


Figure 1. *Comparative view of how much speed is a limiting factor in the use of communication techniques with a high level of anonymity.* (Created by the authors.)

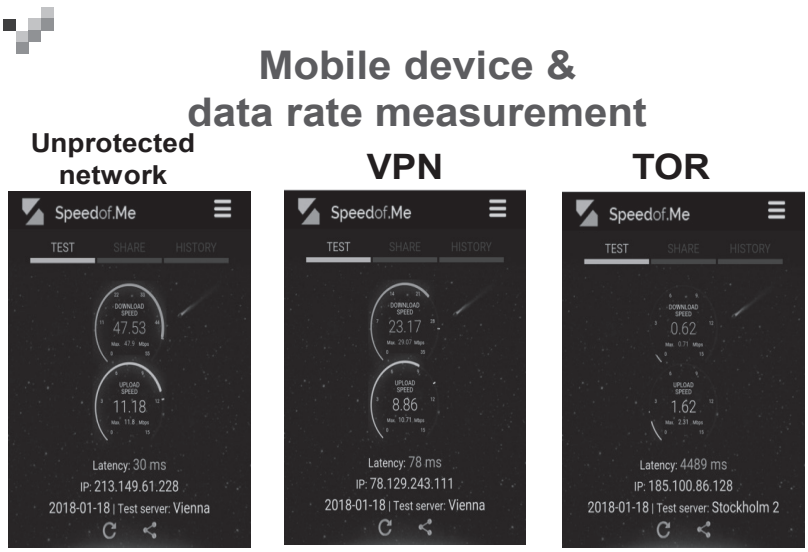


Figure 2. *Comparative view of how much speed is a limiting factor in the use of communication techniques with a high level of anonymity using a mobile device.* (Created by the authors.)

Conclusion

Numerous cases of police practice confirm that new information-communication technologies are abused by criminals, violent extremists and terrorists. The abuse of new technologies is not overwhelming. The goal of a high level of anonymity is achieved in full. In order for the police to cope with these abuses, they must be provided with hardware, software and human resources. A small police, such as the one of Croatia does not have the strength to develop hardware and software, so it needs to be purchased from partner countries. The Croatian police have created an organizational framework for combating cybercrime, which needs to be filled with experts in the field of combating cybercrime. Completing a structured organizational structure with a quality staff should not be a big problem since the Croatian Academic Community creates human resources that can handle the most demanding technological challenges. It is only necessary that police managers allow them to be employed in the police, so that they can be actively involved in combat teams against all forms of cybercrime as soon as possible.

References

[1] ANTOLIŠ, K.: Police Investigation and Abuse of Darknet. *9th International Conference "Days of Corporate Security 2018"*, 14.03.2018, Ljubljana.

[2] ANTOLIŠ, K., VARJAČIĆ, I.: Analysis of Computer Crime in the Republic of Croatia. *Suvremeni promet*, 32 3–4 (2015), 231–238.

[3] ANTOLIŠ, K.: Internet forensics and cyber terrorism. *Journal: Police and security,* 19 1 (2010), 121–128.

[4] BAČA, M.: Introduction to Computer Security. *The Official Gazette*, (2004).

[5] CRAWFORD, D.: *Using VPN and TOR together.* 2016. www.bestvpn.com/using-vpn-tor-together/ (Downloaded: 19.03.2018)

[6] DRAGIČEVIĆ, D.: *Computer Crime and Information Systems. Zagreb,* IBS – Informatorov biro sustav d.o.o., 2004.

[7] GOLDSCHLAG, D., REED, M., SYVERSON, P.: Onion Routing communications of the ACM for Anonymous and Private Internet Connections. *Communications of the ACM,* 42 2 (1999), 39–41. www.cs.bgu.ac.il/~dsec121/wiki.files/j2b.pdf (Downloaded: 19.03.2018)

[8] KATZ, G.: UK minister: WhatsApp must make itself accessible to police. *The Times of Israel* (online), 26 Match 2017. www.timesofisrael.com/uk-minister-whatsapp-must-make-itself-accessible-to-police/ (Downloaded: 19.03.2018)

[9] MARJANOV, S.: Šta je to Deep Web? (What is Deep WEB?) *saznaj novo* (online), 04.04.2015. www.saznajnovo.com/2012/07/sta-je-to-deep-web/ (Downloaded: 19.03.2018)

[10] NAKASHIMA, E.: FBI chief: Terrorist group turning to encrypted communications. *The Washington Post* (online), July 8, 2015. www.washingtonpost.com/world/national-security/fbi-chief-terror-group-turning-to-encrypted-communications/2015/07/08/89167f74-2579-11e5-aae2-6c4f59b050aa_story.html?utm_term=.7a219b3a255e (Downloaded: 19.03.2018)

[11] PROTRKA, N.: Computer data as an electronic (digital) evidence. *Journal: Police and Security,* 20 1 (2011), 1–13.

[12] TAN, R.: Terrorists' love for Telegram. *Vox* (online), Jun 30, 2017. www.vox.com/world/2017/6/30/15886506/terrorism-isis-telegram-social-media-russia-pavel-durov-twitter (Downloaded: 19.03.2018)
[13] VARJAČIĆ, I. : *Computer crime and digital evidence*. Zagreb, Police Academy, 2014.
[14] WEISE, E.: 2017. Terrorists use the Dark Web to hide. *USA Today* (online), Mar 28, 2017. www.usatoday.com/story/tech/news/2017/03/27/terrorists-use-dark-web-hide-london-whatsapp-encryption/99698672/ (Downloaded: 19.03.2018)
[15] WILSON, E.: *The Dual State: Para politics, Carl Schmitt and the National Security Complex*. London and New York: Routledge, Taylor & Francis Group, 2016.
[16] *Convention on Cybercrime.* Chart of signatures and ratifications of Treaty 185. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (Downloaded: 01.10.2014)
[17] Criminal Code. *The Official Gazette of the Republic of Croatia "Narodne novine"*, number: 110/97, 27/98, 50/00, 129/00, 51/01, 11/03, 190/03, 105/04, 71/06, 110/07, 152/08, 125/11 and 144/12.
[18] Criminal Procedure Act. *The Official Gazette of the Republic of Croatia "Narodne novine"*, number: 152/08, 76/09, 80/11,121/11, 91/12,143/12,53/13,145/13
[19] Ministry of the Interior of the Republic of Croatia, Statistics:
Overview of basic indicators for public saftey in the Republic of Croatia for 2004–2013. www.mup.hr/UserDocsImages/statistika/2014/PREGLED_OSNOVNIH_POKAZATELJA_JAVNE_SIGURNOSTI_%20U_RH2004.%20%E2%80%93%202013.pdf (Downloaded: 04.10.2014)
Survey of safety indicators in 2010. www.mup.hr/UserDocsImages/statistika/2011/statistika2010.pdf (Downloaded: 27.10.2014)
Survey of safety indicators in 2011. www.mup.hr/UserDocsImages/statistika/2012/pregled%202011.pdf (Downloaded: 28.10.2014)
Survey of safety indicators in 2012. www.mup.hr/UserDocsImages/statistika/2013/statistika2012.pdf (Downloaded: 29.10.2014)
Survey of safety indicators in 2013. www.mup.hr/UserDocsImages/statistika/2014/Statisticki%20preg2013_konacni%20prom_WEB.pdf (Downloaded: 30.10.2014)
[20] Republic of Croatia, Central Bureau of Statistics. Publications by Statistical Subject Matter Areas, Administration of Justice. www.dzs.hr/ (Downloaded: 19–20.11.2014)
Adult Perpetrators of Criminal Offences, Complaints, Charges and Convictions 2009, Statistical reports (SR) 1421. (2010)
Adult Perpetrators of Criminal Offences, Reports, Accusation and Convictions 2010, Statistical reports (SR) 1451. (2011)
Adult Perpetrators of Criminal Offences, Reports, Accusation and Convictions 2011, Statistical reports (SR) 1478. (2012)
Adult Perpetrators of Criminal Offences, Reports, Accusation and Convictions 2012, Statistical reports (SR) 1504. (2013)
Adult Perpetrators of Criminal Offences, Reports, Accusation and Convictions 2013, Statistical reports (SR) 1528. (2014)
Juvenile Perpetrators of Criminal Offences, Complaints, Charges and Convictions 2009, Statistical reports (SR) 1422. (2010)

Juvenile Perpetrators of Criminal Offences, Reports, Accusation and Convictions 2010, Statistical reports (SR) 1452. (2011)
Juvenile Perpetrators of Criminal Offences, Reports, Accusation and Convictions 2011, Statistical reports (SR) 1479. (2012)
Juvenile Perpetrators of Criminal Offences, Reports, Accusation and Convictions 2012, Statistical reports (SR) 1505. (2013)
Juvenile Perpetrators of Criminal Offences, Reports, Accusation and Convictions 2013, Statistical reports (SR) 1529. (2014)

[21] *The Office of the National Security Council.* Republic of Croatia. www.uvns.hr/hr (Downloaded: 21.03.2018)

[22] *National CERT.* Republic of Croatia, Computer Emergency Response Team. www.cert.hr/onama/ (Downloaded: 21.03.2018)

[23] *Washington Post*, March 24, 2003.

[24] *Act on Security and Intelligence System of the Republic of Croatia.* July 5, 2006.

[25] *Code of Criminal Procedure.* October 11, 2011.

[26] *Act on Police Businesses and Officials.* June 30, 2009.

AARMS Vol. 17, No. 3 (2018) 47–62.

Social Media and Terrorism[1]

Péter BÁNYÁSZ[2]

Today, terrorism is one of the most significant security risks. The spread of infocommunication technologies (ICT) resulted in new types of challenges. Innovation in ICT tools represents new means that terrorists, law enforcement and armed forces have to face. Some of the actions on different platforms of social media can be included here, which can be considered a challenge for all these organizations trying to adapt to them. Today we cannot talk about cyberterrorists and cyberterrorism, nevertheless this does not mean that terrorists would not use the cyberspace or that this platform would not mean a significant threat. This study aims to examine the correlation between social media and terrorism, including psychological operations and intelligence to several other areas.

Keywords: *terrorism, social media, Islamic State, PSYOPS, OSINT, social engineering*

Introduction

Cyber threats are categorized into four groups in the literature. These are: [1]

- cybercrime;
- cyberterrorism and hacktivism;
- cyber espionage;
- cyber warfare.

The purpose of cybercrime is to gain material benefit using IT systems, its targets can be both business and political actors. [2] Although hacktivism and cyber terrorism are conceptually two different phenomena, common points can be identified. In both cases, we can talk about decentralized, small groups, whose purpose is to represent the ideology they advocate before a larger media attention. Hacktivists basically consider the free access to information one of the most important values, and they carry out their attacks for this purpose. The concept of cyberterrorism was first used in the mid-1980s but there is still no generally accepted definition for it. [3] According to Keith Lourdeau *"Cyberterrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda."* [4] In case of hacktivism, a paradigm shift can also be seen; instead

[1] The work was created in commission of the National University of Public Service under the priority project PACSDOP-2.1.2-CCHOP-entitled "Public Service Development Establishing Good Governance" in the Concha Győző Doctoral Program.

[2] Ph.D. candidate, Assistant Lecturer, National University of Public Service, E-Governance Institute; e-mail: banyasz.peter@uni-nke.hu

of amateurs, professionals well supported by politics use this tool, who many times attack with a military purpose, such as the hacktivists of the Islamic State or the Syrian Electronic Army. [5]

However, we can tell that, fortunately, there are no cyber terrorists at the moment, although there are terrorists who use the Internet. Cyber espionage means the intelligence activities of states or market players are carried out on IT tools, and cyber warfare occurs in case of conflicts between states, in which conventional warfare is supported (or triggered) in order to render the information systems of the opponent state completely inoperative.

Terrorism can also be identified as one of the most significant security risks because it unites the toolkit of cybercrime and cyber espionage and aims to create such a capability with which it is empowered to carry out cyber warfare related actions. However, social media was initially a means of communication, but its spread and ever-expanding functions provide many opportunities for both terrorists and criminals.

The Emergence of Cyberterrorism in the Scientific Community

I've conducted a keyword analysis using the Scopus database. Scopus, founded in 2004, is the largest abstract and citation database of peer-reviewed literature, which enables the analysis of scientific journals, books and conference proceedings. I've built my database based on the keyword "cyberterrorism" using Scopus. The search concerned every scientific statement that included the search term "cyberterrorism" in its title, abstract or keywords. The database, similarly to Google search, only interprets the connection between words based on several keywords if they are in quotation marks, otherwise every result will be displayed that include the terms "cyber" or "terrorism". The search was conducted with this restriction. I've examined the result list according to scientific domain distribution.

The reason for the keyword analysis is the fact that the more frequently a certain keyword occurs the more relevant it can be viewed. I've conducted a trend analysis based on the occurrence of relevant keywords in order to examine whether a pattern could be determined for the proliferation of single keywords.

Further, I've conducted an international examination by limiting the scope to Hungary in order to find out how researches related to Hungarian cyber security are fitting in global trends.

Up until 2018, to August 2018 included, Scopus found 188 results on the search term "cyberterrorism". Figure 1 shows the scientific domain distribution of statements.

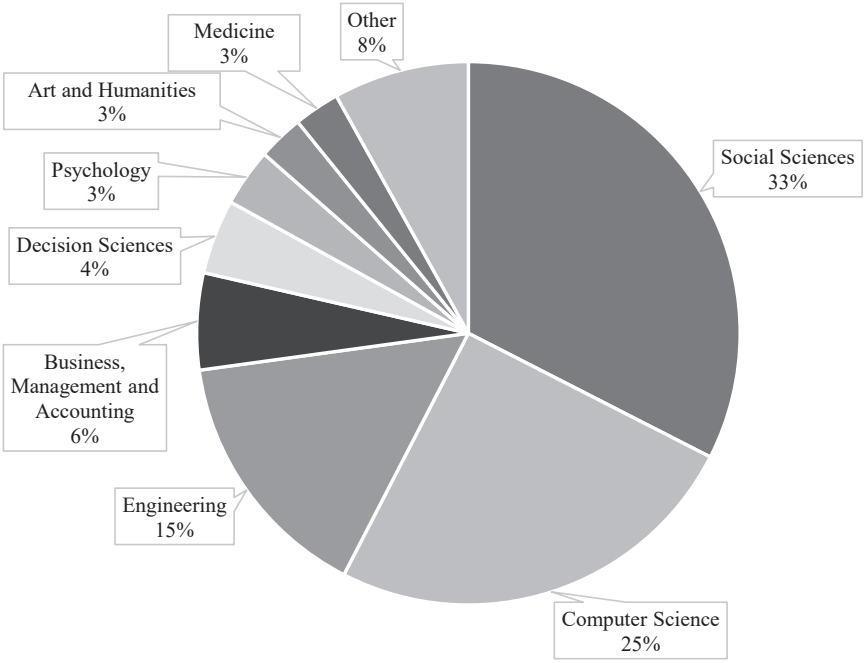


Figure 1. *Distribution of the search terms cyberterrorism globally per scientific domains according to Scopus.* [Based on Scopus; edited by the author.]

As shown in the figure, publications of technical nature are dominating researches related to cyberterrorism, 32.2% of all publications can be subject to Social Sciences and 24.8% to the scientific domain of Computer Science.

Table 1 shows the distribution of each publication according to country based on the top 8 countries.

Table 1. *Top 8 distribution amongst countries on the search term cyberterrorism.* [Based on Scopus; edited by the author.]

Country	Documents
United States	68
United Kingdom	25
Ireland	7
Australia	6
Netherlands	6
Germany	5
Israel	5
South Korea	5

Scopus database only stores 3 scientific statements after narrowing down the scope to Hungary. 100% of all publications can be subject to Social Sciences.

Figure 2 contains the yearly distribution of each publication. It is apparent that the first result for the search term cyberterrorism can be dated back to 1997.

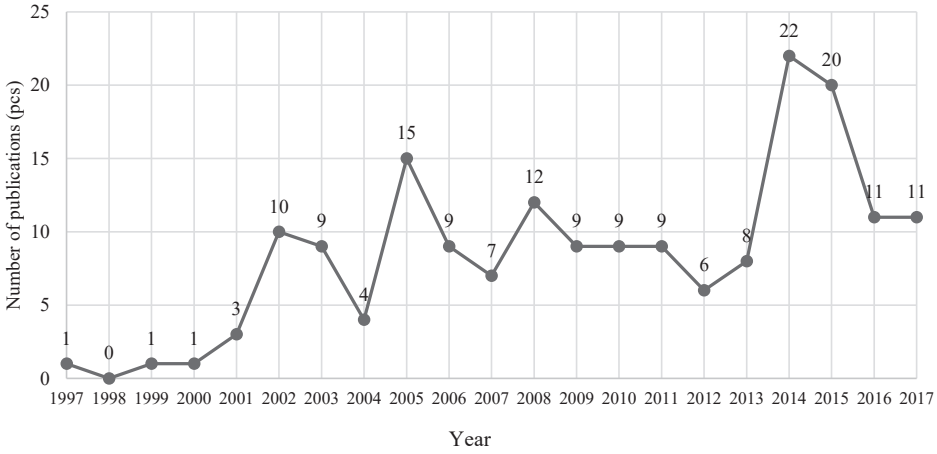


Figure 2. *Yearly distribution of the number of publications globally based on the search term cyberterrorism.* [Based on Scopus; edited by the author.]

The trend of the number of Hungarian publications is represented in Table 2.

Table 2. *Yearly distribution of the number of publications in Hungary based on the search term cyberterrorism*
[Based on Scopus; edited by the author.]

Year	Documents
2009	2
2006	1

The publications include overall 459 keywords, which needed to be narrowed down in order the manage them in a consistent manner. This was justified by the use of the singular and plural form of each keyword, by their different spelling,[3] and typos. In table 3 I've displayed those search terms where the result rate was over 3.

Table 3. *Occurrence of keywords in scientific statements for results on the search term cyberterrorism.* [Based on Scopus; edited by the author.]

Keyword	Occurrence
cyberterrorism	59
terrorism	25
internet	20
cybercrime	12

[3] For example cyber terrorism, cyberterrorism, Cyber terrorism, Cyber Terrorism, Cyberterrorism.

Keyword	Occurrence
cybersecurity	11
security	7
cyberspace	7
propaganda	5
postmodernism	5
networks	5
hacking	4
information security	4
cyberwar	4
counterterrorism	4
cyberattack	4
attack	3
critical infrastructure	3
cyber threat	3
semiotics	3

I've built another database based on the keyword "cyberterrorism" and "social media" using Scopus and found 3 results. The publications include overall 9 keywords. In table 4 I've displayed those search terms.

Table 4. *Occurrence of keywords in scientific statements for results on the search term cyberterrorism and social media.* [Based on Scopus; edited by the author.]

Keyword	Occurrence
cyberterrorism	2
affiliation	1
authur pendragon	1
cyber threat	1
mimetic virus	1
rumor mongering	1
social attachment model	1
social media	1

Social Media and Cyberterrorism

Numerous attempts have been made to define social media, the vast majority of which are related to the field of marketing, which at the same time bears the impression that it operates primarily with marketing-related concepts. The online Oxford Dictionary [6] describes social media as a set of web pages and applications that allow users to create and share content on social networks. This concept originates from Andreas Kaplan and Michael Haenlein, according to whom, social media is a *"set of internet applications that builds upon the ideological and technological basis of Web 2.0, which promotes the creation and transformation of user-generated content."* [7: 61]

Accepting the concept of Kaplan and Haenlein, but complementing the definition, social media is considered to be a set of web pages and applications in which the service provides

only the main frameworks, but the content is generated by the users. It follows that social media consists of primarily the interactions of users and, including the share or supplement of other users' content which can mean the production of totally new content. Theoretically, this content may change or expand by the effect of new information. Social networking sites have become a part of our daily lives: the inevitable parts of homes, workplaces, schools and leisure. Figure 3 shows the most popular social web sites.

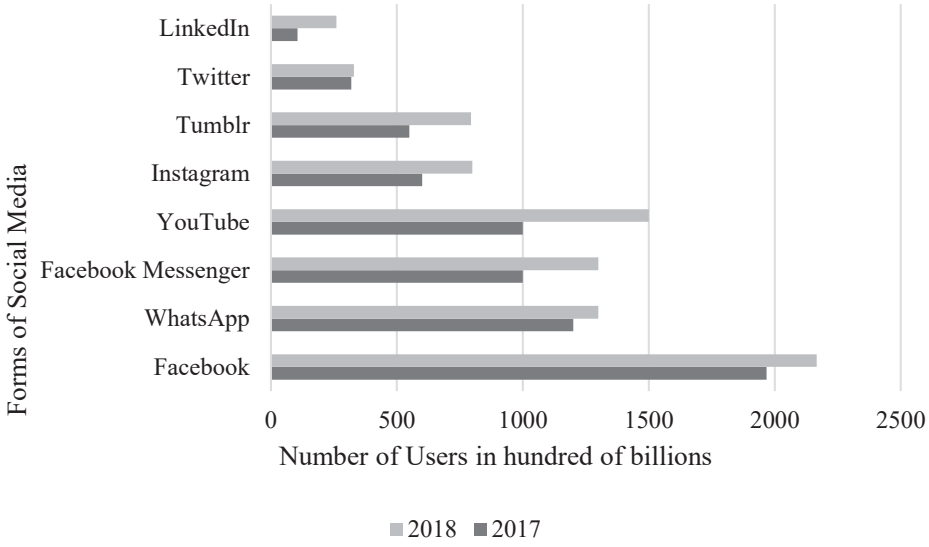


Figure 3. *Social media sites by visits globally 2017–2018.* [8] [Edited by the author.]

It is no exaggeration to say that social networking sites have been used by Islamic State terrorist groups in a paradigm shift way. In the followings, the areas of application how terrorists use or might use social media sites will be examined through the example of the Islamic State. Terrorists can use these websites for the followings:

- obtaining information;
- social engineering;
- contacting;
- propaganda;
- recruiting new members;
- receiving supporters;
- committing psychological operations;
- cyber-attacks.

Although the importance of the Islamic State has diminished considerably by today, the procedures and technics used by them, in my view, can be considered the examples of how future terrorist groups would use social media sites.

Obtaining Information and the Social Media

When designing a terror attack, selecting the target, spot, date, tools and methods mean the starting points. Collecting the right information is essential for which the *open-source intelligence* (OSINT) is an important tool. Following the concept of Lévay Gábor *"OSINT means the research, collection, selection, analysis-evaluation and use of not-classified data which are legally and publicly available (for everybody) based on professional aspects besides the military intelligence."* [9:6] Taking into account that open-source intelligence can be carried out by anybody, and scouts and operators of terrorist groups can obtain a huge amount of information from the internet and social media sites, the right data and information sensitivity have become crucial. [10] However, the OSINT is a necessary but not a sufficient condition of intelligence. In case the target of a terrorist group is a traffic subsystem, even though they have access to the Google Earth, satellite images of the area taken by Street View, or 3D panoramic photos, the going-over of the area cannot be neglected. Social media is the golden mine of the open-source intelligence. One of the main reasons is that the average users of these sites do not have sufficiently high data and information awareness so they share many moments of their lives. The longer and the more social media sites are used, the more detailed profile can be built up about the user—in case the visibility is not limited.

The activity itself can be really long if the operator is not familiar with the methods, but there are websites that accelerate it.[4] We need the ID Number of the target person which can be obtained by websites generating ID Numbers.[5] For this, the link of the Facebook profile of the target person should be copied to the website, and the ID number will appear in a few seconds. Then, the ID number should be pasted to the right cell to get the required information. Such information can be for example the places we have visited, what pages we have liked, the groups we are members of, images, posts liked or commented by us, events we have registered, colleagues, friends, etc. It is important to note that the website will display only the open-source information. This means it will not display anything which are not publicly shared, nor the personal messages. The majority of these information can be blocked also, but in case we comment under the post of a friend who has not limited the visibility of the post, then our comment will be displayed as well.

On the other hand, there are information which cannot be blocked, page likes, the list of applications which we have used, membership of groups, etc. In case we do not know our target person, fortunately (?) we can still browse[6] based on several variants if we know some information about this person, e.g. address, age, what he/she likes, etc. This way, we can select the targets based on the given features, who can be taken under further examination later. Of course, users will be displayed only if they have let the visibility open on their pages.

In my opinion, the applications developed for smart devices mean a kind of grey zone of open-source intelligence, that require certain permissions in return for the use. Every application, being free or paid, requires different permissions. These can be varied, but normally require only essential permissions for the application's function. In case of

[4] A good example is the webpage of www.uk-osint.net/facebppl or the https://inteltechniques.com/OSINT/facebook.html

[5] See also http://lookup-id.com/

[6] See also www.peoplefindthor.dk/

a flashlight application, it is adequate to access to the flash, likewise in case of a dictaphone application to the microphone control and to device's storage and modify it, in case of a messenger to our messages, or a photo application should have access to the camera, etc. The problem comes when the users are not careful enough when installing an application, and they do not read what permissions they give for the application. The application then may also get such permissions which are not necessary for their function. The information gathered this way, which can consist of everything stored on our mobile devices, are later sold for marketing purposes, but they can become the tool of target monitoring because a camera or microphone control, or the access to the user's messages let the developers of the application monitor and intercept the user at any time even real time. Not to mention, that some applications store medical data about us,[7] the security of which is extremely important. We can add a list of things we are allergic of, which can be important in case of emergency. This is really important and useful, but the problem is that if the security of our devices is not appropriate, the applications can obtain all stored information. This can be circumvented by offering food containing the ingredients the potential victim is allergic of, and being consumed these ingredients can cause harm.

It is a grey zone because even though the user gives several permissions for the applications in return for the use, this can relate to information which cannot be classified as open information at any time. The geo-positioning, the list of our friends, our profile photo can be open information in case the user treats them as open information, but the question of whether our friends treat their own networks as open information arises. Besides the already mentioned examples, we can permit the access to our messages, which, in my opinion, cannot be classified as open information at any time.

Social Engineering and Social Media

Collecting information does not play a role only in designing, but it is essential also in social engineering. The social engineering is a form of attack when the attacker exploits human factors[8] to gain access to protected information or systems by deceit or extortion. [11] According to Kevin D. Mitnick[9] *"The social engineering deceives people, manipulates or persuades them that the social engineer is really the one who he is said to be, by manipulation and persuasion. As a result, the social engineer—by the use of technology or without it—is able to exploit people to gather information."* [12: 1]

The social engineering is usually categorized by human [13] or IT [14] based attacks, whether an IT tool is used while carrying out the attack. These types of attacks can be effective

[7] What is more, with the iOS Health application we can save medical certificates on our cell phones and share them with other devices.

[8] Naivety, gullibility, assistance, curiosity, lack of security awareness, inattention, sexuality, etc.

[9] According to Kevin Mitnick, one of the most famous hackers these days, who has never considered himself a very prominent hacker, he could succeed mainly by social engineering. After being arrested, he broke up with illegal penetrations, founded a security firm and is currently working as an ethical hacker.

even if the target system has been strengthened by physical and logical security.[10] The danger of this was proven by the experiment of two security experts by connecting a fictitious young, female user with unreal Facebook and LinkedIn profiles to employees of an unidentified US government agency working in the field of cyber security. [15] The result is astonishing: during networking activities the experts have infected the computers of the employees by an e-postcard, so they got access to their confidential data. The senior officer responsible for the agency's IT security was among the victims, as well. It is not hard to understand that this way terrorists can easily enter platforms which are strictly protected (for example, by extorting a member of a security staff).

Contact and Social Media

Due to the particularities of terrorism, the operation of the groups must be characterized by a high level of conspiracy. Social media sites and applications mean new sets of tools of conspirative contacting. The methods of this can be different depending on whether the contact is real time or not. In the latter case, we can talk about placing a message in the form of a blog post, supported by lyrics, or a video uploaded, which let decode the message only for the insiders. The tools of real-time contact are the different chat rooms and the not public chat rooms of online social games.[11] Based on the information coming to light by Edward Snowden, it may be assumed that terrorists use these methods regularly, as the National Security Agency (NSA) maintains a separate department to coordinate agents infiltrating to online games.

Propaganda and Social Media

The terrorist groups recognized the relevance of their recordings about the terror attacks for propaganda purposes relatively early during the Chechen wars. Ibn al-Hatták Saudi guerrilla leader is considered the first Jihadist, who recorded his outrage for this purpose. Nowadays, in the age of social media, the number of tools used by terrorists for scaremongering, recruiting new members, convincing supporters, propaganda, intelligence and cyber-attacks has been excessively increased.

The Islamic State has published regularly their actions in the social media: crucifixions, mass executions, decapitations, etc. When designing terror attacks and selecting the target, it is of utmost importance that the attack implemented provides the utmost publicity. [16] Propaganda is one of the most important elements of organizational existence.

One of the aims of a terror attack is to draw attention to the principles of the terrorist group, for example the critique of the consumerist society, or the fight against repression, etc. Because of this, when selecting the target, newsworthiness gets priority. Due to this,

[10] Physical security means the protection against threats in the physical space, including the protection from natural disasters, mechanical protection, electronic control system, security personnel, identification systems, surveillance systems, power supply, air conditioning and fire protection. Logical security means the protection of IT systems provided by IT tools and procedures (software, protocols).

[11] For example, World of Warcraft, Second Life.

propaganda has different purposes: increasing the visibility of the terrorist group by the news about their attacks, representing their declared purposes, scaremongering in the groups defined as enemies, recruiting new members and supporters.

Psychological operations are one of the most important tools of propaganda. Psychological operations, based on the dissertation of Pix Gábor written in the topic, are the actions in which the opposing parties use conscious psychological influences to achieve their goals. [17]

The first station of the Islamic State's propaganda was the choice of the name; from their establishment in 2003 to the declaration of the Caliphate in 2014.[12]

The Islamic State carried out its propaganda at master's level. Contrary to the Al-Kaida's poor quality propaganda videos, the Islamic State spread their videos on numerous platforms of the social media in HD quality, in English with Arabic subtitle with hashtags.

József Margitics summarizes these platforms in his study. [18] Based on the list of the author, the followings are included:

- Jihad Media Platform website, where the registered users can share news and comments. In 2015 the number of registered members exceeded 3,000, who written more than 400 thousand comments. News could be found by regional breakdown, fresh news—in multiple languages, including English, French and German. Topics about the Coran, propaganda photos and videos, but also posts about family or health topics have been published.
- Islamic State Archives website, where reports, photos, videos including the messages of soldiers have been shared for recruitment and propaganda.
- There have been several pages and groups on Facebook, including the fresh news of the Islamic State, Mujahed's news, Abu-Bakr Baghdadi etc. Groups: "United Islamic Cyber Force" network, Umma Jihad on top, and the media of the Islamic State, etc.
- In the first half of 2017, nearly 300 thousand terrorist propaganda profiles have been deleted from Twitter. The deletion of accounts has become intensive since August 2014, that can be attributed to the decapitation of the American journalist, James Foley.[13]
- There have been numerous YouTube channels as well, showing the training, messages of detainees and moments of everyday life. In addition to this, to find the common voice with the youth to show the "cool" side of the terrorist group, they integrated terror actions, flags and clothes into videos based on the GTA V game.
- Dabiq and Rumiyah online newspapers contain news, tactics and also propaganda.
- Mobile applications have been used not only for contacting, such as the Telegram Messenger, but also for propaganda. After executing James Foley, when their profiles

[12] In 2003 it was known as Iraqi Al-Qaida, in 2011, when the civil war broke out in neighboring Syria, the Iraqi and Levantei Al-Qaeda names appeared there, expressing the fact that Eastern Syria and northern Iraq were one. During the civil war in Syria, the ideological difference with Al-Qaeda, which essentially regards the struggle against the West as an organizing element, has been demonstrated, and the Iraqi and Levantei Al-Qaeda Islamic Caliphs are working on it. Of course, the ideals of Al-Qaida appeared in the early 2000s as the idea of the global Caliphate, which was intended to be the outcome of a 20-year plan, but it was represented by the Islamic State in the early 2010s. This ideological discrepancy led to the suspension of violence, and in the end, in 2013, the Islamic State of Iraq and Levante (ISIS) was renamed to the known name change in 2014.

[13] Shortly after Foley was executed, a video on the murder of another abducted US journalist Steven Sotloff was accidentally released to the Internet, which was, however, not part of the IS's propaganda, because it was published beforehand for which the Islamic State was formally apologized to his followers.

and channels have been started being deleted, the Islamic State developed an application with the title *Dawn of Glad.* The application was available for downloading from Google Play for a long time. In exchange for downloading, the users gave permission for the application to share news in their name on their social websites. This way the Islamic State became ineradicable from social media.

- Several blogs, including the Islamic Caliphate and Islamic State has shared propaganda messages and news with a similar content as the above-mentioned examples.

The intensive presence of the Islamic State in the social media reached a lot of Western youth who, giving up their lifestyles, joined the organization.

According to some assumptions, Ahmad Abousamra, a Syrian–American IT expert, who had formerly worked for telecommunication companies, is responsible for the professional presence of the Islamic State in the social media. [19] Contrary to the previous poor quality videos shared on VHS and not too modern communication strategy, the IS caught the youth's attention by high quality, professionally designed videos, and hash tagged[14] Twitter campaigns. It is no accident then when recruiting new members, the Islamic State emphasizes the points which are easily understandable for youth and determining the organization as a youthful, cool group. The organization stresses particularly on children, as it became apparent from the report of Medyan Dairieh prepared for Vice News. [20]

An important tool for psychological operations is the propagation of fake news, the success of which can be best described by the "post truth" phenomena. The post truth concept describes a situation when public opinion is not based on facts but influenced by emotions and convictions.

Cyber-Attacks and Social Media – The Future?

In the introductory section of this paper, I stated that even though currently terrorist groups are not able to carry out attacks related to cyber warfare, they intend to develop their capacities in this direction. A complex cyber-attack against critical infrastructure requires a high level of technical knowledge, but on the Darknet[15] cyber criminals offer different services which can be used for serious cyber-attacks. The Internet Organised Crime Threat Assessment published in 2016 by the Europol defined the concentration of the cyberspace and terrorism as one of the main focus. [21]

The role of social media can be identified indirectly in the cyber warfare in the infection of IT tools by malicious software, which is called computer-networking operations. These operations serve two purposes. On the one hand, they are used for network detection, and gathering information, on the other hand, modifying, interfering, destroying the gathered information or achieving dysfunction in networks. [22]

---

[14] Hashtag was first introduced and disseminated to other platforms by Twitter. It means a simple tag system that allows to filter and categorize different contents and serves as an easy way to skip between different contents within a given topic. Hashtags can be generated by the # symbol.

[15] Darknet means the webpages on the Deepweb platform where supported by high level encryption, illegal assets and services can be bought, including weapons, narcotics, assassination, sexual services.

Malwares seem to be ineradicable from social media. They appear as campaigns and often cause massive infection. However, they can be relatively easily filtered, the features indicating the links and videos infected by malware codes; they appear regularly, often infecting the same victims as before. The features of the malwares expanded on social media platforms such as Facebook are the followings:

- we get message from our friend in a foreign language that he does not speak;
- link or video promising erotic content about a celebrity or about ourselves;
- our friends tag us in a bulk at a shared content;
- abbreviated link promising the above-mentioned contents or any other sensation;[16]
- content promising huge discounts (e.g. branded sunglasses for some dollars, etc.).

The computer infected this way can be used for a lot of things depending on the purpose of the developer of the malware. These can be the followings:

- our device can become a member of a botnet network, and our resources can be used by the attackers to reach their aims, e.g. mining crypto currency, sending spams or DoS attacks;
- ransomwares can be placed on our device that encrypt our files;
- can give access permissions to our system;
- spywares can be placed on our devices.

The Possibilities of Defence

In the previous section of the paper we could see that terrorists use a wide range of tools to achieve their aims and the past examples confirm that whenever they get the chance, and their capacities make them able, they will carry out such attacks that have not occurred so far (e.g. a cyber-attack against an essential constituent). In early 2013, presumably Chinese hackers broke into the system of the US Army Corps of Engineers which led them gather information about 79 thousand dams. The dams are not only the important elements of energy producing but entail high risks because by obtaining control over them, in case of inundating the nearby areas they jeopardise human lives. [23] We should not have illusions then, we must be prepared for this kind of attacks as well, because their occurrence is only a matter of time.

In the followings, I introduce the possibilities that can be used, that have to be used by the counter-terrorism organizations for prevention and remediation. These statements intend to reflect the results of the examination of the previous section. Accordingly, operations are necessary to be performed mainly in the following areas:

- counterpropaganda;
- psychological operations;
- mapping networks;
- intelligence;
- communication monitoring;

[16] In the case of abbreviated URL, it does not always mean risk, but it should be suspicious when it is sent by an acquaintance who does not know how to make URL abbreviation.

- integration;
- monitoring, disqualifying, recruiting managers;
- trend analysis;
- education;
- recruiting supporters and experts;
- inducing political decision making.

As we could see, terrorists place particular emphasis on "winning hearts", so one of the main tasks is the organization of counterpropaganda. This is not only relevant for the given state, but it is essential in the operations of Civil-Military Co-operation (CIMIC). As the IS finds the common voice with the youth, the counter-campaigns must also use those platforms where the targets of terrorist recruiting are present. Not only the Western European and American youth but also the population of the mission territories have to be considered as priority target groups in the counterpropaganda since it cannot only play a role in justifying the presence, but they are the elements of legitimacy of actions of terrorist groups in the fight against foreign invaders. One of the main points of the CIMIC is that the local population should not consider their presence an invasion, and should not perceive those who serve there as enemies. The notorious Abu Ghraib jail and the related violations have increased the opposition of the local population against the mission units. The strengthening of the Islamic State is explained by the dissatisfaction and mistrust with the corrupt Iraqi political and military leadership, which is compounded by the close relationship with the United States. It is therefore important to carry out counterpropaganda on the social media sites.

The network dimension of social media comes from its conceptual definition. Therefore, the methodology of network analysis provides an excellent tool to map the relations and networks on social media sites.

The role of social media in intelligence cannot be approached only from the aspect of OSINT. From the information coming to light by Edward Snowden, the relevance of Signals Intelligence (SIGINT) can be outlined for anybody, one part of this is the monitoring and analysis of the data generated on social media sites. The introduction of the Snowden case is not included in this article because its complex analysis would take multiple pages. Here, we must mention the relevance of the fact that the national security services can access the whole communication of any user. The monitoring may be mass or individual.

As terrorists use the different social media sites, chat rooms, online games, the presence of authorities is also necessary which in case of success results in the infiltration into the organization itself. By the information gathered applying SIGINT operations, possibilities to compromise the target people arise, with which or the recruitment, or in case of denying cooperation, disqualification can be achieved. From the Snowden documents, we got to know that the NSA has monitored the porno watching habits of several Muslim leaders. By using these devices, we can gather a lot of compromising information, as I have verified this using smart phones.

Taking into account the take-up of social media sites, the systematic analysis of different blogs and social networks, etc. provides the possibility for real-time and automated analysis and the preparation of prognosis and trend analysis of communication and content sharing on a national, as well as international level. The programs used by national security services

can synthesize and visualize huge amount of data. Besides this, these programs are developed constantly, which drives towards the development of artificial intelligence. For example, the American Secret Service has published an open call for the development of an application that is able to detect sarcasm in the media. [24] Considering the extent an average user can detect it, if the algorithm approaches this, in my opinion, we can talk about success.

Social media gives the chance for the users to develop their data and information sensitivity. We need to create campaigns not only to develop their awareness, but also to reduce the spread of different malicious software, which may cause cyber-attacks. Taking a look at the experiment of Aamir Lakhani and Joseph Muniz in the previous section, we could see what kind of dangers the inappropriate data and information protection may contain, so the education of the right internet use is crucial for the staff working in the defence sphere.

All the above-mentioned processes have followed the principle of "action-reaction". It is also relevant for counter-terrorism how terrorists intend to recruit supporters by propaganda. Counter-terrorism actions are not performed by the public opinion because it is the main task of counterpropaganda. The significance of cybersecurity does not even need to be emphasized, but reaching the appropriate capacities is not possible without experts. One tool of this can be the involvement of the domestic hacker community.

In addition to the experts dealing with counter-terrorism, politicians play an important role, as well. One of most significant steps has been carried out by Germany in the fight against fake news. In the summer of 2017, a new legislation was adopted to punish up to 50 million EUR those social media sites which do not remove contents applicable for incitement to hatred within 24 hours.[17] The legislation entered into force on 1st January 2018, and it must be enforced in case of every social media site having at least 2 million German users. If the user enters the site from a German IP address, he/she has to see a platform on which they can register the post applicable for incitement to hatred or being against the German constitution or being a criminal offense. Altogether twenty German laws allow registering these posts, including the legislation on the prohibition of arbitrary symbols, and the attempt to subvert the constitutional order.

In order for the social media sites to comply with the statutory provision, the number of moderators has been enlarged who must decide whether the registered content is really infringing and, if so, should be deleted. A number of German political parties and lawmakers have raised their voices against the law.

The most significant argument is the privatization of the judiciary, as deciding that something is unlawful is normally the task of courts. This cannot be taken over by companies. Related to this, this regulation imposes an extremely short deadline for making the decision, so there is no guarantee that a huge amount of content will be deleted automatically without reading the content in detail, and this can lead to a censorship. Besides Germany, Great Britain is considering a similar regulation, and the French President, Emmanuel Macron has also announced that the French media regulation will be reviewed to fight against fake news spread on social media sites.

In January of 2018, Mark Zuckerberg announced that they would modify Facebook in a spirit of fighting against fake news. The modifications would highlight the posts of our friends and overshadow news portals. This step has attracted a lot of criticism, because this

[17] In case of unspecified content within a week.

way not only the portals of fake news would be reduced radically but also the sites which do not pay for the display.

It is not a question, that we must take action against fake news and contents of incitement to hatred. These are not only political contents but other harmful contents, such as fake news against vaccination, and contents about harassment. But the way to regulate effectively these national social media sites is a very complex and difficult question; no appropriate answer to them has been born so far. If the anonymity decreases, which was a basic principle of the internet in the beginning, the governments and social media sites would know much more about the users and this would infringe the freedom of expression. This would not only increase the censorship of governments and companies but self-censorship, as well. Furthermore, it should not be neglected that even if a social media site is related to one country, it can have global impact; so for example the American practices may intervene in the life of other sovereign states. Referring back to the German regulation, the social media sites would have limited incentives in the anonymity of their users, and this would lead to the internet's high level of regulation, foreseeing public control of a State.

Summary

In my study, I attempted to present the role of social media in counter-terrorism. For this purpose, I examined the possibilities terrorists can use to achieve their aims, and the possible reactions. In view of the limited space, the paper described only the theoretical frameworks, the listed points would require further researches. I believe that if once we open Pandora's box we cannot close it anymore. It is especially true in terms of terrorism as it can be seen in case of the Islamic State. New methods and new procedures are created constantly and even if we learn coping with them, another appears. We can successfully react to these only if we do not refuse the use of these new technologies and tools and we constantly renew them.

References

[1] KRASZNAY Cs.: A polgárok védelme egy kiberkonfliktusban. *Hadmérnök,* VII 4 (2012), 142–151. http://hadmernok.hu/2012_4_krasznay.pdf (Downloaded: 18.03.2018)

[2] MOSKOWITZ, S. L.: The Global Cybercrime Industry. In. MOSKOWITZ, S. L.: *Cybercrime and Business – Strategies for Global Corporate Security.* Oxford: Elsevier LTD, 2017. 3–22.

[3] LUIIJF, E.: Definitions of Cyber Terrorism. In. Akhgar et. al. (ed.): *Cyber Crime and Cyber Terrorism Investigator's Handbook.* Oxford: Elsevier LTD 2014. 11–17.

[4] fbi.com: *Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security February 24, 2004*. www.fbi.gov/congress/congress04/lourdeau022404.htm (Downloaded: 18.03.2018)

[5] CALDWELL, T.: Hacktivism goes hardcore. *Network Security,* 5 (2015), 12–17.

[6] oxforddictionaries.com: *Definition of social media in English.* www.oxforddictionaries.com/definition/english/social-media (Downloaded: 23.13.2018)

[7] KAPLAN, A., HAENLEIN, M.: Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, 53 1 (2010), 59–68.
[8] *Statista*, www.statista.com
[9] LÉVAY G.: *OSINT (Open Source Intelligence) – Nyílt információs hírszerzés.* (egyetemi jegyzet) Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2006.
[10] STEELE, R. D.*: Searching for Bin Laden: The Use of Intelligence in the War on Terror or How NOT to Spend the Taxpayers' Treasure*. (The Smart Nation Act: Public Intelligence in the Public Interest, Foreword by Congressman Rob Simmons (R–CT–02) Sponsor, The Smart Nation Act.) Oakton: OSS International Press, 2006.
[11] DEÁK, V.: Biztonságtudatosság az információs környezetben. *Szakmai Szemle*, 3 (2017), 59–77.
[12] MITNICK, K. D.: *A legendás hacker. A megtévesztés művészete.* Budapest: Perfact-Pro, 2003.
[13] DEÁK V.: A social engineering humán alapú támadási technikái. *Biztonságpolitika*, 2017. április 10. http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-social-engineering-human-alapu-tamadasi-technikai (Downloaded: 21.03.2018)
[14] DEÁK V.: A számítógép alapú social engineer támadási technikák. *Biztonságpolitika*, 2017. április 28. http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-szamitogep-alapu-social-engineering-tamadasi-technikai (Downloaded: 21.03.2018)
[15] LAKHANI, A., MUNIZ, J.: Social Media Deception. In. *RSAConference Europe*. Amsterdam, October 29–31. 2013. http://itcafe.hu/dl/cnt/2013-11/102992/hum-w01-social-media-deception.pdf (Downloaded: 12.08.2014)
[16] HORVÁTH L. A.: *A terrorizmus csapdájában.* Budapest: Zrínyi Kiadó, 2014.
[17] PIX G.: *A lélektani műveletek jellemzőinek vizsgálata.* (PhD-értekezés), Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2005.
[18] MARGITICS J.: *Az ISIS által használt internetes propaganda eszközök áttekintése*. Budapest: Nemzetbiztonsági Szakkollégium, 2017.
[19] McPHEE, M., ROSS, B.: Official: *American May Be Key in ISIS Social Media Blitz.* http://abcnews.go.com/blogs/headlines/2014/09/official-american-may-be-key-in-isis-social-media-blitz/ (Downloaded: 03.09.2014)
[20] DAIRIEH, M.: *The Islamic State (Part 2).* https://news.vice.com/video/the-islamic-state-part-2 (Downloaded: 17.08.2014)
[21] Europol: *The Internet Organised Crime Threat Assessment 2016.* Hague: Europol, 2017. www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 (Downloaded: 02.04.2018)
[22] ANDRESS, J., WINTERFELD, S.: *Cyber Warfare (Second Edition). Techniques, Tactics and Tools for Security Practitioners*. Waltham: Elsevier Inc., 2014.
[23] GERTZ, B.: *The Cyber-Dam Breaks*. http://freebeacon.com/the-cyber-dam-breaks/ (Downloaded: 11.09.2014)
[24] ZEZIMA, K.: *The Secret Service wants software that detects social media sarcasm. Yeah, sure it will work.* www.washingtonpost.com/blogs/the-fix/wp/2014/06/03/the-secret-service-wants-software-that-detects-social-media-sarcasm-yeah-sure-it-will-work/ (Downloaded: 21.09.2014)

AARMS Vol. 17, No. 3 (2018) 63–70.

Hungarians Fighting for France in Indochina

Zoltán HARANGI-TÓTH[1]

After the Second World War, hundreds of thousands of young Hungarians became prisoners of war (POW). Most of them were transported to the east, to the Soviet Union, but still large numbers were captured by French, British or American troops after the collapse of the Third Reich. Hungarians and Germans joined the French Foreign Legion (FFL) in large numbers due to the terrible living conditions of the prison camps. Thousands of former Honvéd soldiers and members of the Hungarian Royal Levente Movement joined the Légion Étrangère to escape those camps, just to die for France in Indochina, from the mountains of Cao Bang to the fields of Dien Bien Phu. This period of the FFL is less researched than the well-known "période hongrois" (Hungarian Period), the wave of refugees after the ill-fated 1956 Revolution. This article is about those young men, who went from a war to another just to fight on an even more lethal battlefield.

Keywords: *Hungarian prisoners of war, French Foreign Legion, Indochina war*

After the collapse of the Nazi regime, hundreds of thousands of Hungarian soldiers, relatives, government members and supporters of the far right Arrow Cross Party became prisoners of war. The unstoppable Red Army marched west, so the soldiers of the Royal Hungarian Army, and the pro-Nazi government had to withdraw from Hungary to southern Germany and Austria (also part of the Third Reich in 1945). They were there at the time of the armistice, and most of them were captured by American troops. The allies later agreed about the creation of a French led occupation zone in southern Germany close to the river Rhine. With this decision, some of the former American prison camps became French led ones.

The Hungarians suffered heavily in those camps, the conditions were harsh. However, the French offered an option, to cut short their suffering – they allowed them to join the ranks of the French Foreign Legion (Légion Étrangère). The worse the conditions, the more people joined the Légion. What they did not know was that France had already been at war in Indochina.

This short, post-war era is a less researched topic in our history and the researchers mainly concentrate their efforts on the political events of the Communist takeover. The important connection between the prisoners of war and the Foreign Legion is often overlooked, however it has a direct link to thousands of our former military members. Every period of the twentieth century has its distinctive mark on the FFL. It is called the Polish, the Russian, and now, the German, later the Hungarian period. The influence and importance of the refugees after 1956 often took all the spotlight when we talk about the relationship of the Légion and Hungary – which is understandable, since those legionnaires, the veterans of the Algerian

[1] Army Captain, Ph.D. candidate, National University of Public Service Doctoral School of Military Sciences; e-mail: harangi-toth.zoltan@uni-nke.hu

war are still living among us. But the post-war period, and the memory of the Hungarians fighting in the Far East is only available from the Foreign Legion's archives – which are mostly closed for the common researchers.

Hungarians in French Captivity

The French made no difference between the nationalities of their captives. From their point of view every POW was simply German. And they were cruel with the Germans. It was something like a revenge for the humiliation of France during the war. They made no difference between Germans and Hungarians – although during the war the few French prisoners of war were held in very good conditions in Hungary. [1]

After the war, the American forces held more than 2 million POWs all around Southern Germany and Austria, but according to the agreements between the Allies, they handed over parts of their occupation zone and also a large number of captives to the French during the summer of 1945 to help them rebuild their country. This included 50,000–60,000 Hungarians too, [2: 201] along with Germans, Austrians, some Romanians and also a few Italians. The French asked for more than 1.5 million POWs, but the Americans handed over only 600,000 due to the lack of living conditions and infrastructure. Usually former officers or clerks helped the American officials to decide who to hand over to the French – and in most camps, they were ethnic Germans. They usually sent everybody – other than their fellow countrymen – to France, since they knew that the Americans would release them soon to help rebuild Germany.[2] [3: 22]

In general, people think the prisoners of war of the Western camps (or in short: "the Westerners"), who spent months in captivity in Germany or Austria were simply more lucky than the ones who were captured by the Soviet troops. However, everybody agrees that the French camp conditions were terrible, the worst of all Western Allies' camps. After a few months, the captives from the Rhine area and Austria were moved to camps all over France where they were forced to work on the rebuilding of the country's economy. These road marches went through hostile territory because the frustrated citizens of this once proud country often threw rocks on the slow moving columns of the POWs, spat on them, sometimes even beat random people to death. [2: 203] They never heard about the good living conditions of the French POWs in Hungary during the war, nor were they aware of the fact that Hungary was not at war with France. Everybody was simply German for them, the enemy who deserved their fate.

The colonial African troops were brutal guards. They harassed, abused or sometimes simply shot them without much reasons. The food was far from enough, people starved. They slept on the ground, without any cover for months and they suffered because of the weather. In the infamous Dieppe camp where most of the young Levente boys were

[2] The Supreme Headquarters Allied Expeditionary Forces (SHAEF) planning for operations at the end of the war in Europe expected only approx. 900,000 German POWs, but their number rose to more than 5 million in May 1945. To avoid the logistical nightmare, general Dwight D. Eisenhower, the commander of SHAEF allowed the creation of the category Disarmed Enemy Forces (DEF) or Surrendered Enemy Personnel (SEP, in British terminology). This made it possible for the Allies to disregard the rights of the Prisoners of War granted by the Geneva Convention, and the International Committee of the Red Cross.

imprisoned, the guards raped and sexually abused them to make things even worse for the 14–16-years-old kids. [2: 212] The situation only started to change when the Hungarian Catholic Mission started to supervise the living conditions of these camps. Almost all of the survivors remembered the fact that the guards and even the commanders of those camps stole all their belongings, the supplies sent by their home countries or the Red Cross and sold them on the black market. Sometimes they even took their Hungarian uniform, and gave them German instead.

The prisoners of war were forced to do heavy physical labour which was inadequate for the weakened people. The conditions were so bad that after the signing of the peace treaty in Paris, but before the release of the prisoners of war, the Americans had to create camps to feed and hospitalize the living skeletons to avoid international scandal. [2: 216]

A lot of people died due to the harsh conditions but some of them chose another option. The recruiters of the French Foreign Legion showed up in the camps day by day, sometimes twice or more times a day. They offered good food and good conditions for the volunteers and they kept their word. They gave the fresh recruits meat and fruits but they made them eat these in front of the other camp members to make the choice even more desirable. Those who decided to join the Légion were sent to special camps for up to 6 months to get some weight, rebuild their health and to make them an ideal recruit for the organization. Most people chose the FFL as the only possible escape from the living hell of the prison camps – although some of them were aware of the fact that the Soviets were still occupying Hungary, so they decided to accept the offered contract to serve for five years to get a French citizenship. However, almost none of the new recruits were informed about the rising conflict on the other side of the world, the Indochina war. [1]

The War in Indochina

The events started to worsen for the French forces in the spring of 1945 – the Japanese disarmed the colonial troops, and sent them to prison camps. In the meantime, the Communist backed Viet Minh, led by Ho Chi Min, started a successful uprising against the Nipponese occupation forces. In the last days of World War Two, the British-led Allies embarked close to Saigon, and finally overthrew the Japanese rule. The French Government wanted to re-establish its colonial rule, but faced fierce opposition, as the communists wanted to create their own independent state.

The leaders of the Fourth Republic did not want to sacrifice more French blood for a conflict far away after the bloody world war but still, they wanted to regain the country's former glory and to show force for the other colonies. [4: 547] France already had a large colonial force in the area built up with Vietnamese, Laotian, and Cambodian troops led by French colonial officers, but this force was unable to fight successfully with the Viet Minh, even with the help of the growing number of African units. They decided to build up the numbers of the Foreign Legion, France's foreign mercenary force, since their losses were far from a sensitive topic for the French people.

This all volunteer, mixed colonial and mercenary force was fighting for the country for almost 10 years, from 1945 to 1954. The French nation did not sacrifice its young men in the conflict but they bore its economic consequences. On its climate, the French Far

East Expeditionary Corps (Corps Expéditionnaire Français en Extrême-Orient – CEFEO) consisted of more than a quarter million people.

To supply this force, the post-war French state was not economically strong enough but they were not able to get foreign support for a colonial conflict. Due to the Korean war, the United States finally realised the threat of the spreading South-East Asian communism, and decided to support France's war in Indochina. In the last years of the conflict, the USA was the greatest supporter of the fighting with paying most of the expenditures of war.

Even with this huge financial support and supplies the French forces started to lose ground. On the other side, the communist Viet Minh was supported by the newly born communist China, and had an infinite pool of reserves. In the last phase of the South-Asian-type communist uprising,[3] [5: 443] they stood on an even ground with the French, and they managed to achieve a sound military victory at the valley of Dien Bien Phu. This final battle was also the bloodiest one for the Foreign Legion, it's most elite units perished in the fighting and in the following death marches. Dien Bien Phu broke the Legion's core.

The French Foreign Legion

The French Foreign Legion was the heir of the centuries old tradition of the Monarchy. The King of France used mercenary units to fight for his flag from the middle ages. This tradition survived the foundation of the standing armies – the Kingdom of France had many foreign regiments in its ranks even in the eighteenth century. After the fall of the Ancien Régime, Napoléon Bonaparte also had many nations under his army flag. From the Polish to the Swiss, half of Europe fought for his First Empire, as far as the outskirts of Moscow. It was well accepted in France even after nationalism appeared in the nineteenth century and other countries turned to their own people to build "national" armies.

The king founded the Légion Étrangère or the French Foreign Legion in 1831 just after France conquered Algeria, the cornerstone of its new colonial empire. It was a mercenary force led by French officers to guard its provinces. The FFL was open to everybody, who wanted a new start – in the first decades of its existence it welcomed criminals, former nobles, almost anybody, from all over the World. It was a melting pot for all its members, who wanted to fight for the French flag; that was the only sacred rule of the Légion. They were among the fiercest fighters of the country's history, although they were mostly foreigners, not even native French. [6: 64–67]

After WWII, the Foreign Legion was low in numbers due to the heavy fighting from North Africa to Germany. On the other hand, the French had hundreds of thousands of possible new recruits in their prisoner of war camps. The experienced veterans of the war were the first targets of the recruiters. They were the desired target group.

[3] According to Mao Ze Tung, the three phases of revolutionary warfare are: guerrilla war, fight with mixed regular and guerilla forces and the last phase is marked by large scale regular operations.

Although there was an unmentioned rule that none of the participating nations were allowed to cross a percentage per capita to avoid the possible "Pretorian Guard" effect.[4] No soldiers from the same nation were allowed to be more than one quarter of the total number to avoid a single national character to dominate the unit. [7: 280] This was hard to keep since it was not necessary for a new recruit to tell his real nationality – Germans and French usually joined the Legion as Swiss or Dutch, maybe Belgian.

However, there were some decisions simply dictated by common sense. The former German paratroopers, the Fallschirmjägers became the nucleus of the 1st and 2nd Foreign Paratrooper Battalions (1re/2e Bataillon Étranger de Parachutistes – BEP), and the prisoners of war from the Panzer Divisions became members of the 1st Foreign Cavalry Regiment (1re Régiment Étranger de Cavalerie – 1REC). [8: 98] The presence of the eastern front veterans among the ranks of the 3rd Foreign Infantry Regiment (3e Régiment Étranger d'Infanterie – 3REI) was also a distinctive feature.

The total number of legionnaires in the late 1940s and early 1950s was around 35,000 strong, with half of the units of the FFL deployed to Indochina. The 1st and 2nd Foreign Paratrooper Battalions, the 2,nd 3,rd and 5th Foreign Infantry Regiments, the 13th Half-Brigade of the Foreign Legion (13e Démi-Brigade de Légion Étrangère – 13e DBLE), the 1st Foreign Cavalry Regiment and some supply and engineer units, totalling a number around 20,000 legionnaires. Among that number 7,000–8,000 Germans fought for France in Indochina at that time. [7: 280] So not every member of the French Foreign Legion was German or Austrian but the legionnaires fighting in Indochina were predominantly (more than a third of the total) of German origin. [7: 280]

In March 1946, when the 3REI deployed to Indochina with 1,740 legionnaires, 33% of its members were Germans, 17% were Swiss, 7% were Spanish, 6% were Polish, 5–5% were French and Italians. [9: 12] However, anecdotes tell that among the members of the paratrooper battalions, the common talk was about the comparison of the sieges of Dien Bien Phu and Monte Cassino. The truth is, that at Dien Bien Phu (1954) the average age of the enlisted legionnaires was 23 years – so it was less likely to find WWII veterans in the ranks of the frontline units. [7: 280]

The new recruits rarely came from units blamed with crimes against humanity, namely the Waffen SS. It is a common misconception that whole units joined the Foreign Legion after the war. Hungarian survivors of the prison camps (wherever they were) remembered that the guards commonly checked the arms and armpits of the POWs looking for SS tattoos and that recruiters often refused to allow them to join the organization. They were allowed to join only if they had special experience or military qualification and they were not put on trial before a public court.

After the Germans, the French were the second largest group to join the FFL. A lot of clerks and officials involved in the collaborationist Vichy Government were treated like war

[4] This effect was named after the late roman Pretorian Guard, the Emperor's bodyguard. They were often a force with a power to influence political leaders and their decisions or simply interfere with the political leadership, murder emperors, etc. They were a closed military type of unit, with the best equipment and quality of troops available, and they were faithful to their own leaders instead of the state. This nightmare scenario took effect in Algeria, 1961 when the most elite unit of the French Foreign Legion, the 1st Foreign Parachute Regiment (1er Régiment Étranger de Parachutistes – 1er REP) joined the coup d'état against general de Gaulle. After this incident the FFL lost most of its power and de Gaulle disbanded the 1er REP on scene.

criminals by the majority of the French society. Joining the legion as a Belgian or Swiss was a viable option for them to get a new and clean identity and a chance to reintegrate into the society. To get a tabula rasa was even harder for the soldiers of the Charlemagne (French) SS Division or the fighters of the Legion of French Volunteers Against Bolshevism (Légion des Volontaires Français – LVF) who were clearly outcasts of the society at that time. [10: 273]

Another misconception is that the Legion was open for criminals after the war; it was impossible for somebody with a civil court sentence to join the legion. Only people with military court martial sentence were allowed to join the official military. A special unit was created for the criminals, collaborationists and Nazis: The Overseas Light Infantry Battalion (Bataillon d'Infanterie Légère d'Outre-Mer – BILOM). Their service time was based on the duration of their sentence in prison. After the first two companies deployed in Indochina, the program was closed due to public outrage fuelled by the French communists.

During the Indochina war, the French Foreign Legion was always at the places where the fighting was the heaviest. Its units fought along the Colonial Road 4 and at the valley of Dien Bien Phu. From the 72,833 legionnaires deployed in Indochina during the war, 380 officers, 1,082 non-commissioned officers and 9,092 legionnaires never came back to France. [11: 13] The fierce battles were just one reason of the high loss rate of the Foreign Legion. The other was the deadly jungle battlefield and the tropical climate. The average legionnaire came from Central Europe and was not prepared for the Far Eastern environment. Hundreds of miles of death marches followed the lost battles and the members of the FFL had the worst chance to survive it – comparable only to the mainland French soldiers. 70% of the legionnaires needed medical treatment after the liberation of the French prisoners of war in 1954 but only 24% of the African unit members [7: 301] were hospitalized. The Foreign Legion lost 12% of its deployed numbers, which compared to the losses of the whole French Expeditionary Corps average (7%) is the highest total loss rate of the war.

Hungarians in Indochina

The Hungarians joined the Legion for multiple reasons. First in 1945–1946 to escape from the French prison camps. The second wave arrived when they realized the Soviet takeover in Hungary. From the Second World War until the end of the Algerian war, 3,136 Hungarians joined the Légion – approximately 330 died in Indochina (and 120 in Algeria). [6: 587] One third of the new recruits in 1945–1946 were very young teenagers, former Levente members and military school students who sometimes lied about their age to join the FFL. [11: 13] They mostly came from the returned Hungarian territory outside of the so called "Trianon border" (the pre-1920 state border of Hungary).

The other large group of recruits was the members of the former Royal Hungarian Gendarmerie, Hungary's paramilitary police force. [2: 219] Since some of their members were heavily involved in the Jewish holocaust and were far right sympathizers, the whole organization was unwelcomed in the new Democratic Hungary. After the war they fled to the west or joined the Foreign Legion to avoid public punishment and humiliation.

During the war the North Vietnamese used propaganda to target the multinational or supranational Légion more than any other unit type. The Viet Minh offered safe return to

home for the Central European legionnaires – if they left the Legion; they allowed them to return home, from a communist country to another. [12: 120] After the end of hostilities in 1955, 1,234 legionnaires were still missing. Some of them died in captivity, but the others possibly deserted. 58 Hungarian POWs returned to their home country before the end of the war thanks to the agreements between the Democratic Republic of Vietnam and the Peoples Republic of Hungary. [13: 5]

Conclusion

Most of the Hungarians joined the Foreign Legion because they were in a desperate situation – it was especially true for the teenagers, or the supporters of the old regime. Central and East Europe was always the primary recruiting ground for the FFL but after the Second World War this area provided the organization with the much needed experienced manpower to have a chance to win the war on the Far East. In the end, the war was lost on the political ground in Geneva and also on the fields of Dien Bien Phu. The French Foreign Legion did its best and suffered heavier losses in Indochina than any other unit during the conflict. Among its ranks the many Hungarian recruits also lost their lives fighting for France.

References

[1] TARCZAI B.: *Magyarok a nyugati hadifogolytáborokban*. Miskolc: Herman Ottó Múzeum, 1991. http://epa.niif.hu/02000/02030/00024/pdf/HOM_Evkonyv_28-29_305-327.pdf (Downloaded: 20.05.2018)

[2] SZABÓ P.: *Keleti front, nyugati fogság*. Budapest: Jaffa Kiadó Kft., 2018.

[3] McCREEDY, K. O.: *Waging Peace: Operations Eclipse I and II—Some Implications For Future Operations*. Carlisle: U.S. Army War College, Carlisle Barracks, 2004. www.dtic.mil/dtic/tr/fulltext/u2/a423621.pdf (Downloaded: 22.05.2018)

[4] FRANCHINI, Ph.: *Les Guerres D'Indochine, Tome I*. Paris: Texto, 2011.

[5] Mao Ce-tung: A kínai forradalmi háború stratégiai kérdései. In. Mao Ce-tung: *Mao Ce-tung válogatott művei. 1–4.* (1. kötet). Budapest: Szikra Könyvkiadó, 1952. 329–464.

[6] NÓVÉ B.: *Patria Nostra*. (PhD-értekezés) Eger: Eszterházy Károly Főiskola, Történelemtudományi Doktori Iskola, 2016.

[7] FALL, B. B.: *Street Without Joy*. South Yorkshire: Pen & Sword, 2006.

[8] BENE, K.: *Une migration atypique. Le parcours et l'identité des volontaires centreeuropéens de la Légion étrangère au lendemain de la Seconde Guerre mondiale (1945–1954).* 98. http://acta.bibl.u-szeged.hu/49679/1/chronica_016_089-100.pdf (Downloaded: 20.05.2018)

[9] BONNECARRERE, P.: *Par la sang versé*. Paris: Perrin, 2006.

[10] BENE K.: *A Nagy Károly hadosztály. A Waffen-SS francia önkénteseinek harcai a keleti hadszíntéren.* Pécs: Pécsi Tudományegyetem Bölcsésztudományi Kar, 2016. 273. http://real.mtak.hu/40452/ (Downloaded: 20.05.2018)

[11] NÓVÉ B.: *Magyarok az Idegenlégióban.* 2012. 13. www.balassiintezet.hu/attachments/article/827/NoveBela.pdf (Downloaded: 20.05.2018)

[12] KUDRNA L., BOGNÁR I.: Harcoltak és haldokoltak Indokínában. Az első vietnami háború és a csehszlovákok az idegenlégióban. *Klio*, 1 (2013), 120. www.c3.hu/~klio/klio131/klio118.pdf (Downloaded: 20.05.2018)

[13] CADEAU, I.: 1954–56, le départ du cors expédionnaire francais d'Extreme Orient. *Revue Historique des Armées*, 258 (2010), 67–81. https://journals.openedition.org/rha/6925#body-ftn21 (Downloaded: 20.05.2018)

AARMS Vol. 17, No. 3 (2018) 71–82.

Comprehending Gerasimov's Perception of a Contemporary Conflict – The Way to Prevent Cyber Conflicts

Robert JANCZEWSKI,[1] Grzegorz PILARSKI[2]

Alongside with the appearance of the so far unknown reality called cyberspace, the new conditions of the course of conflicts emerged, consequently both the scientists as well as practitioners started to use the term cyber conflict. Unfortunately, presently there is no consistent, common view concerning a cyber conflict.

The article presents a theoretical basis of cyber conflicts based on the research carried out by the authors. The article itself is an added value since it provides the suggestion and explanation of the perspective for the understanding of cyber conflicts through the prism of Gerasimov's perception of a contemporary conflict. Moreover, it presents a new definition of a cyber conflict as the process being the system of activities. The authors also present the stages of a conflict according to Gerasimov, as well as the structure of a cyber conflict. Additionally, the article envisages the aspects of Russian attitude to conflict solving which are worth paying attention to. The presented article offers the perspective of the Russian understanding of the resolution of conflicts, it bridges the gap in research on cyber conflicts as well as assures a strong theoretical basis for the understanding of a Russian point of view on the solution of contemporary conflicts, which might be useful for counteracting cyber conflicts. The authors hold the view that the article is the incentive for further research on cyber conflicts during competition.

Keywords: *component, cybernetic environment, information processes, Signals Intelligence, information processing*

Introduction

In a changing world the state, non-state, military and non-military entities still cooperate with one another both in the national and international dimension. Alongside with the positive cooperation, the interactant states run campaigns for the development and protection of their own national interests, which can often lead to conflicts. Still, whenever people cooperate, competition and conflict are natural and inevitable phenomena.

The civilization development of societies has contributed to the creation of the so far unknown sphere which has been named cyberspace. Cyberspace creates possibilities for countries, their allies and partner countries to obtain and keep constant benefits, as well as to assure the safety of their countries. Cyberspace in its range is not limited by the geographical

[1] War Studies University, Section of Cyber Security, Warsaw; e-mail: r.janczewski@akademia.mil.pl
[2] War Studies University, Section of Cyber Security, Warsaw; e-mail: g.pilarski@akademia.mil.pl

and geopolitical borders. The access to the Internet and other spheres of cyberspace provides the users with a worldwide range, creates chances for fast development, but at the same time it creates proper conditions for cyber threats e.g. the possibility of infringing the integrity of critical infrastructure in a direct and indirect way without physical presence.

The latest experience indicates that activities performed against countries are transferred from physical dimension i.e. land, sea and air space into cyberspace. Scientists have been expressing their points of view on the new areas of combat for many years. In 2009, Colin S. Gray wrote that it has been rare in history for a new geography to be added to the elite short list of environments for warfare. Now there are two such new geographies, space and cyberspace, and we are becoming ever more dependent upon them both. Thus far, at least, we have not taken space or cyber system vulnerability as seriously as we shall have to. It is a law of war: The greater the dependency on a capability, the higher the payoff to an enemy who can lessen its utility, in effect turning our strength into a weakness. [1] This remark clearly depicts the meaning of cyberspace for competition and conflict.

It seems to be a cliché the statement that there are still more advanced technological and technical solutions and the theatre of operations is still changing. However, in the context of conflicts, the issue is not as trivial as it seems to be. The emergence of the new space where societies function resulted in the fact that we live in the era of cyber conflicts. Thus, the question emerges whether the phenomenon is understood and whether it is possible to counteract it.

In order to understand the meaning of the new, so far unknown piece of reality – cyberspace for security, it must be realized that the constant, dynamic development of methods, techniques and measures of combat contributes to the multi-dimensional character of the area of conflicts and new technologies, technical solutions, methods or methodology of operations determine the reasons and course of conflicts.

The main methodological assumption of the article is a deep belief of the authors that the acquaintance and comprehension of the character of the contemporary understanding of conflicts in general, the characteristics of cyberspace as well as the essence of operations run in this domain as well as making use of it by the potential adversaries allow to know the nature of cyber conflicts and most of all how to counteract them. Thus, the main goal of deliberations presented in the article will be the quest to find the answer to the question: whether the comprehension of the views of Gerasimov on the contemporary conflict shall allow to counteract cyber conflicts?

This paper makes the following novel contributions:

- cyber conflict as the process being the system of operations;
- the structure of a cyber conflict;
- the factors and elements of a cyber conflict;
- the identification of a cyber conflict as the element of a conflict in the general meaning;
- the decomposition of a cyber conflict into stages.

According to the authors the primary stakeholders of interest for the outcome of this analysis should be the military, non-military, state and non-state actors.

Cyber Conflict – Whether We Realy Understand It

The connotation of the concept of a cyber conflict seems to be fairly simple and clear-cut. Unfortunately, a deeper analysis of the concept leads to a conclusion that it is not like this. As M. Afzalur Rahim [2: 17] noticed, the term "conflict" has no single clear meaning. Much of the confusion has been created by scholars in different disciplines who are interested in studying a conflict. It is exactly the same with the concept of cyberspace.

Thus, there is a question if it is possible to expressly indicate the referents of a cyber conflict if it is impossible to indicate the referents of a conflict and cyberspace. The scope of a cyber conflict is unfortunately not examined enough and because of that, it is misunderstood by the scientists and practitioners. Thus, it is not clear, in what way the conventional mechanisms of security such as deterrence or collective defence refer to the new phenomenon.

The subject literature presents the view that a conflict is an improved relative position, without concern for absolute welfare consequences ("zero-sum" orientation – the sum of winnings equals the sum of losses). This reflects a classic game-theory outcome with non-cooperative players and often occurring in real conflicts. The authors of the article hold the view that if you ask the wrong question, you probably will get a wrong answer. And cyber—and what to do about cyber conflict—is an arena where there is generally no agreement on what is the question, certainly no agreement on what is the answer, and evolving so fast that questions are transmuted and affect and change the validity of answers that have been given. [3]

A prove for the rank of the issue is the bilateral cooperation signed in 2011 between the East West Institute and the Information Security Institute of Moscow State University aiming at a terminological convention in the scope of cyber. As a result, 20 terms were established through the initial bilateral negotiations and publication in April 2011. Building on the then-established collaborative relationship, the joint team reinitiated the discussion in 2013, to further define critical terms.

Moreover, the vitality of the problem issue is proved by the fact that in June 2013 presidents Vladimir Putin and Barack Obama signed an agreement on the commencement of cooperation in the scope of cyber security. The common understanding and the definitions of the key terminology concerning a cyber conflict elaborated by the above mentioned institutions were of significant importance for the agreement.

Lexically, a cyber conflict is determined very laconically. According to the Macmillan Dictionary a cyber conflict is a conflict in cyberspace and at the same time a cyber conflict is a cyber warfare. [4]

The above mentioned Report Critical Terminology Foundations 2 defined a cyber conflict (Russian: Киберконфликт) as a state that is on a continuum with war, but falls short of a critical threshold, is a tense situation between or among nation-states or organized groups where unwelcome cyber-attacks result in retaliation. At the same time the report defines a cyber conflict as a tension between states and/or organized political groups where the hostile (unwanted) cyber-attacks provoke (lead to) retaliation. The phenomenon of a cyber conflict is also of significance for the definition of a cyber war. Cyber war, according to the Report, is an escalated state of a cyber conflict (Russian: высшая степень киберконфликта) between or among states in which cyber-attacks are carried out by state actors against cyber

infrastructure as part of a military campaign. Cyber conflict can be also a precursor to an escalated situation. [5]

The subject literature indicates objectives in preventing and managing a cyber conflict. L. Kello claims that to prevent or minimize activities that threaten the functioning of the global Information Communication Technology (ICT) system and the global political economy, states and relevant private actors should be expected to undertake a range of policies and activities to fulfil the following functions:

Military cybernetics distinguishes three basic directions:

- enhance the capacity to detect and attribute cyber exploitations and attacks and to distinguish their purposes;
- augment various forms of defence against such activities, both to protect assets and raise the costs to potential perpetrators;
- increase the resilience of key cyber dependent systems;
- while more difficult, pursue political and technical analogues to arms control agreements, or understanding that could inspire confidence that malware and other "weapons" will be sparingly used and will not have unintended consequences, including proliferation;
- assert state control over actors that use their territories to conduct unlawful cyber activities and over their citizens who do so abroad;
- upgrade capabilities to signal, threaten and initiate cyber and other actions to inflict sufficient "pain" on adversaries to motivate them to eschew or desist from hostile activities; and
- develop, over time, norms to restrain the most potentially destabilizing sorts of cyber activities.

These steps would contribute to the prevention and mitigation of actions that could threaten the dynamic stability of the domain and of the international political economy. [6]

The subject literature presents the view that the term "cyber conflict" denotes an offensive cyber-attack for political or strategic purposes as well as responses to such an attack. [7]

A cyber conflict is also the use of computational means, via microprocessors and other associated technologies, in cyberspace for malevolent and/or destructive purposes in order to affect, change or modify diplomatic and military interactions between entities. [8]

At the same time, according to the subject literature, a cyber conflict might not have any political basis. [9]

The results of the research carried out by the authors allow to formulate a conclusion that a cyber conflict is a process that is a system of activities. Details will be described later in this article.

Cyber Activities – Russian's Point of View

The analysis of subject literature revealed that the Russians also started to use the concept of cyberspace and to develop abilities to run operations in the cyberspace or with its use. It is significant in the context of the role of cyberspace in the course of a conflict.

On the 21st of March 2012 during a meeting with military scientists, the vice Prime Minister of the Russian Federation being responsible for the defence industry, Dmitrij Rogozin announced that the Russian authorities are taking into consideration the idea to form forces proper for operations in cyberspace within the structure of their own Armed Forces. He said that at that time they were deliberating on the creation of a cyber command. It stemmed from the need to assure the safety of information both of the armed forces, as well as of the state infrastructure as a whole. [10] Rogozin assured at the same time that all documents had been already prepared and he expressed hope that the technical predator, as he dubbed it, would appear soon. According to him, the main tasks that forces need to tackle include the monitoring and processing of information coming from the outside, as well to combat cyber threats, as he said "in other words it would be something similar to American cyber army. The officers who had been trained to serve in those forces would have to go through a language training, namely learn a foreign language, first of all English language". As we learnt from the press, in order to attain a maximum control of the cyberspace, general Siergiej Szojgu announced the beginning of "a great hunt" for computer programmers. This is enforced by the multitude of computer software which is needed by the Army within the next five years. [11]

At the beginning of July 2013 also the Ministry of Defence of the Russian Federation announced publicly that Russia will have forces responsible for combating cyber threats and for fighting cyber-attacks. [12] The head of the Russian Foundation for Advanced Research Projects, Anderei Grigoriev, also confirmed that in the Russian armed forces a new type of forces specializing in the fight against cyber threats was being created. In the radio station Echo of Moscow, A. Grigoriev announced: "cyberspace—now the task has been formulated, a decision has been made to create cyber command within the Ministry of Defence as well as to create a new type of forces. We have already contacted the potential people who will work there and now we are preparing a common programme which will have to be constantly developed."

In 2014 a Concept of the Russian Federation of cyber security strategy was created. [13] In this document the Russians noticed that Information and Communications Technology (ICT) was developing very fast exerting still bigger influence on all key spheres of citizens', organizations', and state's activities in the Russian Federation. The Internet and other elements of cyberspace have become a systemic factor of Russian economic development and modernization. The implementation of ICT into the management processes is the basis to create an effective and socially responsible democratic state of the 21st century.

According to the concept, cyberspace is the sphere of activities in information space, created by a set of Internet communication channels and other ICT networks, technological infrastructure assuring their functioning, as well as any forms of human activity (of private people, organizations, the state) realized through their usage. Such understanding of cyberspace differs from the one presented in the above-mentioned Report, where cyberspace is understood as an electronic medium through which information is created, transmitted, received, stored, processed and deleted. In fact, such understanding of cyberspace is limited to only a medium of information processes.

In the concept, it has been noticed that the cross-border character of cyberspace, its dependency on advanced information communication technology create not only new possibilities but also new threats in the sphere of the rights, interests and the functioning

of people, organizations, or state bodies. Cyber-attacks carried out by cyber criminals and cyber terrorists pose a threat to the secured information resources. It is possible to use cyber weapons in special operations and cyber war, as well as during traditional war operations. The last sentence is clearly incorporated in the philosophy of a hybrid conflict.

The importance of cyberspace is emphasised by the Russians also in the report of the Centre for Strategic Research of the Russian Federation of 22nd of December 2017 entitled *The future of information security: global changes and scenarios for Russia.* [14]

In the Centre's report the authors notice that in the context of Information Communication Technology as the means of running military operations as well as cyberspace as a synthetic concept used to indicated a new technological environment for operations, it is not obvious that it is possible to use the existing set of international norms of humanitarian law and the law of a military conflict. The literal application of the existing basic norms (The Geneva Convention of 1949 and others) is impossible due to the technological specificity of cyberspace, and effective adjustment of such norms, taking into consideration the technical twists and turns, has not been prepared yet. A separate problem is the lack of universal definitions and the classification of the objects and assets (critical information infrastructure/ critical objects) which must be protected.

In the context of a cyber conflict, according to the Centre's report, the key problem is the lack of trust to the system of international relations which enables the creation of common security mechanisms. It is also well-based to set the boundaries of operations which, if crossed, could result in military reaction. Thus, Russia should prepare and introduce into international discussion its own stance towards this issue.

The Centre's report recommends that till the year 2020 the Russian Federation should prepare and publish a separate strategy for the operations of the armed forces in the information realm (similar to the Pentagon's cyber security strategy). Russia reserves the right to limitless use of its military capacity as a response to operations with the use of ICT, the use of force in accordance with Moscow's standards.

According to the Centre's report there is a necessity to carry out work, in the framework of closed consultations and briefings, between the Russian Federation and the United States, NATO, EU, Great Britain, China, Israel as well as other states and organizations in the scope of the interpretations of certain international norms of humanitarian law with reference to cyberspace (including the definition of the threshold of force used in cyberspace), the common management of the escalation of conflicts in cyberspace in order to assure a minimum acceptable level of strategic stability in cyberspace.

The above analysis revealed that the Russian Federation builds military capability to run operations in cyberspace. It is of great importance in the context of the course of conflicts in cyberspace.

Gerasimov's Perspective of Conflict

In February 2013 general Valery Gerasimov, the head of the General Staff of the Armed Forces of the Russian Federation published an article in a weekly magazine *The Military-Industrial Courier* under the title *The Value of Science in Prediction.* [15] The starting point of the article was an opinion that the new challenges require deliberation on new forms and

methods for running military operations. In the article, the general presented his own view on the forms and methods of running military operations in the contemporary conditioning, as well as the role of non-military methods in solving conflicts between countries.

W. Gerasimov has distinguished six stages of conflict development:

1. Concealed primary operations.
2. Intensification.
3. Commencement of conflict operations.
4. Crisis.
5. Settlement of a conflict.
6. Re-establishment of peace (following a conflict).

The analysis of the article revealed that the head of the General Staff of the Armed Forces of the Russian Federation noticed that in the settlement of conflicts between countries, a bigger role is presently played by non-military measures. The latter one include:

In stages 1, 2 and 3:
- Settlement of coalitions and alliances.

In stages 1 and 2:
- Creating political opposition.

In stages 2 and 3:
- Economic sanctions.
- Severance of diplomatic relations.

In stages 2, 3, 4 and 5:
- Political and diplomatic pressure.

In stages 3 and 4:
- Activities of opposition forces.

In stage 4:
- Economic blockade.

In stage 5:
- Rearrangement of the economy into the state of war.
- Change of military-political command.

In stages 5 and 6:
- Seeking for ways of settling the conflict.

In stage 6:
- Running comprehensive activities aiming at the decrease of tensions in relations.

The military measures include:

In stages 1, 2, 3 and 4:
- Military measures of strategic deterrence.

In stages 3 and 4:
- Strategic expansion.

In stages 4 and 5:
- Running military operations.

In stages 4 and 5:
- Peace operations.

While informational confrontation present in every stage of a conflict is, according to the general, both a non-military and military activity.

W. Gerasimov highlighted that presently the achievement of political goals is realized through the use of political, diplomatic, economic and other non-military measures linked with the use of military power, and not only through armed combat. Such points of view create ideal conditions to run activities both in cyberspace, as well as with its use to attain the set goals.

The view that new challenges require re-thinking of the forms and methods of settling conflicts is depicted by Gerasimov on Figure 1.

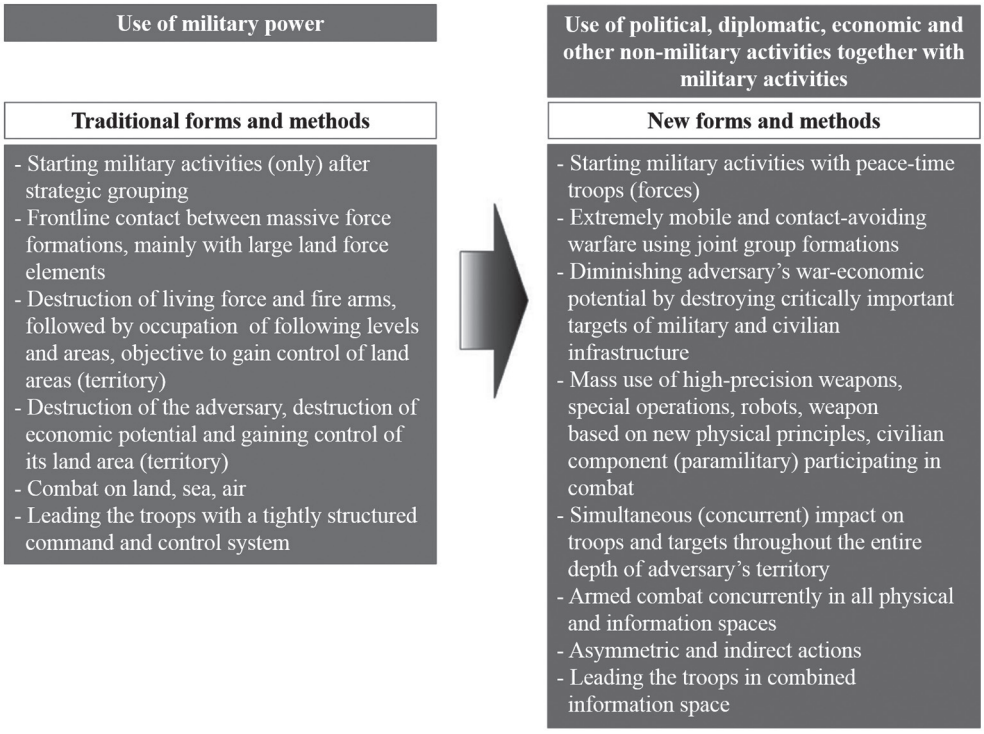


Figure 1. *The evlolution of political goals achievement according to Gerasimov.* [15]

The analysis of new forms and methods presented above in the evolution of the character of combat fight in the process of attaining political goals clearly shows the meaning of cyberspace in the course of a conflict. A cyber conflict can be commenced in cyberspace or with its use by specialized forces (army) proper for the time of peace prepared to act in cyberspace. Moreover, cyberspace creates perfect conditions to support task-oriented groups in conducting highly manoeuvrable, non-contact military operations. It is hard to appreciate enough the role of cyberspace in diminishing the military and economic potential of a country by neutralizing in short time critical objects of military and civilian infrastructure. ICT networks and systems facilitate running special operations and the use of precision-guided munitions, robotic platforms, and of weapons based on the state-of-the-art solutions, civilian forces (paramilitary ones) on a large scale. The characteristics

of cyberspace significantly facilitate simultaneous impact of military forces and civilian objects of the enemy on the whole territory. Cyberspace can be effectively used to run military activities at the same time on all physical areas and in information space, as well as asymmetric and indirect activities. The new operational domain enables the organization of a single information space, which is of great importance for the management of forces and resources at the time of a conflict, and consequently of a cyber conflict.

Presently, next to traditional techniques, non-standard ones are introduced. The role of single, mobile task-oriented groups is increasing due to the use of new possibilities that are offered by the command and support systems. Military operations are becoming more and more dynamic, active and effective. Tactical and operational gaps, which might be used by the enemy, are disappearing. The new Information Communication Technology made conditions for shortening the time, reducing the space and the information gap between the fighting groups and the command and control bodies. Front clashes between big military groups (forces) on a strategic and operational level are going down in history. The development of ICT is one of the reasons for the disappearing difference between operations on strategic, operational, or tactical level. Precision-guided weapons used in combat is based on advanced robotic systems. The use of cyberspace in asymmetric operations allows to balance the predominance of the enemy in armed combat. Owing to that, it is possible to carry out operations on the whole territory of the enemy as well as to exert influence on information and at the same time to constantly improve the forms and methods of activity. The changes which are taking place are reflected in the doctrines of the leading world powers and are being constantly tested.

The considerable meaning of cyberspace is proved by the fact that the Federal Security Service (FSB; Russian: Федеральная служба безопасности Российской Федерации [ФСБ]) of the Russian Federation has formed the Centre for Electronic Communications Surveillance responsible for intercepting, de-coding, and processing of the data and information sent via electronic communication. The Centre is also known as number 16 and for protective aims FSB unit 71,330.

The analysis of internet sources proved that the Military Unit 71,330 called for a tender to assure access to information from the world and regional IT and ICT networks (including the Internet) that was to begin on the 15th of January 2015. The cost was covered from the federal budget. The contract price totalled 557,500,000,014 RUB. The tender was won by the Limited Liability Company NEO PRINT, located in Mytiszczi – a city in the Moscow district, located 19 km from Moscow. [16]

Cyber Conflict – A Process

L. R. Pondy has argued that "organizational conflict can be best understood as a dynamic process underlying organizational behaviour. This is a very broad definition that excludes very little of anything transpiring in a group or individual". [17]

The authors' research proved that a cyber conflict is a process. The process is based on the elaborated methodology and a system of activities realized with certain resources. It has its beginning and the end, it also lasts continuously in time. The structure of a cyber conflict is formed by sub-processes which include stages, phases, and activities. The primary

and secondary factors qualify the structure and the course of a cyber conflict. A cyber conflict can be disturbed by organizational, procedural, and technical barriers. They exert a negative influence on the course of a cyber conflict.

The threshold of a cyber conflict is of great importance. This is the point which if crossed can trigger a cyber conflict. The threshold of a cyber conflict indicates that disagreements, incompatibilities or differences between subjects are so serious that the parties move on to the state of a conflict. However, some quality of a cyber conflict is worth paying attention to. It does not take place only because of disagreements, incompatibilities or differences between the potential parties of a conflict. In order for the cyber conflict to take place, each party must be convinced that the threshold of a cyber conflict has been crossed. The difficulty is based on the fact that the subjects might have (and usually have) different vulnerabilities and tolerance, if they are exceeded, it marks the beginning of a conflict. It means that in the same conditions some subjects might engage in a cyber conflict earlier than others, and some of them might even not notice the conflict aspects.

A cyber conflict as a process has a structure dependant on the adopted criterion, i.e. a spatial, informational, organizational, procedural and technical one.

Spatial structure – it means that particular elements of a conflict can be identified in a given location, in places which have been purposefully chosen and properly prepared to realize activities in the framework of a cyber conflict.

Informational structure – the structure refers to the data and information resources. It is strictly connected with information processes at a time of a conflict. The informational process gathers information for further proceeding which means that the information is obtained in different language or sign systems (e.g. Morse code). Information resources are obtained by different functional teams and analysed in different analytical teams. The informational structure concerns both data as well as information which are a material in the information process.

Procedural structure – the structure entails the procedures of conduct during a conflict.

Organizational structure – the structure entails the parties of a cyber conflict divided functionally and organizationally. There are official and functional relations both between the personnel, as well as between the teams taking part in a conflict.

Technical structure – technical resources e.g. technical (ICT) devices, information carriers, transmission media, software or data bases. A cyber conflict as a process in intangible, i.e. it does not include material resources and consequently it uses technical resources of information systems used in a cyber conflict. The transfer of intelligence data and information between the technical resources creates specific technical relations.

A cyber conflict is determined by twofold factors: primary and secondary. A primary factor is the goal. The goal's realization is the reason for the appearance of a cyber conflict. The secondary factors of a cyber conflict include the resources of the information system used in a cyber conflict. At the same time, a cyber conflict determines the resources of information systems and it depends on them. The goal of the information process exerts influence on the choice of proper sources of information at the time of a conflict. Running a conflict in such a way that it would be beneficial requires proper technical devices, specialized personnel, as well as proper organizational structures and procedures that would assure the effective realization of tasks. Each of the elements has a secondary influence on a cyber conflict. Each factor has impact on a cyber conflict individually and

in connection with others. Synergy effect is observed here. The factors also exert influence on one another. Different factors exert influence on different parameters of a cyber conflict to different extents.

The factors of a cyber conflict are:

- Primary: The goal of a cyber conflict.
- Secondary:
  - the sources of data and information;
  - data and information;
  - the resources of an information system:
    - technical;
    - organizational;
    - procedural.

Conclusion

Taking into consideration the fact that international alliances, coalitions and any multilateral agreements create peculiar organizations, a cyber conflict has a distinctive feature. On the one hand, it is an internal conflict since it takes place inside an alliance or a coalition. On the other hand, from the point of view of the member state, it is an external conflict since it takes place between subjects who care about their own interests.

Cyberspace, in spite of its short history, has already been used to run cyber conflicts, which is vital for the national security. Cyberspace is changing gradually, such progressive change is also observed in the way of perceiving and settling conflicts. Thus, the understanding of the perception of a cyber conflict, the evolution of the way of settling it by a potential adversary or the real enemy is the main manner of counteracting cyber conflicts. Making use of the experiences gained from the course of conflicts in the latest history depicts the implications of the development of the new cognition of the course of a cyber conflict. A cyber conflict might be as destructive as the conflict run with the use of conventional measures and methods.

The article presents theoretical aspects of a cyber conflict. The presented results shall be helpful in counteracting cyber conflicts. The presented analysis showed that knowledge concerning the phases, stages and factors, as well as the structure of a cyber conflict as a process is indispensable and necessary to prevent cyber conflicts. The depicted knowledge will help to understand the way of thinking of the Russian army about the course of a cyber conflict. Due to the lack of scientific grounds for the research problem, the article complements the gap in the field of science concerning the prevention of cyber conflicts, it provides a theoretical basis and inspires for further research on the understanding of the course of cyber conflicts and the way to prevent them.

References

[1] GRAY, C. S.: *The 21st Century Security Environment and the Future of War.* www.hsdl.org/?abstract&did%2520=38291 (Downloaded: 21.11.2017)

[2] AFZALUR RAHIM, M.: *Managing Conflict in Organizations.* Piscataway: Transaction Publishers, 2012.

[3] REVERON, D. S. (ed.): *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* Washington D.C.: Georgetown University Press, 2012.

[4] *Cyber conflict.* [Online]. www.macmillandictionary.com/dictionary/british/cyber-conflict (Downloaded: 12.06.2018)

[5] GODWIN III, J. B., KULPIN, A., RAUSCHER K. F., YASCHENKO, V.: The Russia–U.S. Bilateral on Cybersecurity. *Critical Terminology Foundations,* 2, (2014). (Policy report.)

[6] KELLO, L.: The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security,* 38 2 (2013), 7–40.

[7] PERKOVICH, G., LEVITE, A. E.: *Understanding Cyber Conflict: Fourteen Analogies.* Washington D.C.: Georgetown University Press, 2017.

[8] VALERIANO, B., MANESS, R. C.: The 10 things you need to know about cyberconflict. *The Washington Post* (online), September 11, 2015. www.washingtonpost.com/news/monkey-cage/wp/2015/09/11/the-10-things-you-need-to-know-about-cyberconflict/?nore-direct=on&utm_term=.4421a9d469b5 (Downloaded: 17.03.2017)

[9] Kaukasus-Konflikt tobt auch im Cyberspace. *Vorwärts* (online), 12.08.2008. www.vorwaerts.ch/tag/cyberkonflikt/ (Downloaded: 07.06.2018)

[10] В российской армии может появиться киберкомандование, заявил Рогозин. *Риа Новости* (online), 21.03.2012. https://ria.ru/defense_safety/20120321/601798789.html (Downloaded: 12.02.2018)

[11] Минобороны может создать отдельный род войск по борьбе с киберугрозами, (online) Available: https://ria.ru/defense_safety/20130705/947802340.html

[12] Источник: в России появятся войска для борьбы с киберугрозами, *Риа Новости* (online), 19.08.2013. https://ria.ru/defense_safety/20130819/957318341.html (Downloaded: 03.03.2018)

[13] *Концепция стратегии кибербезопасности российской федерации – проект.* (online) http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (Downloaded: 28.03.2018)

[14] *Будущее информационной безопасности: глобальные трансформации и сценарии для России.* Москва: Центр Стратегических Разработок, s.d. (online) www.csr.ru/?s=информ ационной+безопасности (Downloaded: 16.04.2018)

[15] ГЕРАСИМОВ, В.: Новые вызовы требуют переосмысления форм и способов ведения боевых действий. *Военно-Промышленный Курьер,* 8 476 (2013).

[16] *Информация о заключенном контракте.* (online) http://zakupki.gov.ru/epz/contract/printForm/view.html?contractInfoId=19087186 (Downloaded: 16.04.2018)

[17] PONDY, L. R.: Organizational conflict: Concepts and models. *Administrative Science Quarterly,* 12 2 (1967), 296–320.

AARMS Vol. 17, No. 3 (2018) 83–100.

Evolution of Phishing and Business Email Compromise Campaigns in the Czech Republic

Jan KOLOUCH[1]

Cyberspace is an environment in which cyber-attacks can be committed. Fraudulent attacks are one of the oldest cyber-attacks of all. The aim of this article is to familiarize the reader with the evolution of phishing and Business Email Compromise (BEC) attacks that occurred to a large extent in the cyberspace of the Czech Republic from 2014 to 2018. The article describes scam, phishing and BEC definitions, as well as individual ways of implementing specific attacks. Special attention is also paid to the possible criminal liability of the attacker for the described cyber-attacks, both according to the international legal regulations (enshrined in the Convention on Cybercrime) and according to the legislation of the Czech Republic.

Keywords: *scam, phishing, Business Email Compromise, cybercrime, cyber-attack, fake email, execution*

Introduction

Cybercrime[2] is considered a new kind of crime but the major part of this criminal offence uses or transfers notorious kinds of illegal conduct (e.g. fraud, copyright breach, theft, bullying, etc.) in the digital environment where such crimes can be committed in a more "effective" way compared to the real world.

The approach which is very frequently adopted by attackers in a virtual environment can be compared to an "area bombing" while with such massive extent of the attack, one can assume that there will be someone who will fall for it.

On the other hand, currently there are more and more cyber-attacks[3] which are very specifically targeted, prepared for a long time and which use elements of social engineering in a way that the attackers can achieve their goal.

[1] Associate professor, dr. jur., Ph.D., Ambis (www.ambis.cz/); e-mail: jan.kolouch@ambis.cz

[2] Cybercrime represents a crime where the means of information and communication technologies are used as a tool for committing a crime and also represent a target for the perpetrator's attack, while such an attack is a criminal offence. All this is subject to the condition that the means are used or misused in the information, system, program or communication environment (i.e. in cyberspace). See [12: 55].

[3] Prosise and Mandiva define a "computer security incident" (that can be perceived as a cyber-attack or cyber-crime) as an unlawful, illegal, unauthorised, unacceptable action that concerns a computer system or a computer network. Such action can take the form of, for instance personal data theft, spam or other intrusion, misappropriation, proliferation or possession of child pornography and others. [16: 13] The other definition can be found in [5: 9; 12: 55]. Cyber-attack can also be defined as any illegal action by the offender in the cyberspace, targeted against the interests of another person. Such action needs not always constitute a criminal offence; the key is that it hinders the everyday life of the injured. A cyber-attack can be either completed or it can be in preparation or only attempted.

This paper primarily deals with the evolution of fraudulent attacks in the Czech Republic. However, in order to understand the issue better, it provides definitions of the terms "scam", "phishing" and "Business Email Compromise" first (as well as the specifics of such cyber-attacks) and presents some significant fraudulent attacks that occurred in the Czech Republic. Towards the end, the paper deals with the possibilities of criminal prosecution of the perpetrator for such acts.

Cyber Attacks: Scam, Phishing, Business Email Compromise (BEC)

Scam

The term "scam" is simply defined as: *a* dishonest scheme; a fraud. [18] However, from the point of view of cybercrime, such a definition is insufficient and it would include a much wider group of criminal acts, not just cybercrime.

A more suitable definition of scam, from the point of view of cybercrime, can be found in the Business Dictionary: "A fraudulent scheme performed by a dishonest individual, group, or company in an attempt to obtain money or something else of value. Scams traditionally resided in confidence tricks, where an individual would misrepresent themselves as someone with skill or authority, i.e. a doctor, lawyer, investor. After the internet became widely used, new forms of scams emerged such as lottery scams, scam baiting, email spoofing, phishing, or request for helps. These are considered to be email fraud. Also see phishing, scheme." [17]

Scam represents spam[4] with criminal or other deceptive contents, while scam currently constitutes a significant part of spam and its purpose is, typically with the use of social engineering, to gain the user's trust and make the user carry out the required tasks (e.g. open an email attachment, go to a certain URL, etc.). Scam may include *phishing, malware, 419, hoax, fake lotteries and offers, donor scam, cold-call scam, Facebook-like scam etc.*[5]

From the point of view of general taxonomy, the term "scam" is a broader term than the terms "phishing" and "Business Email Compromise". It is also possible to say that scam represents a distribution platform which is used by cyber attackers, usually in connection with social-engineering techniques.

---

[4] Spam means any unsolicited message. Very often, this term is incorrectly connected with unsolicited business messages only.

[5] Phishing—see below. 419 scam—this refers to a fraud scheme also known as the Nigerian Prince scam. Hoax—refers to "chain emails". Donor scam typically involves requests for help with alleged illness (of a child, family member, etc.) or financial problems. Cold-call scam—this is usually an email from an IT department or company. The message includes information that the user's computer system has been infected with malware and therefore it is necessary to remotely connect the computer to the IT department to deal with the problem. For further details see e.g. [7].

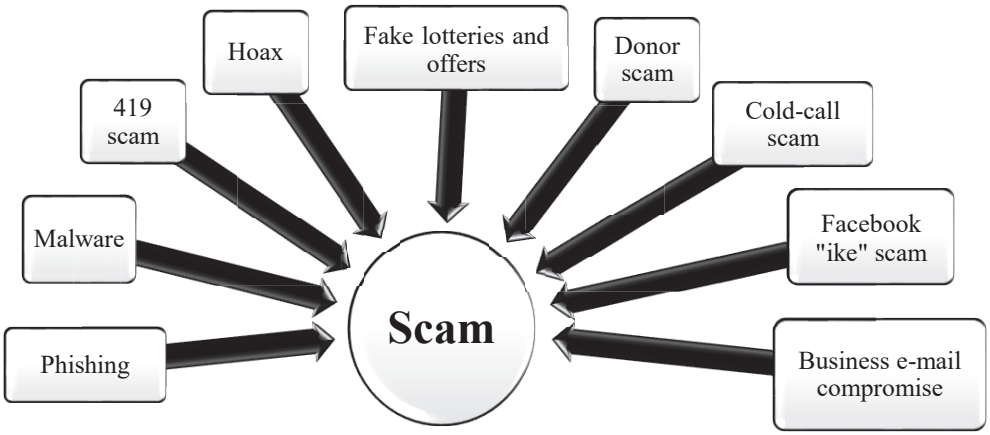


Figure 1. *Scam attacks.* [12: 236]

Phishing

The term “phishing” most frequently refers to a fraudulent or deceptive act the purpose of which is to obtain information about the user, typically the user’s name, password, credit card number, PIN, or other data and information which might be used by the attacker.

The principle of a typical phishing attack usually consists in the practice of sending a phishing email to the injured party while at first sight such an email does not arouse suspicion of a fraudulent message. Such email usually contains a link and the user is encouraged to click on it. When the user clicks on the link, it opens a website created by the fraudster. A fraudulent website may imitate any possible website where the user is used to fill in their “login data” or other sensitive information. This usually regards internet banking websites, e-shops, mail servers, social networks, etc.

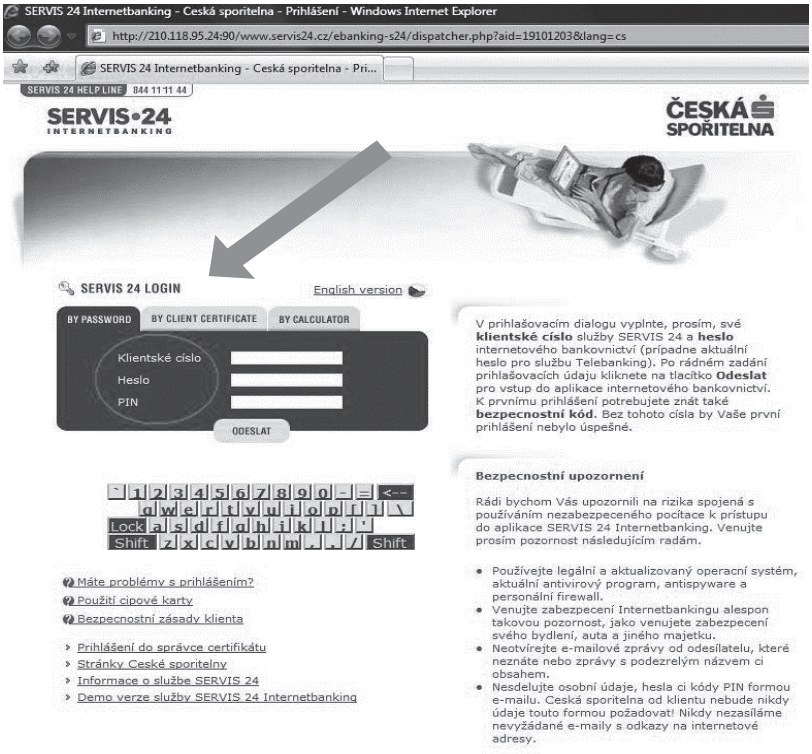


Figure 2. *Phishing site requesting the user to fill in their login data, including the PIN number (2009 attack).* [Print screen created by the author.]

This method of coaxing login data and other sensitive information out of the victim is currently on the decline and only rarely used by attackers. The above act can be called phishing "in a strict sense".

In the broader sense of the term phishing may refer to any fraudulent act the purpose of which is to inspire confidence, make the user drop their guard, or in any other way make the user accept the scenario prepared by the attacker in advance. In this concept, the user is not requested to fill in the login data but they receive a message (or the user is redirected to a website) which usually contains malware that is able to collect the data itself. This broader concept of phishing may also include e.g. scam[6] etc.

An example of this approach includes, but is not limited to, scam that offers interesting job positions. An example of such emails is shown in Figure 3. Figure 4 shows an analysis of the URL referred to in the email.

[6] In 2014, for example, Google stated that scam, having the character of high-quality phishing, has a 45% success rate if user data are obtained. See e.g. [3].

Hello!

We are looking for employees working remotely.

My name is Geneva, I am the personnel manager of a large International company.
Most of the work you can do from home, that is, at a distance.
Salary is $2500-$5000.

If you are interested in this offer, please visit **Our Site**

Best regards!

Figure 3. *Job offer (attack carried out between 2016 and 2018).*
[Print screen created by the author.]

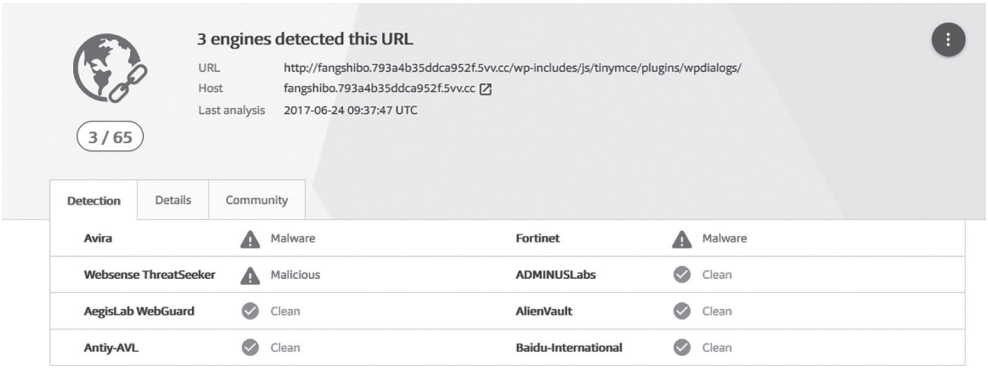


Figure 4. *Analysis result (attack carried out between 2016 and 2018).*
[Conducted with the tool www.virustotal.com edited by the author.]

The aim of a phishing attack, whether in the narrower or broader sense of the term, is to deceive the user. The difference between the individual forms of the attack consists mainly in the level of cooperation required from the user.

For a phishing attack to be successful, the attacker needs to make use of all social-engineering techniques, while phishing is not focused on emails only. Phishing can be found in instant messages, on social networks, in SMS and MMS messages, chat rooms, scam, false browser applications, etc.

The next step in the evolution of phishing was the implementation of various types of malware directly in the scam message body. To demonstrate the evolution of a phishing attack, I am going to present two important campaigns which took place, or which are taking place, in the Czech Republic. The reason for choosing the two specific attacks is the distinctly innovative approach of the attackers and the link between the technical attack and social engineering.

Case 1 – Debt/Bank/Execution

This phishing campaign hit the Czech Republic to a great extent in 2014 and lasted at least till the end of 2015.[7] The principle of this attack was employed again, with minor modifications, at the end of 2017 and in the first quarter of 2018. The attack itself was prepared with precision and included both phishing and malware distribution (to computer and mobile devices). The entire attack can be divided into the following phases:

1. Phishing campaign.
2. Installation of malware on the computer.
3. Access to online banking.
4. Installation of malware on a mobile device.
5. Transfer and siphoning of funds.

Ad 1. Phishing campaign

The first prerequisite for the attackers to successfully obtain the funds is an extensive phishing campaign which would trigger a response from a sufficiently large number of persons. In 2014–2015, fraudulent emails were sent out in three consecutive massive waves of phishing messages:

I. Debt (debt@…); March–April 2014
II. Bank (bank@…); May–June 2014
III. Distress (emissions@…); July–September 2014

The fourth wave of the attack uses what is now a well-established and tried and tested modus operandi, as well as any infected computer system from the previous three waves.

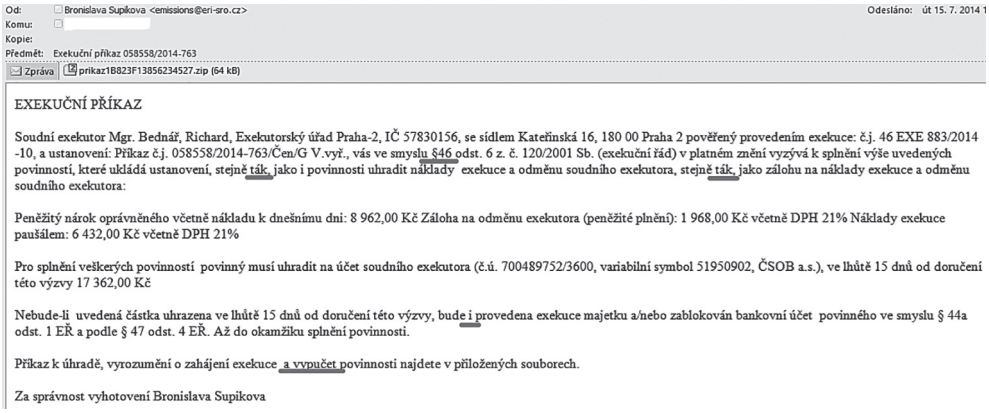
IV. Distress (e.g. podatelna@exekutor.cite etc.); October 2017–March 2018

During the individual campaigns, the "quality (credibility)" of the emails increased and social engineering was used more effectively in relation to the expected victims within the targeted area, i.e. the Czech Republic. However, all of the aforementioned phishing campaigns had at least two characteristics in common. Firstly, the attachment of the email always included a file which looked like a text document but it was an executable file, namely malware: Trojan.[8] The other characteristic in common was the fact that social engineering benefited from concerns of those addressed over lawsuits resulting from a non-existent debt, or distress in the last case.

The first wave of phishing attacks used very poor Czech and the messages were sent from various domains registered in the Czech Republic which were not exactly credible. It used names of various people and existing telephone numbers which could be looked up on the Internet (while the owner of the number had nothing to do with the attack). In the second wave, the Czech language improved. When such phishing attacks started to appear, various

[7] For further information see [14].
[8] For further information see the results from [26].

security organizations and Computer Security Incident Response Team (CSIRT) teams,[9] as well as mass media, issued warnings and provided manuals showing what to do with such messages. [1] [2] [8] [9] [24] Both campaigns were relatively successful but most success was achieved during the third wave when the attacker impersonated a bailiff.


Od: Bronislava Supikova <emissions@eri-sro.cz> Odesláno: út 15. 7. 2014 1
Komu:
Kopie:
Předmět: Exekuční příkaz 058558/2014-763
Zpráva | prikaz1B823F13856234527.zip (64 kB)

EXEKUČNÍ PŘÍKAZ

Soudní exekutor Mgr. Bednář, Richard, Exekutorský úřad Praha-2, IČ 57830156, se sídlem Kateřinská 16, 180 00 Praha 2 pověřený provedením exekuce: č.j. 46 EXE 883/2014 -10, a ustanovení: Příkaz č.j. 058558/2014-763/Čen/G V.vyř., vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění výše uvedených povinností, které ukládá ustanovení, stejně ták, jako i povinnosti uhradit náklady exekuce a odměnu soudního exekutora, stejně ták, jako zálohu na náklady exekuce a odměnu soudního exekutora:

Peněžitý nárok oprávněného včetně nákladu k dnešnímu dni: 8 962,00 Kč Záloha na odměnu exekutora (peněžité plnění): 1 968,00 Kč včetně DPH 21% Náklady exekuce paušálem: 6 432,00 Kč včetně DPH 21%

Pro splnění veškerých povinností povinný musí uhradit na účet soudního exekutora (č.ú. 700489752/3600, variabilní symbol 51950902, ČSOB a.s.), ve lhůtě 15 dnů od doručení této výzvy 17 362,00 Kč

Nebude-li uvedená částka uhrazena ve lhůtě 15 dnů od doručení této výzvy, bude i provedena exekuce majetku a/nebo zablokován bankovní účet povinného ve smyslu § 44a odst. 1 EŘ a podle § 47 odst. 4 EŘ. Až do okamžiku splnění povinnosti.

Příkaz k úhradě, vyrozumění o zahájení exekuce a vypučet povinnosti najdete v přiložených souborech.

Za správnost vyhotovení Bronislava Supikova

Figure 5. *Fraudulent email sent during the "Distress" wave.*
[Print screen created by the author.]

The text in the Czech language used in the "distress warrant" showed errors, especially in diacritics and contained several overcomplicated sentences. However, it mentioned names of real bailiffs which could be looked up on the Internet (again, the bailiff had nothing to do with the attack) and distress proceedings numbers that looked real.

Ad 2. Installation of malware on the computer

As mentioned above, all phishing campaigns contained the following malware in the email attachment: TrojanDownloader (i.e. malware designed for downloading another malware). The malware was primarily created for and aimed at the Windows XP operating system, the support of which ended in March 2014.


Název	Velikost
smlouva_26.06.2013-signed_893589F59975811EF.exe	85 504

Název	Velikost	Komprimovan...	Změněn
prikaz-15.07.2014-signed_6F532B472446324E4.exe	120 832	64 350	2014-07-15 11:00

Figure 6. *Executable file (malware) contained an attachment to fraudulent emails.*
[Print screen created by the author.]

[9] For more information see e.g. [27].

When the attachment was run, it initiated installation of the "Tinba" malware (bank Trojan horse) which was downloaded from the Internet in the background, while a contract or a distress warrant was shown to the user in a text editor.[10]

Malware was written in the following directory: Users/*user*/AppData/Roaming/brothel. In this directory, ate.exe could be found, which is a file that was created when the executable file from the phishing email was opened. At the same time, a key was created in the registers at HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun.

Ad 3. Access to online banking

Once the malware had been installed, the attacker waited until the victim logged into their online banking. The malware on the computer was able to detect the communication between the user and the online banking system and the attacker could monitor the communication. The user had almost no chance to recognize the attack as the URL address in the browser belonged to the bank and the communication was secured (HTTPS).

"The theft of sensitive data occurs when a malicious code is input on the bank's official website. Configuration scripts are downloaded from C&C servers (machines which belong to the attackers and are used to control the botnet) and deciphered as mentioned above. The interesting thing is the use of the same format of the configuration files known as Carberp and Spyeye bank Trojans. For each botuid (unique value which identifies the user's environment), a list of user names and passwords is stored on the C&C server. Other scripts are downloaded depending on the bank, i.e. hXXps://andry-shop.com/gate/get_html.js;hXXps://andry-shop.com/csob/gate/get_html.js; or hXXps://yourfashionstore.net/panel/a5kGcvBqtV, and the download occurs if the victim goes to the websites of Česká spořitelna, ČSOB, or Fia." [10]

Ad 4. Installation of malware on a mobile device

The next step of the attacker was to persuade the user that it was necessary to enhance the security when accessing online banking. The victim was offered a website with a choice of the operating system for the mobile device (OS Android, Windows Phone, Blackberry and iPhone), but only the OS Android version allowed the malware to be downloaded to the phone. Attackers used various methods of how to distribute the malware to the phone—from simply sending a text message with a link where the user was supposed to download the programme, to sending a text message and the QR code.

The malware downloaded and installed on a mobile device was detected by the company Avast! as Android: Perkele-T.

The aim of the malware was to get access to and full control over the secondary authentication tool (two-factor authentication) which is, in a majority of cases, represented by a mobile phone. If the user has an operating system other than Android, the following message was displayed: "Please try again later."

[10] For further information see the analysis of Tinba malware operation. [21]

Ad 5. Transfer and siphoning of funds

The last step of the attacker was to siphon off funds from the account of the person attacked and transfer them to an account of a money mule who was supposed to withdraw cash, or transfer it to other accounts. Thanks to the full control (by means of the malware) both over access data for the internet banking (see the computer attacked) and over the secondary authentication tool (see the mobile phone attacked—when the authentication messages were forwarded to the attacker and not displayed to the victim), the attacker could enter a "legitimate" command to transfer the money.

A modification of the last step can be seen in attacks that occurred between 2017 and 2018 when the attackers not always tried to transfer funds to the attacker's bank account but rather requested a transfer of a sum owed with a virtual currency, etc.

Case 2 – Christmas

Further evolution of phishing attacks can be seen during December 2014 (particularly during the Christmas period), in January 2015 and then again in the same period in 2017. The common denominator of the attacks was the type of file stored in the phishing email attachment. In the attacks, users were sent email messages wishing them merry Christmas through an e-card, or they were sent messages with a confirmation of an order for allegedly purchased electronics.

All the attacks had one element in common and that was the malware contained in the email attachment. The malware was a Trojan horse (the most frequently used malware was Kryptik) which was presented as a screen saver. Same as in Case 1, the malware was compressed in a .zip file so as to pass antimalware protection of the given email service. Nevertheless, when the .zip file was unpacked, many users did not consider the *.scr*[11] file to be a defective and executable (*.exe*) program and thus their computer was infected.

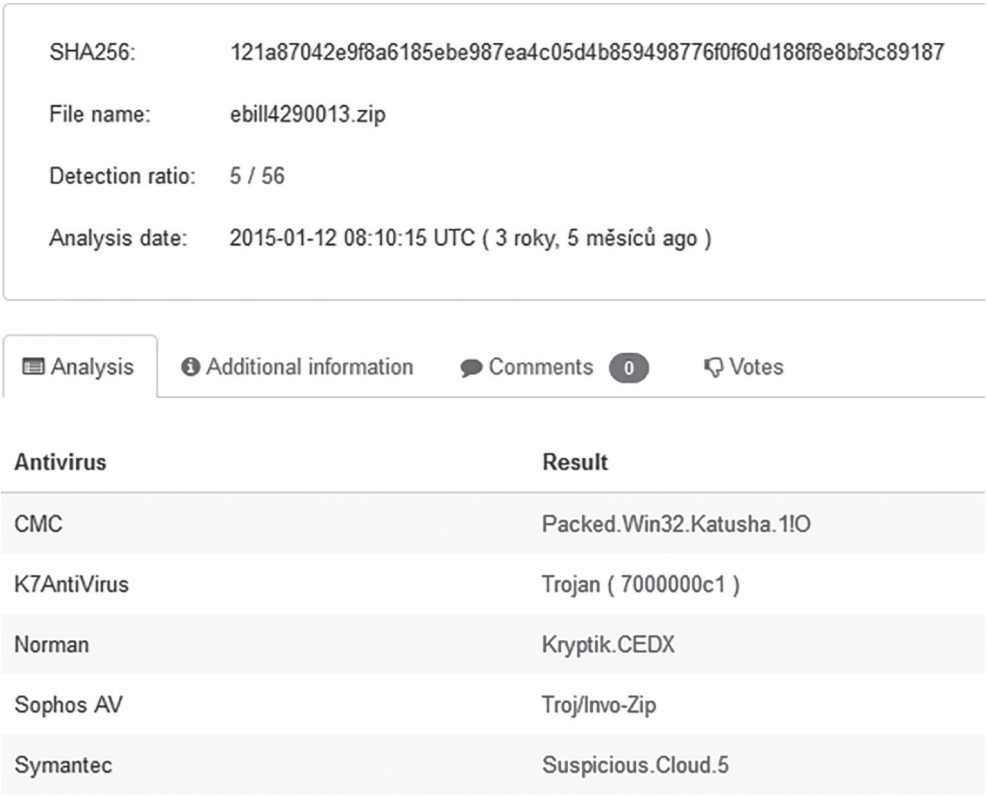
pohlednice.scr

Figure 7. *"Christmas card" attachment – .scr card.*
[Print screen created by the author.]

[11] SCR files are executable files. Primarily they are assigned to the Unknown Apple II File program (found on Golden Orchard Apple II CD Rom). Furthermore, they are also assigned to Windows Screen Saver, Image Pro Plus Ver. 1.x – 4.5.1.x Macro (Media Cybernetics Inc.), TrialDirector Script File (inData Corporation), Screen Dump, Screen Font, Statistica Scrollsheet, Procomm Plus Screen Snapshot File, Movie Master Screenplay, Mastercam Dialog Script File (CNC Software Inc.), Sun Raster Graphic, LocoScript Screen Font File (LocoScript Software), Faxview Fax, DOS DEBUG Input File, Script and FileViewPro. [22]

The attack was specific for several reasons. One reason was the type of file which many users consider to be safe and the other was the timing of the attack. Thanks to various chain emails, users are used to opening e-cards, or attachments that look like e-cards, without careful examination of the contents. Further attacks were planned so that the user had to check whether they really had not ordered some goods which were not delivered to the user due to Christmas holidays.

The last key factor which facilitated the massive extent of this phishing campaign and effective infection of computers with this malware was the relatively long zero-day vulnerability, [25] as the timing of the attack fell on Christmas and Christmas holiday when a number of people (also in anti-virus companies) are off. In the first fortnight of the attack, only a few anti-virus companies were able to analyse that the *pohlednice.scr* file contains malware. (See Figure 7.)



SHA256:	121a87042e9f8a6185ebe987ea4c05d4b859498776f0f60d188f8e8bf3c89187
File name:	ebill4290013.zip
Detection ratio:	5 / 56
Analysis date:	2015-01-12 08:10:15 UTC (3 roky, 5 měsíců ago)

Analysis | Additional information | Comments 0 | Votes

Antivirus	Result
CMC	Packed.Win32.Katusha.1!O
K7AntiVirus	Trojan (7000000c1)
Norman	Kryptik.CEDX
Sophos AV	Troj/Invo-Zip
Symantec	Suspicious.Cloud.5

Figure 8. *Result of the analysis 14 days after the attack.*
[Conducted with the tool edited by the author.]

Business Email Compromise (BEC)

Business Email Compromise[12] is a type of scam attack where an attacker impersonates an executive (typically the CEO), and attempts to get an employee, customer, or vendor to transfer money or sensitive information to the attacker.

The BEC scam could be linked to other forms of fraud like a romance, lottery, employment, and rental scams.

By the definition of the FBI, BEC is a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. [4]

Unlike a traditional phishing attack, BEC is targeted at a certain individual or organization. In case of a BEC, the attacker prepares for the attack very thoroughly and tries to obtain maximum information about the victim before the attack takes place. Usually they use websites, annual reports, information about the organization's employees from social networks, compromised email accounts, etc.

This high level of targeting helps these email scams to slip through spam filters and evade email whitelisting campaigns. It can also make it much, much harder for employees to recognize the email is not legitimate. [23]

The victims of the BEC scam range from small businesses to large corporations. BEC scam is linked to other forms of fraud, including but not limited to: romance, lottery, employment, and rental scams.

The FBI warned that BEC scams would likely "continue to grow, evolve, and target businesses of all sizes." The FBI also mentioned that they have seen a 1.300% increase in business email compromise attacks since January 2015. [4]

The BEC attackers rely heavily on social engineering tactics to trick unsuspecting employees and executives. Some of the sample email messages have subjects containing words such as *request, payment, transfer,* and *urgent,* among others.

BEC scam usually takes one of the following forms:

1. *CEO Fraud*
   Attackers pose as the company CEO or other company executive and send a spoofed email to employees with the ability to send wire transfers, and instruct them to send funds to the attackers.

2. *Fake Invoice*[13]
   A business, which often has a long-standing relationship with a supplier, is requested to wire funds for invoice payment to an alternate, fraudulent account. The attacker typically approaches the victim via email or telephone. An email attack has typically a spoofed email source code (header) and subject of the request, so it appears very similar to a legitimate request.

---

[12] BEC scams are also known as "CEO fraud" or "Man-in-the-Email" scams.

[13] This attack is also called "The Bogus Invoice Scheme", "The Supplier Swindle", and "Invoice Modification Scheme".

3. *Account Compromise*
   This attack is similar to Fake Invoice. The attacker uses an employee's email account (hacked or spoofed), then sends an email to customers to announce them there has been a problem with their payment and they need to re-send it to a different account.

4. *Business Executive and Attorney Impersonation*
   Victims are contacted by attackers, who identify themselves as lawyers or representatives of law firms. The attacker requests a large funds transfer to help settle a legal dispute or pay an overdue bill. The attacker is trying to convince victims that the transfer is confidential and time-sensitive, so it is less likely that the employee will attempt to confirm whether they should transfer the funds.

5. *Data Theft*
   A type of BEC whose goal is not a direct money transfer. Typical victims of that attack include finance or HR departments/employees. The attacker requests them to send highly sensitive data to his account. Social engineering is used and the data theft attack can be a starting point to the above mentioned BEC attacks focused on financial transfer.

Since 2017, there has been a dramatic increase in fraudulent attacks having the character of BEC in the Czech Republic. Yet again, most BEC attacks use similar modus operandi:

1. *Picking a victim and obtaining information about the victim* (medium-sized and small organizations are the most common targets.)
2. *Preparation of a spoofed email* (to create a spoofed email, publicly available free services are used very often, e.g. www.5ymail.com. This service allows the attacker to create and send any spoofed email which corresponds to an existing email. However, this service does not make it possible to receive answers and therefore it is necessary to redirect the email communication to another existing email, registered e.g. with a free-mail service. The real identity can be found from the message source code.)
3. *Sending a spoofed email to an employee of the victim* (the most frequent BEC attacks include CEO Fraud and Fake Invoice. Sums required in this way usually range from several hundred Euros to € 4,000.)
4. *Request for an immediate or "urgent" transfer of money to an account of the attacker or money mules* (validation of the payment, as well as of the person who gives the command to make the payment, is the key moment when the completion of the criminal act can be prevented. If the organization has appropriately set up security protocols, such transfer usually does not take place. From the point of view of identification of the attacker, the attacker's account, or the account of money mules, it is the tool which makes it possible to determine in practice whether it is the case of continuation of a criminal act [i.e. from the point of view of substantive criminal law one criminal act] or whether it is a case of concurrence of criminal acts. At the same time, it is de facto the most significant digital footprint which allows identification of the attacker.)
5. *Money transfer to an account of the attacker or money mules*

Towards the end of this paper on phishing and BEC attacks, I am going to mention some statistics of the Czech national CSIRT team and of the Czech Police, focused on fraudulent acts or spam.

Table 1. *Statistics of CSIRT.cz.*

	2008	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**sum**
Phishing	65	220	209	144	159	175	368	367	363	409	231	2,710
Spam	47	28	103	26	43	73	159	108	290	121	73	1,071
Pharming							18	3	2	3	3	29

Table 2. *Statistics of the Police of the Czech Republic.* [19]

Structure of criminal offences	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
Fraudulent acts	917	1.303	1.863	2.478	2.932	3.235	3.036
Total share	61.05%	59.36%	59.94%	56.99%	58.37%	60.54%	55.76%

Legal aspects of Phishing and Business Email Compromise (BEC) campaigns

Based on the attacks described above, it is possible to apply the individual provisions of *Convention No. 185 on Cybercrime of 23rd November 2001* to penalize the perpetrator, with necessary modifications according to national legal regulations.

When determining which section of the Convention on Cybercrime is to be applied, it is essential to analyse the attacker's specific acts, particularly the fact whether it is just a fraudulent act or a combined attack, which uses e.g. malware, the aim of which is to identify a specific computer system and only then obtain data in the form of access information.

From this point of view, it is necessary to distinguish the following situations:

1. *Sending a phishing or BEC message, infected file, or a link to an infected website*

Most frequently, the victim is sent an email which contains a link which the user is prompted to follow. Once the user has clicked on the attached link, they are directed to a website, the layout and functions of which do not differ from the authentic website. The phishing website collects data entered on the fake websites and sends them automatically to the offender.

Enclosing the malicious code directly in the email is another way to infect the victim's computer.

From the legal point of view, the *Convention on Cybercrime* classifies the action by the offender, i.e. sending of the file through which the offender may gain control over somebody else's computer, or re-directing to the website containing malware, as an *attempt* or *aiding* or *abetting* to criminal offences. In this case, the action most likely constitutes an attempt to commit a criminal offence as defined in Articles 4 through 6 of the Convention on Cybercrime. For future reference, the above-mentioned articles of the Convention on Cybercrime are described below in detail:

Article 4 of the Convention – Data interference

1. *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.*
2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.
   In conjunction with the relevant provisions of national criminal law, this article provides for sanctioning actions consisting of *intentional installation of malware into a computer system without the consent of the system's rightful user.*

Article 5 of the Convention – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

While Article 4 of the Convention defines the merits of a criminal offence against data in a computer system, i.e. the interference with the data does not necessarily cause damage to the computer system (e.g. changing data in a database), this Article protects the functioning of a computer system as a whole, and the actions described in Article 4 here hinder the functioning of the computer system affected.

Article 6 of the Convention – Misuse of devices

1. *Each Party shall adopt such legislative and other measures as may be necessary to establish criminal offences under its domestic law, when committed intentionally and without right:*
   a) *the production, sale, procurement for use, import, distribution or otherwise making available of:*
      i. *a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;*
      ii. *a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,*
      with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
   b) *the possession of an item referred to in paragraphs a) i. or ii. above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.*

In accordance with the above provision, *all offenders who proliferate*, sell, procure for themselves or others, import, distribute or otherwise make available for instance malware (programmes such as computer worms, Trojan horses, key loggers, etc.) should be sanctioned.

2. *Entering the malicious code in the computer*

From the legal point of view, the action by the offender consisting of the malware installation (without the consent of the rightful user) into the compromised device constitutes a completed criminal offence as defined in Articles 2, 4 and 5 of the Convention on Cybercrime. Article 2 of the Convention defines *"Illegal access"* as committed by a person through gaining an unauthorised access to a computer system or its parts.

From the legal point of view, ***Article 8 of the Convention on Cybercrime—Computer-related fraud—can also be applied to the above described action.***

Each Party shall adopt such legislative and other measures as may be necessary to establish criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a) *any input, alteration, deletion or suppression of computer data,*
b) *any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.*

The above described action, which according to this Article should be criminally punishable, occurs most frequently in conjunction with other actions that the Convention aims to mitigate. For instance, the attacker first obtains the programme that enables him to interfere with a computer system without authorisation (Article 6). Next, he uses the programme obtained to execute the attack by simulating the person's authorisation to dispose with a bank account (Articles 4 and 7). Finally, he may give instructions to transfer money to his benefit or to the benefit of a third party (Article 8).

It is precisely the provisions of Article 8 of the Cybercrime Convention that have been adopted to combat attacks in the form of fraud (typically scam, phishing, pharming, spear phishing, BEC).

According to the Czech criminal law, any conduct having the character of "classic phishing" can be penalized according to *sec. 209* (Fraud) of the Criminal Code, [28] while fraud is completed by self-enrichment. Creation of a website replica and obtaining of login names and passwords could be classified as a preparation of a criminal act, or as an attempt to commit a criminal act, according to sec. 209 of the Criminal Code. Obtaining of access data, including account numbers, payment card numbers and PIN codes, without further use thereof, is not necessarily punishable.

In case of combined forms of phishing attacks, when malware is used to infect the computer, such conduct carried out by the perpetrator needs to be penalized also according to *sec. 230* (unauthorized access to a computer system and data medium) of the Criminal Code. If the purpose of a phishing attack is to gain unauthorized benefit for oneself or others, provisions of *sec. 230, par. 3* of the Criminal Code, may also be applied.

In specific cases, provisions of *sec. 234* of the Criminal Code could also be applied (unauthorized obtaining, forging and modification of a payment means).

Conclusion

As mentioned at the beginning of the paper, fraudulent attacks represent one of the oldest cyber-attacks in general, but especially due to irresponsible and careless behaviour of users, they will be one of the most common types of cyber-attacks in the future.

It is extremely difficult to determine how many fraudulent attacks are carried out all over the world every day. Likewise, it is hard to determine how many clients of the companies attacked reply to a scam, phishing or other defective email. The return rate is estimated at approx. 0.01 and 0.1%.[14] [13: 35]

Although the scam return rate is negligible, with the extent at which emails having the character of scam or phishing are sent, the aforementioned percentage represents a significant financial profit for the perpetrators of the attacks.

2007 prognoses estimated that there were going to be more "typical" phishing scams or campaigns in the future.[15] The prognoses have partly come true as "typical" phishing campaigns are on the decrease, but phishing in the broader sense of the word is booming[16]— new phishing modifications appear and phishing is also connected with other types of attacks (malware, connection to the botnet network, etc.).

References

[1] *Beware of a message about an alleged unpaid claim – it is a scam.* CSIRT.cz (online). www.csirt.cz/page/2073/pozor-na-zpravu-o-udajne-neuhrazene-pohledavce---jedna-se-o-podvod/ (Downloaded: 15.08.2016)

[2] *Beware of a notice to pay before distrain – it is scam.* CSIRT.cz (online). www.csirt.cz/news/security/?page=87 (Downloaded: 15.8.2016)

[3] SOUZA, R. D.: *Beware of Fake Android Prisma Apps Running Phishing, Malware Scam.* HackRead (online), 2016. www.hackread.com/fake-android-prisma-app-phishing-malware/ (Downloaded: 14.08.2016)

[4] FBI: *Business E-mail Compromise: The 3.1 Billion Dollar Scam*. FBI Field Office (online), June 14, 2016. www.ic3.gov/media/2016/160614.aspx (Downloaded: 12.06.2018)

[5] CASEY, E.: *Digital Evidence and Computer Crime: Forensic Science. Computers, and the Internet.* Second Edition. London: Academic Press, 2004.

[6] DODGE, R. C., CARVE, C. A., FERGUSON, J.: Phishing for User Security Awareness. *Computers & Security,* 26 1 (2007), 73–80.

[14] As regards the issue of phishing compare e.g. [20] and [11: 9].

[15] For phishing trends, compare e.g. [6].

[16] According to the following study, phishing has increased by 250% over the last 6 months. See [15].

[7] *Does Microsoft call about computer being infected with virus?* Computer Hope (online), updated: May 21, 2018. www.computerhope.com/issues/ch001385.htm (Downloaded: 14.08.2016)

[8] *Fraudulent emails are back again.* CSIRT.cz (online). www.csirt.cz/news/security/?page=97 (Downloaded: 15.08.2016)

[9] *PODVODNÉ EMAILY hrozí exekucí, nic neplaťte a neotvírejte! (FRAUDULENT EMAILS threaten with a distress warrant—do not pay anything and do not open them!)* TN.cz (online). http://tn.nova.cz/clanek/zpravy/cernakronika/podvodne-emaily-hrozi-exekuci-nic-jim-neplatte-a-neotvirejte.html (Downloaded: 15.08.2016)

[10] HOŘEJŠÍ, J.: *Falešný exekuční příkaz ohrožuje uživatele českých bank. (A false distress warrant puts users of Czech banks at risk.)* avastblog (online), July 17, 2014. https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/ (Downloaded: 15.08.2016)

[11] KOLOUCH, J., VOLEVECKÝ, P.: Criminal law aspects of a phishing attack. *Criminal Law,* 12 (2008), 5–12.

[12] KOLOUCH, J.: *CyberCrime.* Prague: CZ.NIC, 2016.

[13] LANCE, J.: *Phishing without mysteries*. Prague: Grada, 2007.

[14] *Uhraďte dluhy, toto je exekuční příkaz. Komora varuje před další vlnou podvodných mailů. (Pay the debts, this is a distress warrant. The chamber warns of another spate of fraudulent emails.)* Aktuálně.cz (online), October 19, 2015. http://zpravy.aktualne.cz/finance/falesne-exekuce-jsou-zpet-komora-varuje-pred-dalsi-vlnou-pod/r~cbdac6de765111e599c-80025900fea04/ (Downloaded: 15.08.2016)

[15] Phishing Activity Trends Report. *APWG* (online), 1st Quarter 2016. https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf (Downloaded: 14.08.2016)

[16] PROSISE, C., MANDIVA, K.: *Incident response & Computer forensic.* Second edition. Emeryville: McGraw-Hill Companies, 2003.

[17] *Scam.* (online). www.businessdictionary.com/definition/scam.html (Downloaded: 11.06.2018)

[18] *Scam.* (online). https://en.oxforddictionaries.com/definition/scam (Downloaded: 11.06.2018)

[19] *Statistics of CSIRT.cz.* (online). https://csirt.cz/page/2635/statistiky-resenych-incidentu/ (Downloaded: 15.06.2018)
Statistics of the Police of the Czech Republic. (online). www.policie.cz/clanek/kyberkriminalita.aspx (Downloaded: 15.06.2018)

[20] VOLEVECKÝ, P., STACH, J.: Jak se krade pomocí Internetu – Phishing v praxi. (How to steal with the use of the Internet – Phishing in practice.) *Digital Doom's Digi World*, May 17, 2008. (online). www.ddworld.cz/software/windows/jak-se-krade-pomoci-internetu-phishing-v-praxi.html (Downloaded: 14.08.2016)

[21] KRUSE, P., HACQUEBORD, F., MCARDLE, R.: *Threat Report: W32.Tinba (Tinybanker) The Turkish Incident.* (online). CSIS Security Group and Trend Micro Incorporated, 2012. www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf (Downloaded: 15.08.2016)

[22] GEATER, J.: *Co znamená přípona souboru SCR?(What does the SCR file extension mean?)* Solvusoft (online). www.solvusoft.com/cs/file-extensions/file-extension-scr/ (Downloaded: 14.08.2016)

[23] HARNEDY, R.: *What is a Business Email Compromise (BEC) Attack? And How Can I Stop It?* Barkly (online), September 2016. https://blog.barkly.com/what-is-a-business-email-compromise-bec-attack-and-how-can-i-stop-it (Downloaded: 12.06.2018)
[24] DURAČINSKÁ, Z.: *Čo sa skrýva v prílohe podvodných e-mailov? (What is hidden in fraudulent email attachments?* CZ.NIT (online), July 23, 2014. https://blog.nic.cz/2014/07/23/co-sa-skryva-v-prilohe-podvodnych-e-mailov-2/ (Downloaded: 15.08.2016)
[25] *Zero-day (computer).* (online). https://searchsecurity.techtarget.com/definition/zero-day-vulnerability (Downloaded: 13.06.2018)
[26] *prikaz1B823F13856234527.zip* www.virustotal.com/cs/file/62170532b1f656c6917fa66d0ed98462e106f3aa139273c9f2c3a370a67d265f/analysis/1471330723/ (Downloaded: 16.08.2016)
[27] www.csirt.cz/
[28] *Act no. 40/2009 Coll., Criminal Code.*

AARMS Vol. 17, No. 3 (2018) 101–114.

Analysis of Cyberattack Patterns by User Behavior Analytics[1]

Csaba KRASZNAY,[2] Balázs Péter HÁMORNIK[3]

Targeted attacks cause the most serious problems nowadays in the cyberspace, as in most cases they are used for cyber espionage, in cyber warfare activities and have a significant role in data leaks both in the governmental and private sector. Meanwhile, it is very difficult to detect such attacks in time, due to the strategy, tactics and chosen tools behind them. Therefore, a new way of cyber defense is needed to reduce risk caused by Advanced Persistent Threat (APT). In this paper we review the process of targeted cyberattacks, focusing on the challenges of authentication, then we introduce user behavior analytics (UBA) as a potential countermeasure. We also emphasize through a case study, how devastating a cyberattack can be for a company and why UBA would be a good candidate in a modern cyber defense system.

Keywords: *user behavior analytics, cyberattack, targeted attack, authentication*

Introduction

Per definition, information security is a reactive activity, as it has to manage those risks that may have a serious effect on the organization, if they happen. Historically, the Pareto principle is true here. It states that, for many events, roughly 80% of the effects come from 20% of the causes. Therefore, departments responsible for information security try to focus their limited resources to those 20%. Sometimes it works, sometimes not. In the past decades, a simple firewall or an antivirus software was enough for preventing the vast majority of attacks. Meanwhile, tools and tactics on the attacker side were continuously evolved and evaded the already implemented measures. Moreover, IT usage patterns of employees and customers has also been changed that resulted an infinite loop in the risk management process with constant re-evaluation of threats and finding the right countermeasures for the identified risk. The Pareto principle cannot be used anymore in cyber security. All hardware and software elements with or without network connectivity can be the source of an attack. There are various motives and strategies on the rogue side that are unpredictable from the CISO's chair. In this paper we analyze how new technologies can tackle this challenge. We are focusing on the problems of authentication and behavior analytics as a good example of future technologies that can reduce the risk of some specific but serious cyber security threats.

[1] The work was created in commission of the National University of Public Service under the priority project PACSDOP-2.1.2-CCHOP-entitled "Public Service Development Establishing Good Governance" in the Ludovika Cybersecurity Workshop.

[2] Ph.D., Associate Professor, National University of Public Service, Faculty of Science of Public Governance and Administration; e-mail: krasznay.csaba@uni-nke.hu

[3] Ph.D., Associate Professor, Budapest University of Technology and Economics, Faculty of Economic and Social Sciences; e-mail: hamornik@erg.bme.hu

Cyber Security Challenges of our Time

Challenges of security professionals can be described best with two definitions. A few years ago, they had to deal with the questions of information security. As the ISO 27000:2018 standard states "The purpose of information security is to protect and preserve the confidentiality, integrity, and availability of information. It may also involve protecting and preserving the authenticity and reliability of information and ensuring that entities can be held accountable." [1] Nowadays, it has to be understood that cyber security is much more complex. The International Telecommunication Union defines this term as: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- availability;
- integrity, which may include authenticity and non-repudiation;
- confidentiality." [2]

If we are trying to keep the topic simple, we can say that there are two major types of cyberattacks. The first one is similar to a shotgun. Attackers shooting out their virtual bullets to the internet not knowing who the victim will be, if any. Ransomware is a good example for this. Cybercriminals own or rent a botnet and spreading their malware through this network, using those e-mail or social accounts that were stolen before from an internet service provider's large database and were sold on Darknet. Their investment is quite low, but the income can be very high, if they are able to mislead a lot of unsuspecting internet users with a well-constructed message. With the ransomware-as-a-service model, virtually everyone can create his own code, spread it to the target audience and harvest the paid ransom in Bitcoin. In such cases the motive is fairly simple: earn as much money as possible. As they are usually targeting end users, they are building on their ignorance, the fact that they do not understand how things are going in the cyberspace. Unfortunately, those home users are many times sitting in an office and use corporate devices connected to the corporate network. From the defense perspective, this type of attack seems to be manageable, although still causes huge problems for those companies who did not invest into human awareness or latest technologies.

The second model is similar to a sniper's rifle. It targets only one organization with a special cyber weapon crafted and sharpened against its weaknesses. Many times, this attack is indirect as attackers hack a trusted third party first and reach the target organization from their network. Rogue actor has the necessary resources, such as time, money and expertise and it has a special motivation why it does this intrusion. We can call this type of activity targeted attack or Advanced Persistent Threat (APT). The National Institute of Standards and Technology in the USA defines this term as "an adversary that possesses sophisticated

levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives." [3: 6] As the intruder can use any vulnerability in the infrastructure, from the defense perspective this is similar to find the needle in the haystack. Meanwhile the initial steps were usually taken months or years before and usually stay under the radar, exfiltration needs seconds or minutes. Victims do not have time to even realize that something bad has happened.

The Process of Cyberattack

To understand why commonly used security measures, fail, we have to understand the nature of targeted attacks. Lockheed Martin in its well-known Cyber Kill Chain [4] model defines an APT in the following seven steps:

- *Reconnaissance:* Attacker defines its target, gets as much information as possible from it, and tries to find vulnerabilities in the target infrastructure.
- *Weaponization:* Attacker creates a cyber-weapon that enables remote access to the target infrastructure. This is usually a malware, such as a virus or worm, which exploits one or more identified vulnerabilities.
- *Delivery:* Attacker delivers weapon to victim. It can be transmitted via e-mail attachments, websites or USB drives.
- *Exploitation:* Cyber weapon takes effect and exploits relevant vulnerabilities on the target network.
- *Installation:* Cyber weapon opens a remote connection, usually a backdoor and lets attacker access the target infrastructure.
- *Command and Control:* through the already opened access, cyber weapon lets the attacker to persist its presence on the victim's infrastructure.
- *Actions on Objective:* as the attacker has goals, it takes the necessary actions towards them, such as data exfiltration, data destruction, or encryption for ransom.

Naturally, those seven steps cover hundreds of tactics, thousands of known tools and the same amount of currently unknown tools. With that wide variety of tools and technics only imagination sets limits to attack strategies. NotPetya ransomware is a good example how well-known tools and tactics enable a new strategy. [5] Based on experts' opinion, the motivation behind this malware was to influence Ukraine's normal daily operation and to test the resistance of maritime industry, though it seemed like an ordinary ransomware. It utilized the same EternalBlue vulnerability like Wannacry did a month before and used the hacker's favorite Mimikatz tool to extract privileged accounts from the memory. Nothing what we did not see before. But the malware is believed to be originated from

the software update mechanism of M.E.Doc, a Ukrainian tax preparation software, widely used in the country. No one expected that the source of a global malware campaign would be a local software's update, that by definition, has to be installed due to security reasons. Masterminds on the attacker side did their job perfectly as they built on known vulnerabilities, both on the human and technology side and utilized already existing tools and techniques to reach their strategic goals, whatever those might be.

The MITRE Corporation, which is a not-for-profit organization that operates research and development centers sponsored by the federal government, published a huge database on cyberattack tactics and techniques. MITRE's Adversarial Tactics, Techniques and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's lifecycle and the platforms they are known to target. It fits well to Lockheed Martin's Cyber Kill Chain and provides a good insight as to how those seven steps can be carried out. During the pre-attack phase, that is Step 1–4, 173 different techniques were identified under 17 attack categories. In the attack phase, between Step 5–7, 10 categories were set up for 169 techniques. The attacker can freely use these techniques, meanwhile implementing countermeasures against all of these steps is virtually impossible in a complex environment. [6]

In a targeted attack, the turning point is when the rogue actor tries to break out from the already hacked computer. This is the so-called lateral movement. MITRE's framework enumerates several potential techniques how an attacker can extend its footprint. Back to NotPetya, the ultimate goal of gathering credentials from an infected computer was to enable lateral movements. Credentials of privileged accounts mean the keys to the kingdom, if the intruder can e.g. steal such passwords, it is very difficult to find him as from that point, he will do apparently legitimate activities. This can be presented through the Remote Desktop Protocol (RDP) example.

FireEye's Mandiant, that deals mostly with investigation of targeted cyber security incidents, writes the following on its blog: "While performing incident response, Mandiant encounters attackers actively using systems on a compromised network. This activity often includes using interactive console programs via RDP such as the command prompt, PowerShell, and sometimes custom command and control (C2) console tools." [7] Usage of RDP is also confirmed by MITRE as based on its information, even the most advanced cybercriminal groups, such as APT1 or Lazarus used this protocol many times. In practice, Windows servers usually enable remote connection through RDP as they need to be managed somehow. Those servers can be on premise or in the cloud, as well. Therefore, if the attacker has a privileged account, he has a great chance to access the whole Windows infrastructure.

Challenges of Authentication

How can RDP connections be secured? If we browse for this topic on the internet, we can find several good advices of strong password usage to enable Network Level Authentication, but none of them solves the issue of stolen credentials, even password managers can be tricked with an authorized privileged user account. Only multifactor authentication seems to be an effective measure, but many times, this is unfeasible due to infrastructure restrictions and attacks against multifactor authentication can be seen before.

As Mashable highlighted from the previously leaked NSA files, some governmental employees were attacked by "hacking" their two-factor authentication at Google through intercepting and forwarding their verification code. Although, in fact that is not a "hack", rather a good example of how social engineering can help in a man-in-the-middle attack. [8] The two-factor authentication scheme is still unbroken, but not as secure as we could imagine due to the human factor. We also have to emphasize that this attack method is not something new. We should just go back to 2009 and recall the breach at Ferma: "The theft happened despite Ferma's use of a one-time password, a six-digit code issued by a small electronic device every 30 or 60 seconds. Online thieves have adapted to this additional security by creating special programs—real-time Trojan horses—that can issue transactions to a bank while the account holder is online, turning the one-time password into a weak link in the financial security chain." [9]

As many examples prove, passwords do not mean a sufficient protection. As most information security standards and recommendations contain the need of secure password usage, we need to review the basic rules! As it is widely known, an 8 characters long password, with small and capital letters, numbers and special characters in it is essential. According to the state-of-the-art, this is a little bit outdated. Not so long ago the National Institute of Standards and Technology in the United States has closed the comment period of their NIST SP 800–63–3 on Digital Identity Guidelines and made a huge step towards user-friendly, password-based authentication. Its 800–63B part deals with the questions of Authentication & Lifecycle Management and recommends a new approach of password usage that is well-summarized by Infoworld. [10] According to this document, the new style of password creation rules are the following:

- "Users should be able to choose freely from all printable ASCII characters, as well as spaces, Unicode characters, and emojis;
- increase the minimum length of passwords to eight;
- check passwords against blacklists of unacceptable credentials, including previously breached databases, dictionary words (monkey), common passwords (letmein), and passwords with repeating or sequential characters (pass123);
- lock accounts after several incorrect attempts to login;
- hash passwords with a salt when storing passwords to prevent cybercriminals from acquiring passwords that are stored in plaintext or with weak hash algorithms." [10]

Make a step further! NIST SP 800–63B also recommends the usage of multi-factor authentication, because "password managers only solve the password challenge; they don't address the overall authentication problem when attackers already have the password" as it is stated in the Infoworld article. [10] Password managers are useful tools for storing the memorized secrets, but they are insufficient to address the full user authentication problem, especially in case of privileged users' access management. There are several user-friendly multifactor solutions that utilize the smartphone's capabilities, e.g. its fingerprint scanner and NIST recommends using such solutions, with only one exception. According to Infoworld, "NIST warned against relying on sending one-time passwords via SMS messages as a form of two-factor or multifactor authentication. SMS can easily be intercepted, so NIST suggests using software-based one-time-password generators, such as apps installed on mobile devices." [10]

The SS7 vulnerability in mobile networks[4] reminds us that SMS based authentication is risky, but the suggested software-based solutions are also vulnerable from the human direction as it was described above. Bruce Schneier was right in 2005: "Two-factor authentication solves this problem. It works against passive attacks: eavesdropping and password guessing. It protects against users choosing weak passwords, telling their passwords to their colleagues or writing their passwords on pieces of paper taped to their monitors. […] What two-factor authentication won't do is prevent identity theft and fraud. It'll prevent certain tactics of identity theft and fraud, but criminals simply will switch tactics." [11] Changing tactics is very common. As Schneier continues: "Security is always an arms race, and you could argue that this situation is simply the cost of treading water. The problem with this reasoning [that]is it ignores countermeasures that permanently reduce fraud. By concentrating on authenticating the individual rather than authenticating the transaction, banks are forced to defend against criminal tactics rather than the crime itself." [11]

The Cost of Cyberattack – Analysis of Maersk's Case

It is very rare that we hear exact numbers from companies who were victims of a cyberattack. Although the Ponemon Institute publishes a research report annually on this topic that gives an insight on a global perspective, it is anonymized and does not expose the details of unique cases. That is why the quarterly report of A.P. Moller – Maersk is an extraordinary reading for security professionals. A.P. Moller – Maersk was one of the major high-profile victims of NotPetya malware at the end of June 2017. According to Splash247.com report that time "in the two days since the Maersk Group was hit by the Petya ransomware attack, operations at many of its sites across the globe have returned to manual". [12] As the company's press release states "in the last week of the quarter we were hit by a cyber-attack, which mainly impacted Maersk Line, APM Terminals and Damco. Business volumes were negatively affected for a couple of weeks in July and as a consequence, our Q3 results will be impacted. We expect the cyber-attack will impact results negatively by USD 200–300m." [13] That is approx. 1% of the global yearly revenue of the Danish shipping behemoth.

As it turns out from the Ponemon research, US organizations have the highest average cost of cybercrime ($17.36 million), and Australia has the lowest ($4.30 million) as shown on Figure 1. [14] In that case the numbers are 10 times higher. As Maersk is the 558th on Forbes Global 2000[5] list we can be sure that there are many more companies who had, have or will have the same amount or even higher loss due to cybercriminals. Meanwhile, we have not spoken about those thousands of smaller companies who may have a loss around Ponemon's average. Therefore, we can state that cyberattacks are costly and expenses are rising according to the report.

[4] Security researchers identified some critical security holes in the Signaling System 7 (SS7) that could allow rogue attackers to listen in phone calls and access text messages, despite the encryption used by mobile networks.

[5] Forbes Global 2000 list can be found at www.forbes.com/global2000/list.

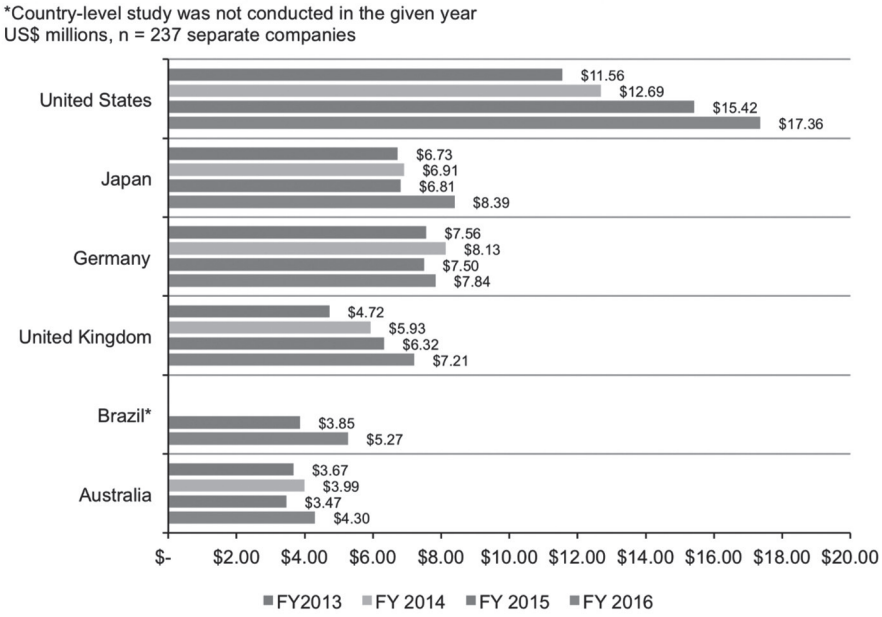


Figure 1. *Total cost of cybercrime in six countries over four years.* [14]

But there are various solutions to reduce this loss. First of all, cybersecurity should be a priority for all companies. There are no verticals or companies whose daily operation does not rely on IT, but there are verticals and companies who do not care about IT security as they are unregulated or simply, they follow the "nothing has happened yet" principle. We have to emphasize that a whole industry can suddenly get into trouble, as it has happened with the shipping industry in the Summer of 2017. Besides the Maersk case, HMS Queen Elizabeth is running outdated Windows XP and theoretically she is exposed for exploits; industry reports say that some crucial nautical infocommunication systems, such as Ecdis and VSat also have vulnerabilities. Moreover, when two modern, highly equipped US Navy ships collide with vessels in 3 months (4 in total last year), cyberattack is one of the first thing that come into the experts' mind.

Amongst others, Ponemon highlights some key factors from the technical perspective of successful companies that are also essential to reduce the cost of cybercrime (excerpt):

- *Detection and recovery.* To reduce the time to determine the root cause of the attack and control the costs associated with a lengthy time to detect and contain the attack, these organizations are increasing their investment in technologies to help facilitate the detection process.
- *Third-party risk.* These organizations are able to reduce the risk of taking on a significant new supplier or partner by conducting thorough audits and assessments of the third party's data protection practices.
- *Insider threat.* A possible negative consequence of reorganization or acquisition of a new company can be disgruntled or negligent employees. These organizations ensure

that processes and technologies are in place to manage end user access to sensitive information. Further, there are training and awareness programs in place to address risks to sensitive data caused by changes in organizational structure and new communication channels.

- *SIEM*. These companies deploy advanced *security information* and *event management* (SIEM) with features such as the ability to monitor and correlate events in real-time to detect critical threats and detect unknown threats through user behavior analytics.

These are just some examples of the challenges that need to be solved. As attackers improve their attack strategies, companies should also improve their defense strategies and the supporting toolset. There are some new technologies that are very promising and hopefully restore the balance between attackers and defenders. According to Gartner's Hype Cycle for Emerging Technologies 2017, Machine Learning or Software-Defined Security are very close to mainstream adoption and we can already see some cyber security solutions that utilize these technologies. [15]

User Behavior Analytics in Cyber Security

Finding a targeted attack nowadays is quite challenging. Cyber security industry tries to react with several new technologies to the above-mentioned challenges. One of the most promising techniques is User Behavior Analytics. Gartner has the following definition for this technology: "User and entity behavior analytics offers profiling and anomaly detection based on a range of analytics approaches, usually using a combination of basic analytics methods (e.g., rules that leverage signatures, pattern matching and simple statistics) and advanced analytics (e.g., supervised and unsupervised machine learning). Vendors use packaged analytics to evaluate the activity of users and other entities (hosts, applications, network traffic and data repositories) to discover potential incidents commonly presented as activity that is anomalous to the standard profiles and behaviors of users and entities. Example of these activities include unusual access to systems and data by trusted insiders or third parties, and breaches by external attackers evading preventative security controls." [16]

We have to emphasize that this countermeasure combines traditional security approach using rules and known patterns with machine learning as an emerging technology. Why is this mixture necessary? As attacking strategies and tools are developing, human beings responsible for cyber defense are less able to define predictable rules from the past events. Although incident management process ends up with a learning phase, when security teams can define a new rule and eliminate the chance of similar attacks for the future, a targeted attack by its nature will be slightly different from all previous attacks. "There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know" said Donald Rumsfeld, former Secretary of Defense of the United States about the types of threats. [17] This became very popular among cyber security experts and data scientists. Most traditional security products deal with known unknowns by looking for things like malware in the system, using already existing patterns and rules. The real problem, however, is the case where the attacks are previously

unknown, commonly referred to as 0-day or 0-hour attacks. We need some way of handling the "unknown unknowns" of cyber security, which are the main challenges for the future.

On the human side the existence of "unknown unknowns" also causes a huge challenge. Security teams should deal with "known unknowns" as a daily routine, but the risk of such attacks is much lower than the risk of "unknown unknowns". Goodall, Lutters, Komlodi highlighted that in such workplaces the major issues are time pressure, monotony of time consuming but not cognitively demanding tasks, and information overload. They defined the usual tasks of security teams as follows (excerpt): [18]

- *"Monitoring:* the first phase of intrusion detection (ID) work involves the ongoing surveillance of systems and network activity looking for indications of anomalous or malicious activity. This process is centered on the intrusion detection system (IDS), but is augmented by other monitoring tools and vulnerability scanners. In addition, analysts monitor an extensive set of resources, including web sites and mailing lists, for news of new attacks and vulnerabilities. These are the mundane daily tasks of ID. One analyst described how "keeping up with everything" constituted the majority of her time.
- *Analysis:* the transition from the monitoring phase to the analysis phase begins with a security trigger event. For network monitoring, this event is usually an IDS alert or recognition of an anomalous event occurring in the environment, such as a sudden spike in traffic or user complaints of slow systems. Analysis of alerts involves not only the alert itself, but many sources of data that provide the contextual information necessary to determine whether or not the alert is an actual intrusion and if so, to assess its severity. For external resource monitoring (e.g., mailing lists), the announcement of a new vulnerability or attack method necessitates further research to determine its applicability and possible severity to one's network environment.
- *Response:* the most common forms of response in ID are intervention, feedback, and reporting. Intervention depends on the role of the analyst in the organization and organizational policies. […] Feedback is usually directed at the IDS or other elements of the security infrastructure. It includes tweaking or removing IDS signatures that generate an excessive amount of false positives, even if the signature was not guaranteed to always generate a false positive."

"Unknown unknowns" can't be identified with such routine easily. With the help of machine learning from the big data set collected by cyber security tools, there is a good chance to automatically identify strange events that deviate from the normal behavior. Gartner describes the feature set of user behavior analytics as follows:

- "Profile, baseline and make visible the activity of users, peer groups and other entities.
- Detect anomalies using a variety of analytics approaches—primarily statistical models, machine learning, rules and signatures, delivered as prepackaged analytics used to create and then compare user and entity activity against their profiles.
- Correlate user and other entity activity and behaviors, and aggregate individual risky behaviors, to highlight anomalous activity.
- Rely on information about users obtained from IT directories (e.g., Active Directory) as a primary data source to feed analytics as well as provide context on users.
- Primarily address security-and-risk-management-oriented use cases, focusing on the activities of "trusted" users inside an organization, whether they are users demon-

strating abusive, noncompliant or illegal activity, or internal users who have had their accounts and hosts compromised by external hackers.
- Perform near-real-time monitoring and alerting." [16]

From the scientific perspective, Eldardiry et al. wrote a remarkable paper on the question of identification of insider attackers using machine learning. [19] In their work they prove that data from multiple sources can be used to efficiently identify anomalies of internal users' activities. They used the following data for analysis that are all related to a targeted attack as well:
- "Logon and logoff events.
- Use of removable device such as USB thumb drives or removable hard disks. Device name and type are logged with each usage event.
- File access events: e.g., file created, copied, moved, written, renamed, or deleted. For each file access the record, file name, path, type, and content are logged.
- Http access events, tagged with URL and domain information, activity codes (upload or download), browser information (Internet Explorer, Firefox, or Chrome), and whether the website is encrypted.
- Email sent and viewed are tagged with from address, to/cc/bcc addresses, subject line, sent date, text, attachment info, and whether the email is encrypted." [19]

Therefore, it is not surprising that user behavior analytics is getting a widespread technology in cyber security. There are two common product types that are unimaginable without this solution. Security Incident and Event Management or SIEM systems are widely adopted UBA as they are the center of the organizational security data collection, in that sense they have everything that is needed for machine learning. Identity and Access Management systems also started to implement UBA as they also have a huge amount of data on user activities that give a good basis for behavior analytics. As Figure 2 shows, the general interest on user behavior analytics has been increased in the last couple of years and our intention is that this curve raise in the forthcoming years as well.

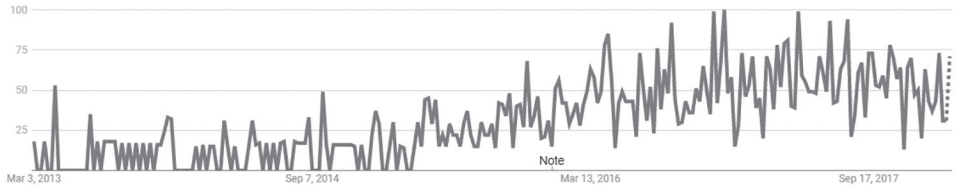


Figure 2. *Report on "User Behavior Analytics" search expression.*
[Google Trends]

Conclusion

In Hungary, the Good State and Governance Report 2017 gives an overview on cyberattacks reported for CERT-Hungary which is responsible for managing the IT security related incidents in the governmental sector. Based on this report only 0.3% of the reported incidents were classified as a targeted attack. [20] In order to identify an APT, several specific countermeasures are needed in addition to the high quality cybersecurity culture in an organization. As an example, well-prepared organizations used to have the following technical solutions:

- central security incident and event management (SIEM);
- network flow analysis;
- threat intelligence;
- malware detection with sandbox technology;
- behavior based endpoint protection;
- anti-phishing solutions;
- continuous cybersecurity awareness training;
- vulnerability analysis with social engineering tests.

This low percentage is a good indicator of how difficult to discover an APT and how far the Hungarian public administration is from the adoption of latest cyber security solutions. The above-mentioned solutions are very expensive and require a mature cybersecurity culture to be able to adopt successfully. The Hungarian public administration lacks funding and cybersecurity is not the major pain point for them, therefore we cannot expect a rapid change in APT detection. Based on the literature review and case studies we investigated in this paper, we are arguing for the wider usage of machine learning based security solutions, as they are usually accessible for the already existing solutions, like endpoint protection or SIEM systems. This situation can ameliorate with more centralization in governmental IT security, e.g. by starting a governmental managed cybersecurity service for the whole Hungarian public sector.

Meanwhile, we want to emphasize the potential challenges as well, that needs further analyses. Among these open questions, data privacy is the prime concern. As user behavior analytics needs to process user activities, such information needs to be collected. Due to regulations of the European General Data Protection Regulation, this practice might be questionable. However, we want to emphasize, that according to Section 49 of GDPR: "The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by *c*omputer *e*mergency *r*esponse *t*eams (CERTs), *c*omputer *s*ecurity *i*ncident *r*esponse *t*eams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned." [21] Moreover, UBA can also be spoofed on many ways in theory, so that area should also be monitored. In our future researches we will keep in mind these aspects.

References

[1] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: ISO/IEC *27000:2018, Information technology—Security techniques—Information security management systems—Overview and vocabulary.* ISO/IEC, 2018.

[2] INTERNATIONAL TELECOMMUNICATIONS UNION: *Definition of cybersecurity 2008.* www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (Downloaded: 17.01.2018)

[3] KISSEL, R.: *Glossary of Key Information Security Terms.* Washington D.C.: U.S. Department of Commerce, 2013.

[4] HUTCHINS, E. M., CLOPPERT, M. J., AMIN, R. M.: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. In. RYAN, J. (ed.): *Leading Issues in Information Warfare & Security Research.* Reading: Academic Publishing International, 2011. 80–107.

[5] FURNELL, S., EMM, D.: The ABC of ransomware protection. *Computer Fraud & Security,* 10 (2017), 5–11.

[6] MITRE CORP.: *Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™).* 29 January 2018. https://attack.mitre.org/wiki/Main_Page. (Downloaded: 30.01.2018)

[7] DAVIS, A.: *Monitoring Windows Console Activity (Part 1).* 1 September 2017. www.fireeye.com/blog/threat-research/2017/08/monitoring-windows-console-activity-part-one.html. (Downloaded: 16.01.2018)

[8] MORSE, J.: *The leaked NSA report shows 2-factor authentication has a critical weakness: You.* 7 June 2017. https://mashable.com/2017/06/06/russia-hackers-nsa-2fa-leaks-election-2016/ (Downloaded: 16.01.2018)

[9] LEMOS, R.: *Real-Time Hackers Foil Two-Factor Security.* 18 September 2009. www.technologyreview.com/s/415371/real-time-hackers-foil-two-factor-security/ (Downloaded: 16.01.2018)

[10] RASHID, F. Y.: *NIST to security admins: You've made passwords too hard.* 5 May 2017. www.infoworld.com/article/3194705/security/nist-to-security-admins-youve-made-passwords-too-hard.html (Downloaded: 16.01.2018)

[11] SCHNEIER, B.: *Crypto-Gram.* 15 April 2005. www.schneier.com/crypto-gram/archives/2005/0415.html (Downloaded: 16.01.2018)

[12] CHAMBERS, S.: *Back to the future for Maersk in the wake of Petya attack.* 29 June 2017. http://splash247.com/back-future-maersk-wake-petya-attack/ (Downloaded: 16.01.2018)

[13] maersk.com: *A.P. Moller-Maersk improves underlying profit and grows revenue in first half of the year.* 16 August 2017. www.maersk.com/press/press-release-archive/20170816-a-p-moller-maersk-improves-underlying-profit-and-grows-revenue-in-first-half-of-the-year (Downloaded: 16.01.2018)

[14] PONEMON INSTITUTE: *2016 Cost of Cyber Crime Study & the Risk of Business Innovation.* Traverse City: Ponemon Institute, 2016.

[15] PANETTA, K.: *Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017.* 15 August 2017. www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/ (Downloaded: 16.01.2018)

[16] BUSSA, T., LITAN, A., PHILLIPS, T.: *Market Guide for User and Entity Behavior Analytics.* Stamford: Gartner Inc., 2016.

[17] WIKIPEDIA: *There are known knowns.* 28 January 2018. https://en.wikipedia.org/wiki/There_are_known_knowns (Downloaded: 30.01.2018)

[18] GOODALL, J. R., LUTTERS, W. G., KOMLODI, A.: The Work of Intrusion Detection: Rethinking the Role of Security Analysts. In. *10th Americas Conference on Information Systems.* New York: AMCIS, 2004.

[19] ELDARDIRY, H., SRICHARAN, K., LIU, J., HANLEY, J., PRICE, B., BRDICZKA, O., BART, E.: Multi-source fusion for anomaly detection: using across-domain and across-time peer-group consistency checks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications,* 5 2 (2014), 39–58.

[20] KAISER T. (szerk.): *Jó Állam Jelentés 2017.* Budapest: Dialóg Campus Kiadó, 2017.

[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

AARMS Vol. 17, No. 3 (2018) 115–130.

Milestones Related to the Development of Organizational Aspects of Cybersecurity and Protection against Cyber-Threats in the Czech Republic

Oldřich KRULÍK[1]

Although the Czech Republic belongs to the most "internetised" countries in the world, its information and communication security policy (as well as the protection of the critical information infrastructure) lagged behind for a relatively long time, when compared to most of the remaining European countries. Building the hierarchy regarding the umbrella teams of the Cybernetic Emergency Response Teams (CERT) and Computer Security Incident Response Teams (CSIRT) type (regardless of whether we call them governmental, national or otherwise) was unthinkable without the contribution of the private sector that substituted many functions of the state in this field. The whole process can be understood as an interaction of international and national pressures appealing to the solution of the situation.

Keywords: *CERT/CSIRT, information and communication security policy, critical information infrastructure protection, measures, recommendations*

CERT/CSIRT Teams and their Role

The integral part of the preventive and active protection of cyberspace is a consistent and effective solution of security incidents, including the elimination of their causes and consequences. Network administrators and users must be prepared and must have functional structures, effective procedures, rules and technical resources to minimize the respective damages as quickly as possible. [40]

In many countries, the issue of cyberspace incidents handling is solved by the so-called CERT or CSIRT teams. [25]

The services provided by the CERT/CSIRT teams can include both *reactive* and *proactive services* (training, alerting against attacks, identification of system's weaknesses, security audits, consultations regarding the specific software, traffic monitoring tools and services, many other activities etc.).

The minimum range of such activities is, however, the addressing of respective security incidents to cover the term "response" (or "ability to respond"), contained in the term CERT/CSIRT itself. [8] [42]

The umbrella (national, governmental) CERT/CSIRT team in each country is a focal point for the individual users (firms, citizens, public institutions) to address with a specific problem

[1] Mgr., Ph.D., Police Academy of the Czech Republic in Prague, assignment; e-mail: "krulik@polac.cz

that they cannot handle themselves. In case of a cyber-attack from abroad, communication between top CERT/CSIRT teams in individual countries of the world is often faster and more efficient than police cooperation channels (and is also usable in communicating with countries with no existing mutual police cooperation channels).

CERT/CIRT Teams in the World and in Europe

The situation with regard to the existence of CERT/CSIRT teams in Europe is as follows:

- "At least some" CERT/CSIRT teams exist in each European Union member state, as well as in many other European countries.
- Some teams or institutions of such nature run the non-governmental (academic) subjects (sometimes with some state support). Iceland can serve as an example. [19]
- In many countries, CERT/CSIRT teams provide some form of service for the widest public (awareness, education, alerts etc.). Germany, the German Federal Office for Information Security can serve as an example. [4] [5]
- In a number of countries, there is a number of CERT/CSIRT platforms serving only individual private customers (firms, internet service providers, universities).
- In some countries, CERT/CSIRT teams serve mostly governmental and military structures (e.g. Turkey).
- In some countries, such structures do not exist at all.

It should be also emphasized that a particular platform will become a CERT/CSIRT team only at the moment when other existing CERT/CSIRT teams will accept it and establish channels of basic mutual cooperation.

The way of the status of a CERT/CSIRT team, however, must not be complicated, if the following key information is clearly and truthfully declared:

- Who is the founder and operator of the team?
- Basic contact information (e-mail for immediate communication, phone number, postal address, etc.).
- Scope (scope of responsibility) of the team.
- Overview of the offered services.

To get an idea about the "density" of the CIRT/CSERT teams in Europe, the most suitable are the overviews (maps) created by the European Union Agency for Network and Information Security (in 2007, the only platform for the Czech Republic mentioned was CESNET–CERTS). [7]

One of the key prerequisites for the functionality of national CERT/CSIRT teams is its high-quality and efficient *links to foreign counterparts*, which is typically formalized through "accreditation" in key transnational structures:

- The world-wide association Forum of Incident Response and Security Teams (FIRST, interconnecting about 300 teams). [15] [33]
- Organizational and certification site for the Task Force on Computer Security Incident Response Teams (TF-CSIRT) Europe, associated with Trans-European Research and Education Networking Association (TERENA). [53]

- The European Union Agency for Information Technology (ENISA), which focuses on information security from the point of view of manufacturers and operators. [21]

During the accreditation, the "identity, credibility and functionality" of a particular CERT/CSIRT team is verified. This means, in practice, that the individual team has to document its own work, including all relevant information, as well as to guarantee generally accepted patterns of behaviour and response. Preparation for such a process usually takes several years, the process itself several months (structured usually to three tiers):

- recognition (acceptance) of the entity ("listed" status);
- accreditation;
- certification (according to relevant ISO standards).

Through becoming a member of these organizations, the CERT/CSIRT teams will get the way for important and useful information, exchange and cooperation. The forum of Incident Response and Security Teams organizes a five-day conference once a year, TF-CSIRT meetings are held three times a year. The meetings are always hosted by one of the European teams. In January 2008, for example, this meeting was held in Prague, in the Czech Republic. [24]

It is also necessary to emphasize that the national environment in each country is so specific that no foreign model can be copied for the purposes of another country.

A "Tough Way" to Determine the "Umbrella Hierarchy" of CERT/CSIRT Teams in the Czech Republic

"Prehistoric Times"

The Czech Republic certainly does not belong to the countries that would be understood as pathfinders for a CERT/CSIRT team in Europe. This only illustrates the little emphasis connected to information security issues in the Czech Republic in the recent past. [29] [55]

Although the Czech Republic has been connected to the Internet since 1993 or 1994, for a long time it was impossible to talk about a comprehensive security policy in this area.

The topic of establishing a team (hierarchy of teams) of the CERT/CSIRT-type in the Czech Republic was one of the "chronic" aspects of the efforts related to the information security agenda in the Czech Republic for more than 10 years.

The need to create a CERT/CSIRT team in the Czech Republic was mentioned already in the document called *Crime Reduction Policy in Relation to Information Technologies* adopted by the Ministry of the Interior of the Czech Republic in 2001.[2] Very important is

[2] Task: *"To initiate and support CERT-type activities as a non-governmental association of qualified experts informing other professionals about security issues and responding to ongoing attacks."* Responsible body: Ministry of the Interior of the Czech Republic, in cooperation with the Office for Public Information Systems of the Czech Republic, the Chairman of the Government Council for State Information Policy, Ministry of Justice of the Czech Republic, Ministry of Culture of the Czech Republic, Ministry of Education, Youth and Sport of the Czech Republic and the National Security Authority of the Czech Republic; Deadline: 30 June 2002.

the fact that responsibility for information infrastructure in the Czech Republic has long been the subject of competence struggle (mostly "negative competence struggle", when no institution was willing to take the responsibility for the respective agenda).

Between the years 2003 and 2007, the Czech Republic had the Ministry of Informatics of the Czech Republic that was more or less responsible for the cybersecurity agenda. After the dissolution of this Ministry, the agenda was not completely transmitted to another institution, and it caused a period of disputes that had an impact on the situation in the respective area for many years.

In addition, the Ministry of Informatics of the Czech Republic entrusted itself with important tasks specified in a document called *Action Plan Implementing the National Security Information Security Strategy of the Czech Republic*.[3] [52]

Pilot Teams and its Competitors

In 2006 and 2007, the process of building the National CERT/CSIRT team continued through the Consortium, which won the tender of the Security Research Project of the Ministry of the Interior of the Czech Republic for the period 2007–2010 (project called *Cyber Threats in the Security Interests of the Czech Republic*).[4] [48]

The consortium also included the "academic" CESNET–CERTS team, the first domestic CERT/CSIRT team with relevant practical experience, already connected to the relevant transnational platforms. The process of building a *coordinating model workplace-team of CERT/CSIRT-type* (CSIRT.CZ) within the academic network CESNET started in the mid-2007. Its pilot operation was launched on 3rd April 2008. The team has been continuously organizing methodical education (with the participation of a number of private entities, representatives of the Security Information Service, the Police of the Czech Republic and the National Security Authority). During its existence, CSIRT.CZ has gained a reputation at home and abroad, but its formal international accreditation was blocked due to the uncertainty about its future after the end of the project.

A certain blind alley in this regard was the parallel activity of the private firm Relsie, which concluded in a Memorandum of Understanding with the Ministry of the Interior of the Czech Republic in *February 2007* (describing the vision to build a CERT/CSIRT facility, called CERT.ORG). But this company was, in fact, an unknown player for foreign partners, so it cannot reach its goals. [46]

For foreign counterparts, the situation in the Czech Republic became even more unclear. Two competing "CERT/CSIRT" teams were confusing for them.

---

[3] Task: *"To implement the Early Warning and Response System. Establish a National Center for Management, Monitoring and Analysis of the Security Environment of the Information and Communication Systems of the Czech Republic. Establish a CERT-type team with a cross-national competence."* Responsible authority: originally the Ministry of Informatics of the Czech Republic, later the Ministry of the Interior of the Czech Republic, in cooperation with the Security Information Service of the Czech Republic. Deadline: no later than in 2008. Task: *"To establish monitoring of effectiveness of proposed countermeasures in the CERT team."* Responsible authority: Ministry of the Interior of the Czech Republic. Deadline: no later than in 2008.

[4] The Consortium was formed by the individual faculties of the Charles University, Prague, the Czech Technical University, CESNET (Internet Service Provider for numerous academic institutions) and NESS Czech Company.

In *September 2008*, the security team of NIC.CZ[5] (CZ.NIC-CSIRT) was created. The effectiveness of this team has been so far the most advanced of all teams of this type in the Czech Republic. A number of incidents was vigorously resolved, not only "archived" through this team.

Despite all partial shifts, *political consensus* on practical steps towards building a national CERT/CSIRT-type team *had not been achieved since 2007 until the beginning of 2010*. At a later stage, the responsibilities (and costs) associated with this step were refused by the Ministry of the Interior of the Czech Republic, the Ministry of Defense of the Czech Republic as well as the National Security Authority of the Czech Republic. It is no wonder that these delays caused embarrassment not only in the domestic expert community. [14] [32]

Overcoming the Competence Vacuum

The situation (at least for some time) started to clarify after the introduction of the "caretaker government" in the Czech Republic (June 2009 to July 2010), especially due the Resolution of the National Security Council of *5th January 2010* No. 4, *On the Analysis of the Current Level of Cyber Security of the Czech Republic*. This document imposed the main competences and responsibilities for the next steps regarding the cybersecurity agenda unambiguously on the Ministry of the Interior of the Czech Republic. [50]

Following the aforementioned Resolution of the National Security Council, a new Cyber Security Department was established within the Ministry of the Interior of the Czech Republic at the beginning of 2010. [35] [44] [47]

One of its first registrable activities was the participation at the session of the CSIRT.CZ Working Group on *25th March 2010* (interconnecting representatives of major internet service providers, content providers, state security forces, Czech Telecommunication Office, CZ.NIC, NIX.CZ[6] and the academic sector). [26] [47]

But no tangible steps were then taken by the state (the Ministry of the Interior of the Czech Republic), and the initiative was taken over by the private sector, especially by the administrator of the Czech national domain, CZ.NIC. At its own expenses and responsibility, it created a CERT/CSIRT-type team that used the company's background and served the widest public. [34] This situation continued until 16th December 2010, when a Memorandum on Computer Security Incident Response Team of the Czech Republic was signed between the Ministry of the Interior of the Czech Republic and the CZ.NIC,

[5] CZ.NIC is an association of legal persons founded in 1998 by the leading Internet service providers in the Czech Republic. The main activity of the association is the operation of the domain name register .cz. At present, the association is improving the domain management system, supporting new technologies beneficial to the Internet infrastructure in the Czech Republic. CZ.NIC is a member of international organizations that associate with similar organizations around the world (CENTR, ccNSO and others) and also a member of EURid, a European .eu domain. [43]

[6] NIX.CZ (Neutral Internet Exchange) is a platform that interconnects Internet Service Providers in the Czech Republic to interconnect their Internet networks. This association is formed by telecommunication companies operating in the Czech Republic because they have a common interest in ensuring that their computer networks are mutually interconnected and their customers can quickly communicate via the Internet within the Czech Republic. Members of the platform contribute together to the technologies that can improve the exchange efficiency and securely. [41]

according to which the CZ.NIC temporarily (from the 1st of January 2011) took the agenda of the national security team CSIRT.CZ. [10]

The Memorandum also stated that the Ministry of the Interior of the Czech Republic addressed the status of CERT/CSIRT teams within the state administration and sought to support the inclusion of CSIRT.CZ in international structures, in particular by confirming the status of CSIRT.CZ as a "National CSIRT Team". Furthermore, it coordinates the activities of CSIRT.CZ, evaluates information received from CSIRT.CZ in case CSIRT.CZ suspects that the incident could have an impact on the state or state administration systems. The Ministry of the Interior of the Czech Republic also had the right to request an audit of the performance of CSIRT.CZ activities. [34]

As it was already stated above, CSIRT.CZ was a research project carried out by CESNET that ended on 31st December 2010. As of *1st January 2011*, under the agreement of the Cyber Security Department of the Ministry of the Interior of the Czech Republic, the CESNET and CZ.NIC, took the responsibility for the relevant equipment to be able to maintain the continuity of CSIRT.CZ. [34]

CSIRT.CZ, perceived as a "national CSIRT team" since its creation, became in 2010 a co-worker of the European Union Agency for Information Technology (Point of Contact for the Czech Republic). [54]

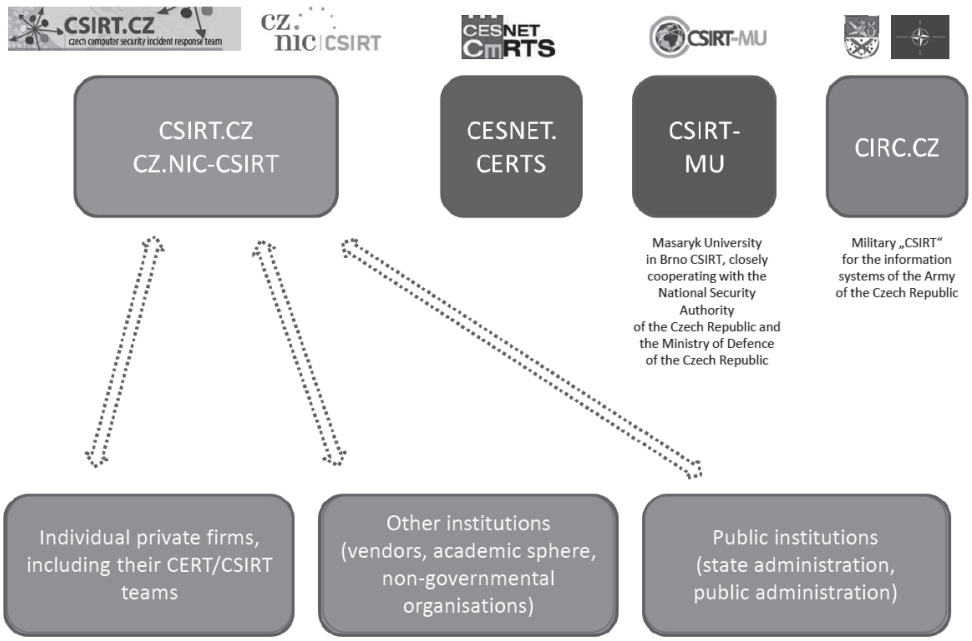


Figure 1. *Perspectives regarding the various stages of possible development of umbrella CERT/CSIRT Teams in the Czech Republic in the years 2010–2011.*
[Edited by the author.]

In connection with the aforementioned facts, the National Security Council of the Czech Republic discussed on *28th February 2011* the document describing the current situation

regarding cyber security issues in the Czech Republic. Due to the importance of the agenda, the Cyber Security Strategy (elaborated by the Ministry of the Interior of the Czech Republic) was submitted to the National Security Council and then to the Government by *30th June 2011.*

The perspectives regarding the various stages of possible development, as expected in the beginning of 2011, are described by the following visualizations (several CERT/CSIRT-type teams, two of them open to the general public questions and proposals). [16]

Transfer of the Agenda to the National Security Authority of the Czech Republic

The "coordination role" of the Ministry of the Interior of the Czech Republic did not last long. On the basis of the Resolution of the Government of *19th October 2011* No. 781, on the Umbrella "National Authority" Responsible for the Area of Information Security Regarding the Public Sector of the Czech Republic, the relevant competence was transferred to the National Security Authority of the Czech Republic. The new administrator was already, whether alone or in co-operation with other stakeholders, very active in many relevant areas. [22]

The Government approved of the establishment of the National Cyber Security Center as a part of the National Security Authority of the Czech Republic. [30]

At the same time, the Government of the Czech Republic set up the Cyber Security Council as a part of the National Security Council and the National Cyber Security Center as a part of the National Security Authority of the Czech Republic. At the same time, the Government imposed a number of specific tasks on the National Security Authority of the Czech Republic. The relevant Cyber Security Strategy for the years *2012 to 2015* was already elaborated also under the coordination of the National Security Authority of the Czech Republic. [49] [36] [37] [38] [49] [58]

In January 2012, CSIRT.CZ reviewed the period of one year of its operation with the following conclusion: The CSIRT.CZ team officially represented the Czech Republic in the world (in the relevant international forums and is also the first contact point for foreign counterparts). In July 2011 it organized the pilot training seminar *The World of Internet and Domains*, intended for employees of the state administration and members of the security forces, especially the Police of the Czech Republic. The team was cooperating with the Internet Service Providers in the Czech Republic. Special attention was paid to the practical issues that should help (especially) the police investigators to orient themselves in the issue of basic forms of cybercrime and to learn to address directly the specific subjects that can support their work. Participants of the pilot course were also the intelligence operations specialists, judges etc. In 2011, CSIRT.CZ was invited to the Law Enforcement Authorities Expert Working Group of the European Union Agency for Information Technology. The work of this expert group resulted in a document, mapping the experience raised from the interconnection of law enforcement and cybersecurity experts, and suggesting a set of recommendations. [6] [12] [20]

This cooperation did not end in 2012. Due to the fact that the National Security Authority of the Czech Republic was not able to launch its Gov-CERT, that was already "under construction" in the former premises of the Ministry of Defense in Brno), the decision was

made to sign another Memorandum, moving this "turning point" until 2015. Until then, the national cyberspace will be dominated by the CZ.NIC. [9] [57]

"The current solution to cyberspace protection is unsatisfactory. CSIRT.CZ *of the CZ. NIC is good and professional, but this fact cannot substitute the absence of the Gov-CERT team, which must be a part of the security system and the protection of cyberspace … The* members of the national CSIRT […] has no powers or responsibilities that are key to handling security threats. *CSIRT has only a consultative role […] Four half-time CZ.NIC specialists are responsible for the security of the Czech cyberspace, but they do not have any competencies as well as the right to handle classified information […] With time, they can be supported and even replaced by the employees of the Gov-CERT in Brno, but without any support in the legislation, it still will be a group of experts with no power to enforce their will."* [27]

Proposal of the Modified Institutional Framework

The proposal, with one of the first drafts of the Act on Cyber Security (February 2012), included the framework for the provision of information security functions in the Czech Republic. It was envisaged to create two umbrella CERT/CSIRT teams in the Czech Republic.

1. The *"National" CERT* will be built on the fundament of the CZ.NIC (CSIRT.CZ), with the use of the experience of the model workplace-team operated by CESNET (CSIRT.CZ), according to the research project of the Ministry of the Interior of the Czech Republic. The "National" CERT will establish or deepen existing links with and among similar teams within the Network Monitoring Cluster and, in the first phase, perhaps, also regarding the public sector. CSIRT.CZ will be involved in resolving cyber-security incidents in networks operated in the Czech Republic. CSIRT.CZ will also provide co-ordination assistance, but not physical support, to resolve individual incidents (but this assistance will not be provided directly to end users). CSIRT.CZ will collect and evaluate data on reported incidents and report respective incidents to those responsible for operating the individual network(s) that is (are) the source(s) of the incident, in accordance with the severity of the incident. CSIRT.CZ will fulfil the role of so-called National Point of Contact (PoC), as well as the center of education and dissemination of cyber security related education. It will also assist to establish the CERT/CSIRT teams in networks operated in the Czech Republic, including help regarding the establishing of co-operation connections with foreign/global security platforms. [34]
2. At the same time (or later) the construction of the *"Government" CERT* team (GovCERT.CZ) would be launched. This team would be primarily designed to monitor government networks and (public) critical information infrastructure, or to coordinate and methodologically run other sub-centers of this type that operate or will operate within specific public institutions.[7]

[7] The National Cyber Security Center will pursue efforts to protect networks primarily within public institutions, such as ministries, energy companies, hospitals or the Czech National Bank. The National Center for Cyber Security (in its embryonic condition) is directly subordinated to the Director of the Office.

In connection with the construction of this workplace-team, it will be especially necessary[8] to interconnect both platforms, as well as ensure their connection to the "military" team of a similar type (CIRC.CZ).

Both teams are to be understood first and foremost as partners who "lighten each other's burden". However, GovCERT would have a veto right in a number of questions, but at the same time it does not possess such technical and human resources (it is reportedly a problem to fill the relevant positions in public institutions), such as the National CERT that was built mainly on the basis of CZ.NIC.

The whole process is planned to go from "more limited" to "more ambitious" goals.

The relevant experts saw this proposal as a shift in the positive direction (compared with many years of inactivity in the past).[9] The limits related to the involved bodies (important and not-important public administration information systems, and "selected" service providers and network operators) were not entirely clear.

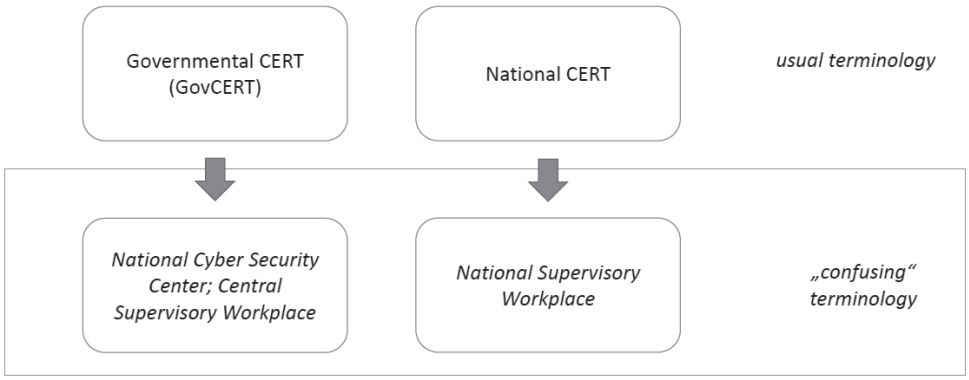


Figure 2. *Mutual ties and connection among individual CERT/CSIRT-like platforms in the Czech Republic, proposal from February 2012.* [Edited by the author.]

This vision has been widely commented by the domestic expert community as somewhat unusual: "In the world of information security, there are certain common terms (see, for example, outputs of the European Union Agency for Information Technology) […] according to which the 'National CERT or CSIRT' is a body, which stands on the top of the whole hierarchy in a particular country, and coordinates the other CERTs/CSIRTs. It is also the primary contact point for communication with CERTs/CSIRTs in other countries, and is also the country's principal representative in cyber-security related international organizations. In addition to 'national' CERTs or CSIRTs, there are still 'governmental' CERT/CSIRT teams that take care of those systems that are serving to the public administration bodies (state and local government) […] Typically, they have somewhat

[8] Due to the fact that there are several platforms in the Czech Republic already bearing the name CERT or CSIRT, it was decided that this "governmental" concept would differentiate (as in other countries) by the prefix "Gov" (derived from the word "government" or "governmental"). In addition, this term indicates the "superiority" of such a platform over the other CERTs (CSIRTs) existing within the state.

[9] At the same time, it is said that this concept could be improved and reshaped according to developments in countries that are more developed in the field of information security (for example, Germany). [3] [5]

different powers (and modes of operation) than the national teams. […] In the Czech Republic, in the proposal of the Cyber Security Act, what is usually 'governmental', on the contrary, refers to 'national' (and what is usually 'national' is referred to as 'central') […] in such a way that the authors of the proposal do not use the 'settled' terminology. […] Let's note one more thing: the 'National Supervisory Workplace' ('governmental' CERT) will be 'plugged in' inside another workplace called National Cyber Security Center (the only contact point for foreign partners). And this National Cyber Security Center is also 'plugged in' the National Security Authority of the Czech Republic as its organizational component." [45]

This begs for a rhetorical question: Will our foreign counterparts understand such an unconventional structure, if a serious incident occurs?

The management of the CSIRT.CZ and NIC.CZ were aware of this situation and tried to "calm down" similar negative or hesitating comments: "Teams designated as governmental and national have a very specific role in the CERT/CSIRT security infrastructure. Teams referred to as government are usually intended to oversee the networks of state administration, self-government and so-called critical infrastructure of the country. National teams usually fulfil the role of the National Point of Contact, sharing information with other teams abroad, and with the entities and organizations of their country […] A similar model is currently being used in the Czech Republic: The National CSIRT of the Czech Republic, fulfils the role of the governmental team, at least temporarily, according to the Memorandum signed in 2012." [6]

Gradual Stabilization, the Way to the National Cyber and Information Security Agency (Years 2012 to 2017)

On *19th December 2014* the regulations implementing Act No. 181/2014 on Cyber Security were published in the Collection of Acts: [51]

- Regulation No. 316/2014 Coll. on Security Measures, Cyber Security Incidents and Reactive Measures.
- Regulation No. 317/2014 Coll. on the Determination of Important Information Systems and their Determination Criteria.
- Decision of the Government No. 315/2014 Coll. which amends the Decision of the Government No. 432/2010 Coll. on the Criteria for the Determination of the Elements of the Critical Infrastructure.

Act No. 181/2014 Coll. on Cyber Security and on the Amendments of the Related Acts (Cyber Security Law) after many and many discussions and changes, came into force on *1st January 2015*. The Act on Cyber Security is "based" on two principles: the first principle is to minimize the interference with the rights of private persons; the second is the principle of the individual responsibility for the security of the respective information systems. The Act came into force together with implementing regulations. [1] [2]

August 2017: The National Cyber and Information Security Agency (NCISA) became the central body of state administration for cyber security, including the protection of classified information in the area of information and communication systems and cryptographic protection. It is also in charge of the public regulated service of the Galileo satellite system.

It was created on the basis of Act No. 205/2017 Coll., amending Act No. 181/2014 Coll., on the Cyber Security and on the Amendments of the Related Acts (Cyber Security Act).

National Cyber and Information Security Agency with its 120 employees took over the agenda of the National Security Authority of the Czech Republic that previously fell under the responsibility of the National Cyber Security Center that had been operating since 2011. The National Cyber and Information Security Agency's headquarter in Brno is in offices that previously served the National Cyber Security Center.

The situation in the Czech Republic grew closer to what is considered a standard in advanced European countries.

Main areas of the activity of the *National Cyber and Information Security Agency* are as follows: [39]

- operating of the Government CERT (GovCERT.CZ);
- cooperation with other domestic CERT/CSIRT teams;
- cooperation with international CERT/CSIRT teams;
- drafting of security standards for information system regarding critical information infrastructure and "Important Information Systems" (defined by law);
- support of education in the field of cyber security;
- research and development in the area of cyber security;
- protection of classified information in the field of information and communication systems and cryptographic protection.

The National Cyber and Information Security Agency operates the National Public Regulated Service Center (NCPRS), which fulfils the task of the so-called Competent Public Regulated Service Authority; it is one of the services provided by the European satellite system Galileo.

A new building in the barrack premises in Brno is planned to be built that will serve almost 400 staff members. The new office should be opened in 2023.

Conclusion

The Czech Republic is a relatively highly "internetised" country, where projects such as Data Boxes (state-guaranteed e-mail like communication system) and CzechPoint (offices for dissemination of state-guaranteed data and confirmed documents) are strongly promoted. But the security aspect of the whole issue remained for a long time behind the "edge of interest", and the whole country was in this regard understood by its foreign counterparts as an "untrusted partner".

Public sector institutions within the Czech Republic, for a long time, have only been looking after their own "cyberspace-sections" and the nationwide structure remained rather in the hands of active private sector players.

Only after 2011 the country invested more in a coordinated way of protecting its information infrastructure.

Table 1. *Weak points that took place in the history of the Czech Republic's cybersecurity related effort.* [Edited by the author.]

Weak points that took place in the history of the Czech Republic's effort	Proposals regarding cybersecurity issues
A protracted long-standing negative competence dispute where no resort or authority wanted to accept new costly and complicated agenda.	Resolute political (governmental) decision in this regard.
Only formal and rhetorical "fulfilment" of necessary tasks and demands of the transnational and foreign counterparts.	Efforts realistically meet individual requirements, being aware of their importance.
Non-standard terminology, problematic for both home and foreign/transnational counterparts.	Use of standard terminology as much as possible.
"Waiting tactics" regarding the relevant private actors.	Sincere public-private cooperation, with clearly defined rules.
When co-operation with private players started, its results were bodies without formal competencies.	Delegating unambiguously specified competencies to renowned and trusted private players.
Rigidity in relation to the possible employment of top-level (and adequately paid) experts in the state administration.	Accepting the need to remunerate top experts adequately.
Total underestimation and under-dimensioning of the topic.	Accepting the theme of cyber security as today's major priority, the failure of which would lead to serious and quantifiable negative effects regarding the state and society.

Instead of Conclusion: Recommendations Related to the Issue of Cybersecurity

As part of the "umbrella" cybersecurity institutions in the Czech Republic, it is necessary to address specific aspects of collection and distribution of information about threats from/to participating centers, as well as creation of a register of incidents, threats and vulnerabilities accessible by relevant entities to enhance the active protection of the cyberspace of the Czech Republic. [17] [18] [28]

It is also necessary to clarify the relevant communication and competence flows set within the Czech Republic as well as regarding the communication abroad. [56]

In addition to building a hierarchy at the national level, a clear hierarchy of responsibility for information security within the Police of the Czech Republic should be built. The qualified interconnection of the professional and strong team with sufficient equipment and staff cannot be perceived only in terms of the structure of the Police, but it is necessary to point out the existing need for co-operation with other bodies of state administration and commercial sphere.

Outside the Police of the Czech Republic, it is necessary to establish the links of the direct cooperation with the intelligence services, the critical infrastructure elements and the IT security specialist in the private sphere.

In all concerned public institutions, unambiguous contact points should be created regarding the topic of information security (which should remain stable regardless any personnel and organisational turbulence). Stakeholders from each institution need to exchange relevant experience on a regular basis (or even daily), or even create a joint "knowledge fund".

References

[1] *On Cyber Security and Change of Related Acts (Act on Cyber Security).* https://nukib.cz/download/legislation/container-nodeid-1122/actoncybersecuritypopsp.pdf (Downloaded: 27.06.2018)

[2] *Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020.* Praha: National Cyber and Information Security Agency, 2015. www.govcert.cz/download/gov-cert/container-nodeid-578/ap-cs-2015-2020-en.pdf (Downloaded: 27.06.2018)

[3] *Bundesamt für Sicherheit in der Informationstechnik*. www.bsi.bund.de (Downloaded: 20.06.2018)

[4] *Bundesamt für Sicherheit in der Informationstechnik.* www.bsi.bund.de/EN/Home/home_node.html (Downloaded: 20.06.2018)

[5] *Bundesamt für Sicherheit in der Informationstechnik.* www.buerger-cert.de/ (Downloaded: 20.06.2018)

[6] *CSIRT.CZ a jeho první rok fungování v roli Národního CSIRT České republiky.* 12. 1. 2012. http://csirt.cz/page/992/csirt.cz--a--jeho-prvni-rok-fungovani-v-roli-narodniho-csirt-ceske-republiky/ (Downloaded: 20.06.2018)

[7] *CSIRTs by Country – Interactive Map*. Attiki: European Union Agency for Network and Information Security, s.d. www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map (Downloaded: 24.06.2018)

[8] *CSIRTs in Europe.* Attiki: European Union Agency for Network and Information Security, s.d. www.enisa.europa.eu/topics/csirts-in-europe (Downloaded: 24.06.2018)

[9] *CZ.NIC a Národní bezepčnostní úřad podepsali nové memorandum o spolupráci.* 19.12.2012. www.nic.cz/page/1308/cz.nic-a-nbu-podepsali-nove-memorandum-o-spolupraci/ (Downloaded: 20.06.2018)

[10] *CZ.NIC ohlídá kybernetickou bezpečnost České republiky.* 16.12.2010. www.nic.cz/page/830/cz.nic-will-watch-over-cybernetic-security-of-the-czech-republic/ (Downloaded: 20.06.2018)

[11] CZ.NIC převezme systém řešení bezpečnostních incidentů CSIRT. *České noviny* (online), 16.12.2010. www.monitoruji.cz/it-pocitace/349997/cz-nic-prevezme-system-reseni-bezpecnostnich-incidentu-csirt (Downloaded: 20.06.2018)

[12] Česká kybernetická jednotka CSIRT bojuje proti Anonymous. *Živě.cz* (online), 02.02.2012. www.monitoruji.cz/it-pocitace/565556/ceska-kyberneticka-jednotka-csirt-bojuje-proti-anonymous (Downloaded: 20.06.2018)

[13] Českou republiku střeží před kyberútokem čtyři lidé na půl úvazku. *Aktuálně.cz* (online), 21.12.2011. www.monitoruji.cz/it-pocitace/523094/cr-strezi-pred-kyberutokem-ctyri-lide-na-pul-uvazku (Downloaded: 20.06.2018)

[14] DOČEKAL, D.: CSIRT.cz přichází. Kyberzločincům navzdory. *Lupa.cz* (online), 04.04.2008. www.lupa.cz/clanky/csirt-cz-prichazi-kyberzlocincum-navzdory/ (Downloaded: 20.06.2018)

[15] *Forum of Incident Response and Security Teams.* www.first.org/ (Downloaded: 20.06.2018)

[16] HNÍK, V., KRULÍK, O.: *Okolnosti, související s budováním pracoviště typu CERT v České republice.* (Unpublished document for the purposes of the Cybersecurity Department of

the Ministry of the Interior of the Czech Republic). Prague: Cybersecurity Department of the Ministry of the Interior of the Czech Republic, 2010.

[17] HNÍK, V., KRULÍK, O., POŽÁR, J.: Česká republika na rozcestí (I). *Security World*, 1 (2011), 44–47.

[18] HNÍK, V., KRULÍK, O., POŽÁR, J. Česká republika na rozcestí (II). *Security World*, 2 (2011), 44–47.

[19] HNÍK, V., KRULÍK, O., POŽÁR, J.: Zajišťování informační bezpečnosti na Islandu jako inspirace pro Českou republiku. In. JIRÁSEK, P. (ed.): *Kybernetické útoky na informační systémy.* Prague: AFCEA, 2012. www.cybersecurity.cz/data/hnik.pdf (Downloaded: 20.06.2018)

[20] HOŠT, O.: Trendy v bezpečnosti 2012: soukromí, Facebook, mobilní platby a stará dobrá havěť. *Lupa.cz* (online), 02.03.2012. www.lupa.cz/clanky/trendy-v-bezpecnosti-2012-soukromi-facebook-mobilni-platby-a-stara-dobra-havet/ (Downloaded: 20.06.2018)

[21] *Index Inventory. European Union Agency for Network and Information Security.* Attiki: European Union Agency for Network and Information Security, s.d. www.enisa.europa.eu/cert_yinventory/index_inventory.htm (Downloaded: 24.06.2018)

[22] *Informace k usnesení vlády České republiky č. 781 ze dne 19. října 2011*. Praha: Národní bezpečnostní úřad České republiky, 2011. www.nbu.cz/cs/aktuality/994-informace-k-usneseni-vlady-ceske-republiky-ze-dne-19-rijna-2011-c-781/ (Downloaded: 20.06.2018)

[23] Jak CSIRT.CZ došel k akreditaci. *Lupa.cz* (online), 01.11.2011. www.monitoruji.cz/it-pocitace/510651/jak-csirt-cz-dosel-k-akreditaci (Downloaded: 20.06.2018)

[24] January 2008 FIRST Technical Colloquium. *Forum of Incident Response and Security Teams.* Prague, 27–31 January, 2008. www.first.org/events/colloquia/jan2008 (Downloaded: 20.06.2018)

[25] JIROVSKÝ, V., HNÍK, V., KRULÍK, O.: Základní definice, vztahující se k tématu kybernetické bezpečnosti. *Security Magazine*, 03–04 (2007), 46–49.

[26] KHUDHUR, P.: Ministerstvo vnitra chce zřídit CSIRT, vládní pracoviště pro bezpečnost IT. *Security World* (online), 21.05.2007. http://securityworld.cz/aktuality/ministerstvo-vnitra-chce-zridit-csirt-vladni-pracoviste-pro-bezpecnost-it-2498 (Downloaded: 20.06.2018)

[27] KOVALÍK, J.: Česko se začne před kyberútoky bránit až v roce 2015. *DataRama* (online), 06.12.2011. http://datarama.aktualne.centrum.cz/clanek.phtml?id=723306 (Downloaded: 20.06.2018)

[28] KRULÍK, O.: Návrhy a doporučení pro oblast informační bezpečnosti. *Bezpečnostní situace v České republice*. (CD-ROM) Praha: Ministerstvo vnitra České republiky, 2012. (ISBN 978-80-260-3275-5)

[29] KRULÍK, O, HNÍK, V.: Zahraniční inspirace, související s tématem kybernetických hrozeb. *Policista*, 10 (2007), annex, I–XII.

[30] *Legislation.* Praha: National Cyber and Information Security Agency, s.d. https://nukib.cz/en/legislation/legislation/ (Downloaded: 27.06.2018)

[31] MACÍCH, J.: CZ.NIC od ledna přebírá agendu CSIRT.CZ. *Lupa* (online), 17.12.2010. www.lupa.cz/zpravicky/cz-nic-od-ledna-prebira-agendu-csirt-cz/ (Downloaded: 20.06.2018)

[32] MALÝ, O.: Stát chce bojovat s kyberzločinem. *Lidové noviny* (online), 10.02.2010. www.cesnet.cz/sdruzeni/napsali-o-nas/2010/02/20100210_Lidove_noviny.html (Downloaded: 20.06.2018)

[33] *Members around the World.* Forum of Incident Response and Security Teams (FIRST), s.d. www.first.org/members/map (Downloaded: 20.06.2018)
[34] Memorandum on Computer Security Incident Response Team České republiky. *CSIRT.CZ* (online), 27.05.2011. www.nic.cz/files/nic/doc/Memorandum_CSIRT.CZ.pdf (Downloaded: 20.06.2018)
[35] Ministerstvo vnitra představí návrh řešení kybernetické bezpečnosti České republiky. *Český rozhlas* (online), 15.03.2010. www.rozhlas.cz/zpravy/spolecnost/_zprava/706944 (Downloaded: 20.06.2018)
[36] *Národní bezpečnostní úřad České republiky.* www.nbu.cz/cs/ (Downloaded: 20.06.2018)
[37] *Národní centrum kybernetické bezpečnosti se představuje a nabízí zajímavé pracovní příležitosti*. Praha: České vysoké učení technické, 2011. http://oi.fel.cvut.cz/en/node/621 (Downloaded: 20.06.2018)
[38] *Národní centrum kybernetické bezpečnosti*. www.govcert.cz/cs/ (Downloaded: 20.06.2015)
[39] *National Cyber and Information Security Agency.* https://nukib.cz/en/ (Downloaded: 27.06.2018)
[40] NĚMEČKOVÁ, K., KRULÍK, O., POŽÁR, J., HNÍK, V.: Vývoj, související s budováním pracovišť typu CSIRT/CERT v České republice. *Ochrana & Bezpečnost*, 3 (2012), 1–42. http://ochab.ezin.cz/O-a-B_2012_C/2012_C_09_nemeckova.pdf (Downloaded: 20.06.2018)
[41] *Neutral Internet eXchange.* www.nix.cz/cs (Downloaded: 20.06.2018)
[42] *New Guide on Cyber Security Incident Management to Support the Fight against Cyber Attacks.* Attaki: European Union Agency for Network and Information Security, 2011. www.enisa.europa.eu/news/enisa-news/new-guide-on-cyber-security-incident-management-to-support-the-fight-against-cyber-attacks (Downloaded: 20.06.2018)
[43] O sdružení. *CZ.NIC* (online) www.nic.cz/page/351/ (Downloaded: 20.06.2018)
[44] *Odbor kybernetické bezpečnosti.* Praha: Ministerstvo vnitra České republiky, s.d. www.mvcr.cz/clanek/odbor-kyberneticke-bezpecnosti.aspx (Downloaded: 20.06.2018)
[45] PETERKA, J.: Jaký bude zákon o kybernetické bezpečnosti. *Lupa.cz* (online), 22.02.2012. www.lupa.cz/clanky/jaky-bude-zakon-o-kyberneticke-bezpecnosti/ (Downloaded: 20.06.2018)
[46] Pilotní kurz CERT – TERENA. *relsie.cz* (onlie), 2010. www.relsie.cz/rj/pilotni-kurz-cert-terena (Downloaded: 10.02.2013)
[47] *Pracovní skupina CSIRT.CZ o vládním bezpečnostním pracovišti CSIRT.* CESNET, 30.02.2010. www.cesnet.cz/doc/tisk/2010/tz100330.html (Downloaded: 20.06.2018)
[48] *Problematika kybernetických hrozeb.* Praha: Ministerstvo vnitra České republiky, 2009. www.mvcr.cz/clanek/vysledky-projektu.aspx (Downloaded: 20.06.2018)
[49] *Rada na svém zasedání dne 23. XI. 2011 mimo jiné přijala usnesení o harmonogramu budování Národního centra kybernetické bezpečnosti.* Brno: Rada pro kybernetickou bezpečnost a Národní centrum kybernetické bezpečnosti, 2011. www.govcert.cz/cs/rkb/rada-pro-kybernetickou-bezpecnost/ (Downloaded: 20.06.2018)
[50] *Report from the National Security Council Session of 5th January 2010 (Záznam ze schůze Bezpečnostní rady státu ze dne 5. ledna 2020).* Praha: Government of the Czech Republic, 2010. www.vlada.cz/cz/ppov/brs/cinnost/zaznamy-z-jednani/zaznam-ze-schuze-brs-konane-dne-5--ledna-2010-66950/ (Downloaded: 20.06.2018)

[51] ROHEL, V.: *Kybernetická bezpečnost z pohledu státu*. Brno: Národní centrum kybernetické bezpečnosti, 2014. https://konferencesecurity.cz/images/archiv/2014/for-download/Security-2014---M4-2---Rohel.pdf (Downloaded: 27.06.2018)

[52] SVOBODOVÁ, M.: Realizace Národní strategie informační bezpečnosti České republiky. *ISSS Conference 2006.* Hradec Králové: Ministerstvo informatiky České republiky. http://slideplayer.cz/slide/3295272/ (Downloaded: 25.06.2018)

[53] *TF-CSIRT Membership*. Amsterdam: Trans-European Research and Education Networking Association, 2012. www.terena.org/activities/tf-csirt/membership.html (Downloaded: 20.06.2018)

[54] *The Czech Republic*. Attiki: European Union Agency for Information Security. www.enisa.europa.eu/activities/cert/security-month/pilots/czech-republic (Downloaded: 20.06.2018)

[55] *TRANSITS: CSIRT Training.* Amsterdam: Trans-European Research and Education Networking Association, s.d. www.terena.org/activities/transits/ (Downloaded: 20.06.2018)

[56] *Trusted Introducer for CSIRTs in Europe*. www.trusted-introducer.org/ (Downloaded: 20.06.2018)

[57] *Vládní CERT.* Praha: Národní bezpečnostní úřad České republiky, s.d. www.govcert.cz/cs/govcert/ (Downloaded: 20.06.2015)

[58] *Zprávy Ministerstva vnitra o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky.* (Statistiky kriminality – dokumenty) Praha: Ministerstvo vnitra České republiky, s.d. www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx (Downloaded: 20.06.2018)

AARMS Vol. 17, No. 3 (2018) 131–148.

Interoperability Services Supporting Information Exchange Between Cybersecurity Organisations[1]

Sándor MUNK[2]

The security of cyberspace can be ensured by a broad cooperation of different organizations, actors. This cooperation cannot be achieved without interoperable information exchange between cybersecurity actors, organisations, and their IT systems. Interoperable information exchange can be realized using own resources, or using services provided by third parties. IT interoperability service can be defined as a service by which a service provider supports interoperable data exchange between IT systems of service consumers and cooperating actors. This publication provides different categorizations of interoperability services, discusses their benefits, and the necessary user tasks. It determines the types of interoperability service providers and their necessary capabilities. Finally, it defines the special requirements of cybersecurity information exchange and presents the main types of required services.

Keywords: *interoperability, cybersecurity organisations, interoperable information exchange, IT services*

Introduction

Today's social, economic and everyday activities are increasingly dependent on the services provided by globally interconnected, decentralized IT systems and networks that make up the cyberspace. This dependency also means increasing vulnerability and risks. A secure cyberspace, cybersecurity requires a broad range of actors and extensive cooperation, collaboration. It is also clear that successful and effective cooperation is not possible without a similar level of information exchange.

Information exchange between different actors may have and in practice almost always has interoperability problems that require appropriate solutions. This is also the case for the various actors of cybersecurity scene, which include event management centres, operations centres, organisations providing cybersecurity information and IT developers, manufacturers.

Solutions for ensuring and maintaining interoperable exchange of information between IT systems of the actors involved can be implemented by the actors themselves, or they can use services provided by third parties. With the emergence and spread of cloud-based technology, the role of services is gradually increasing. This makes it necessary to examine

[1] The work was created in commission of the National University of Public Service under the priority project PACSDOP-2.1.2-CCHOP-15-2016-00001 entitled "Public Service Development Establishing Good Governance" in the Ludovika Cybersecurity Workshop.

[2] DSc, Professor, National University of Public Service, Faculty of Military Sciences and Officer Training, Institute of Military Maintenance; e-mail: munk.sandor@uni-nke.hu

the possibilities of services supporting interoperable information exchange in general, and in particular for cybersecurity information exchange.

The purpose of this research paper is to outline the basics and the framework of using IT interoperability services to ensure and maintain interoperability during exchange of information between cybersecurity organisations. For this reason it:

- discusses the concept and elaborates the definition of IT interoperability services supporting information exchange;
- suggests classification criteria and classifies IT interoperability services supporting information exchange;
- determines the benefits of using such services and the tasks to be performed;
- determines the types of service providers of such services and their necessary capabilities;
- summarizes the interoperability problems and solutions of the exchange of cybersecurity information;
- identifies possible types and content of cybersecurity interoperability services.

Basics of Interoperability Services

To examine the interoperability services that support the exchange of information between cybersecurity organizations, we first need to summarize the basics of interoperability services. In today's literature, though we may encounter the term, there is no mature definition, or practically, there is not even a definition of the concept of interoperability services. For this reason, I will start from the components of the term, so I will simply consider it a service that supports interoperability.

Interoperability itself is a widely used concept that is in many respects clearly defined, but it has a number of types modified by an adjective. In the following, I will briefly summarize the basics of information interoperability and IT interoperability, their concepts, problems, levels and solutions, largely based on my previous publications. [1] [2] [3]

I will then elaborate the definition of the information interoperability service and then the definition of IT interoperability service concepts used in this publication, and then present the most important occurrences of these terms in the literature. Next, I sum up and analyse the technical implementation forms of interoperability services. Finally, I give a more precise definition of the interoperability service.

Basics of Information Interoperability

A fundamental prerequisite of cooperation between cybersecurity organizations is the effective and efficient exchange of information that meets the information needs of the parties and which can be used in their activity. Its conditions are ensured by the interoperability between organizations and their IT systems.

Information interoperability is a type of the general concept of interoperability, related to the exchange of information between the cooperating actors. Under the concept of interoperability, in general terms, we mean a mutual capability between/among two or more

objects, necessary to ensure successful and efficient interoperation, supporting cooperation. Accordingly, information interoperability is the mutual capability of different actors (persons, organizations, groups) necessary to ensure exchange and common understanding of information needed for their successful cooperation. In case of information interoperability, information is transmitted between the actors in a meaning-preserving mode, at a necessary level for their cooperation. Since all cooperation is based on the exchange of information between participants, information interoperability is a necessary condition for any "higher level" (e.g. organizational) interoperability.

Exchange of information between actors can take place directly between people, between people and their IT systems, as well as between IT systems. In case of traditional exchange of information between people, the preservation of meaning is based on the existing knowledge, experience of previous cooperation and cognitive abilities of the peoples. Nowadays, however, there is an increasing importance of the exchange of information between the actors' IT systems without human interaction, which requires the introduction of another concept.

The *IT interoperability* is a mutual capability of IT systems, devices and applications to receive, provide, i.e. exchange data—using transformations if necessary—preserving the meaning assigned to data by their primary users to the extent necessary for their cooperation. The data itself does not have any meaning, it is essentially a fixed representation of information, to which only their producers and their users assign (intended or interpreted) meaning.

An ***information interoperability problem*** arises only if there are some differences between the cooperating parties, when heterogeneity is present. In terms of information interoperability, heterogeneity and thus interoperability problems can be divided into levels to which independent interoperability types and capabilities belong. The difficulties in the meaning-preserving information exchange by the consensus of the literature can be grouped into three levels, which are:

- the technical level of physical media used in the exchange of information;
- the syntactic level of the language, message and data formats used;
- finally, the semantic level of the content and meaning to be transmitted.

Technical level information interoperability is a set of capabilities to handle, produce, transmit, display material (physical) representations by "interoperable" devices. Nowadays, IT technology ensures the storage and exchange of practically arbitrary representations based on continuous bit streams and finite bit sequences.

Syntactic level information interoperability is a set of capabilities to manage—produce, process and present—intermediate representations in the form of data, based on material representations. These include numerical representations, string formats, character code tables, data structure representations, digital representations of textual and drawing information, and digitized formats of sampled audio, visual and other sensory information. Although the scope of possible syntactic representations is wide, in practice they are limited to a relatively small number of standard solutions.

Semantic level information interoperability is a set of capabilities that make use of the intended meaning of syntactic level representations that carry information. In case of IT systems, the proper interpretation of the received data requires additional knowledge about the meaning of that type of data. Previously, this knowledge was embedded, "hidden" in algorithms (programs). Nowadays, the amount of semantic information manageable by IT

tools about the connection between data and their meaning has been significantly expanded. This includes data about data (metadata) as well as formalized concept systems (controlled dictionaries, taxonomies, ontologies).

Elimination of interoperability problems, maintaining the necessary interoperability can be achieved by ***interoperability solutions.*** One of the interoperability solutions is standardization, reduction or elimination of heterogeneity; the other is the insertion of meaning-preserving transformations between the form used by the sending (data providing) party to the form used by the receiving (data receiving) party.

The *technical and syntactic level interoperability solutions* must ensure that the different material (physical) resources and target representations involved in the transformation carry the same syntactic representation (digital bit sequence, bit stream), and that the different data formats and structures of source and target sides be transformed to each other preserving the meaning to the necessary extent. While technical level solutions in principle can transform bit sequences and streams without loss of information, it is not true for syntactic level transformations. Some syntactic representations cannot be transformed unambiguously to each other.

The most difficult task is to develop *semantic level solutions.* The details of solutions on technical and syntactic levels are of no interest for the users, and can be replaced invisibly, not affecting their activity. By contrast, the meaning assigned to the data processed, the concepts used in the interpretation, and their relationships are closely related to the user activity. Thus, standardization is not always a solution, heterogeneity cannot be completely eliminated or it is not straightforward to eliminate.

Nowadays, practically all IT interoperability solutions are based on the use of agreed (standard) intermediary representations. In this case each actor stores the information in the form of his/her own internal representation and after transformations, it is transmitted in the form of the intermediary representation. This solution leaves the autonomy of the individual actors, does not deal with the internal representations they use, with the possible syntactic and semantic differences (possibly) existing between them and with the tasks of transformation between the internal representation and the intermediary representation. It allows new entrants to flexibly engage in the interoperable exchange of information within the scope of cooperation, without the original actors having new transformation tasks.

Concept and Interpretation of Interoperability Services

There are several possibilities for implementing information (and IT) interoperability, requiring tasks with different content and difficulty. In case of all tasks, such as the creation of the conditions for interoperability, there are two possibilities: a solution based on own resources or provided by an external service provider. In the following, I will examine the concept of information and IT interoperability service and their different interpretations.

In general terms, the ***service*** is an activity that is intangible, a service provider provides to its customers which is of value to the recipients. The use of a service may be justified by the fact that the activity provided:

- cannot be performed by the consumer in the absence of resources or capabilities;
- or the activity's own implementation is less efficient and economical.

Different types of services are distinguished: what benefits they offer to their customers (what results they bring, what their activities support and what activities they perform in place of them).

Information interoperability service is, accordingly, a service by which the service provider supports the interoperable exchange of information between the service consumer and other parties. The interoperability service may provide interoperability conditions in whole or in part. In case of traditional information exchange, an old "interoperability service" is interpreting.

Similarly, the concept of ***IT interoperability service,*** which is relevant to our subject, can be defined as a service by which the service provider supports interoperable (meaning-preserving) data exchange between the information system, tool and application of the service consumer, and the IT systems, tools and applications of other actors. The basic task of an IT interoperability service (hereafter shortly referred to as interoperability service) is the transformation between the internal representation of the information handled by the given actor and the intermediary representation, so the essence of interoperability services is the support and implementation of such transformations.

The meaning-preserving transformation of data was already mentioned in the early 1990s in the form of *mediation services,* in relation to IT systems processing data from heterogeneous sources.

Mediators provide intermediary services, linking data sources and applications, so they do not have to deal with uninteresting differences and details of their solution. Mediators provide integrated information without the need for integration of data sources. [4] Data mediation is a semantic transformation of data structures and data content that maintains semantic equivalence between different representations. [5]

The term ***interoperability service in the literature*** is described in several different forms, mostly without precise definition, most of which denote a component of a software architecture, a software service type that is a functionality provided by a software component to another software component through a defined interface.

The *Interoperability Service Utility* is one of the basic concepts of the *Cooperation and Interoperability for Networked Enterprises* (COIN) project 2008–2011 of the European Union's 7th Framework Program for Research, which is a utility-like capability, provided as a service, that establishes organizational interoperability. [6] The term has already been used in the roadmap of enterprise interoperability research project, as a layer of the open cyberspace, sitting atop of the Internet, and the Web. [7: 2]

The term appears in the title of the Content Management Interoperability Services (CMIS) standard of Organization for the Advancement of Structured Information Standards (OASIS) published in 2010 and modified in 2015. The purpose of the standard is to support information sharing between content management repositories/systems made available by different service providers, by specifying web services and interfaces. [8]

Message-oriented middleware services and *mediation services* are included in the list of services of NATO C3 Classification Taxonomy, released in 2012 and further developed in 2015, in the group of service-oriented architecture platform services of the core technical services. The platform services provide a foundation to implement web-based services in a loosely coupled environment, ensuring flexible, adaptable alignment and coordination of

services, and can be used as a capability integration platform in a heterogeneous service-provisioning ecosystem. [9: 33–34]

Technical implementation forms of interoperability services include middleware services, web services, and cloud-based services. In the literature one can find published concepts and expressions related to interoperability services, and connected to these implementation forms.

Middleware is a software product that provides its own value-added services to applications. Middleware services can complement the operating system features, support collaboration of shared software components, or provide access to various objects (e.g. data, documents, databases). Our topic is best served by the following definition: "Middleware is the software that assists an application to interact or communicate with other applications, networks, hardware, and/or operating systems." [10: 254] As it can be seen from the definition, the main but not the only function of the middleware is to ensure interoperability. In this context we can find the term "middleware services for interoperability" in the literature.

Web services in general are software services provided through the World Wide Web, between software components, in practice, in the strict sense, services that meet the W3C Web Services standard package. According to the latter, the web service is a software system designed to support interoperable machine-to-machine interaction over a network, according to certain web standards.[3] [11: 1.4] Web services are a concrete implementation of the service-oriented architecture (SOA). In this context, the term mediation web services also appear in the literature.

Cloud services are IT services that can be accessed and activated on demand via Internet from a cloud computing provider, and their costs are generally proportionate to usage. Services are built, operated and managed by the cloud service provider. In addition to conventional cloud services,[4] the concepts of "interoperability as a service" and related to this "interoperability service provider" have appeared.

Hereinafter, the interoperability service is considered only a solution in which the functionality of interoperability between IT systems, devices and applications is realized, and is provided by an interoperability service provider, independent of the consumer. Of the three technical implementation types described above, only interoperability cloud services and interoperability web services (or service-oriented architecture services) are operated by independent service providers. We do not include interoperability middleware solutions because, in these cases, the operator of the "service provider" software component is also the same as of the application using the service.

Types of Interoperability Services, their Role in the Implementation of Interoperability

Implementing functions as a service that support the interoperability of IT information systems, tools, applications and meaning-preserving exchange of information, as well as

[3] It has an interface described in Web Services Description Language (WSDL) format, interaction is done by Simple Object Access Protocol (SOAP) messages (typically conveyed using HTTP with an XML serialization).

[4] Infrastructure as a Service, Platform as a Service and Software as a Service.

the range of such services is still limited. In different application areas the basic solution for ensuring and maintaining interoperability of IT systems is the use of agreed, standardized intermediary representations. Implementing a solution based on this is a complicated task, and the cooperating systems have to carry out a significant part of that.

In order to ensure IT interoperability, the systems involved in the cooperation will implement a number of functions that could be utilized or have already been implemented in other systems. Instead of developing, maintaining or improving these features and capabilities, they can be used more efficiently and more economically as services.

In the following, to analyse the aspects of the use of interoperability functions as a service, I will present the main classification criteria, types and characteristics of these services, then examine the benefits and tasks of the services from the user point of view, as well as the types of service providers and their necessary capabilities.

Types of Interoperability Services

Interoperability services can be categorized according to different criteria. In the following, I briefly present some of the classification criteria considered relevant, the related types and their main features.

Interoperability services, according to their level may be syntactic and semantic. Among these I do not count physical level interoperability services, because these are tasks of the communication infrastructure, and today these functions are essentially ensured by IP-based data exchange available on all transmission technology.

Syntactic level interoperability services provide meaning-preserving transformations between data element representations and data structures built up from data elements. The first group includes transformations between elementary data representations corresponding different specifications. During the transformation, the content of the information carried by the data element may not be completely preserved because of the difference between source and target value sets.[5] The syntactic level data element transformations are independent of the application area, knowing the rules of the two representations they can be implemented without any application domain knowledge.

The second group is the transformations between data structure representations. These include transformations between different representations of elementary data structures and transformations between different document formats.[6] Data structure transformation interoperability services transform a source data structure representation into a target data-structure representation, provided that all data elements of the target can be generated from the data elements of the source. These services, therefore, utilize the services provided by the syntactic data element transformations.

From the point of view of syntactic data structure transformations, general purpose markup languages for semi-structured data as well as standard message formats are of paramount importance. Among the former, today the XML format is dominant, but JSON format is

[5] For example, lower numerical accuracy, smaller character count, narrower character set, or lower image colour depth.

[6] For example text, drawing, audio, video, or complex document formats.

also worth mentioning that are application area independent.[7] Standard message formats are predominantly based on these two formats and textual formats that meet simple rules.

Semantic level interoperability services provide transformations at the level of meaning of the information carried by data (independent of representation format). Both data elements and data structures contribute to the meaning, so accordingly the semantic transformations can also be split into two groups.

Among the elementary semantic meaning-preserving transformations, the conversions between different units of measurement, dates given in different calendar systems, or classifications belonging to different classification systems play a significant role. In general terms, the transformation of textual descriptions between different languages or translations of texts into foreign languages should also be considered as a semantic transformation.

As stated earlier, the data alone do not have a meaning, so the meaning-preserving transformation requires additional knowledge that can be "wired" into the transformation software component or be available in the form of semantic information related to the meaning of data. Semantic level interoperable transformations—as opposed to syntactic level transformations—can only be achieved by using specialized application domain knowledge. The rules of the transformations, the order of their implementation, or the semantic information required for this purpose must be determined by domain area specialists. If a transformation that not always, or not completely preserves meaning is acceptable, and the conditions are available, semantic level transformation can be achieved by artificial intelligence solutions based on machine learning.

Interoperability services, according to their nature can be classified into two broad categories. The first includes *services implementing transformation subfunctions*, that are used by one party involved in the exchange of information to transform one part of the information to be transmitted. In this case the parts of the transformation, not supported by services, from the own internal representation to the intermediary representation, or in the opposite direction, and the sending or receiving of the intermediary representation are the responsibility of the party concerned.

The second group is the *services implementing a complete meaning-preserving information exchange.* In this case, the service takes over the information to be transmitted from the sender, transforms it to the extent necessary and transmits it to the receiver(s). This solution is also referred to as an interoperability gateway for the analogy of the tools used for physical level information exchange, and which can also be provided as a service.[8]

An essential characteristic of interoperability services providing complete information exchange is the representations and protocols they "know", among which they provide meaning-preserving transformations. Among them, like in case of other types of gateways, it is expected that standardized representations will be used. Thus, the transformation between the individual internal representations of the actors and the standard intermediary representations remains the responsibility of the actors. The main purpose of the gateways is to interconnect different cooperation groups and the transformation between their intermediary representations.

---

[7] Extended Markup Language, JavaScript Object Notation.

[8] See for example the NATO Information Exchange Gateway, [12] the Medical Interoperability Gateway of the Healthcare Gateway company, [13] or the Semantic Gateway as a Service solution of the Internet of Things paradigm. [14]

Interoperability services, according to their availability may be publicly available to anyone, or closed, accessible only to the members of a cooperation group. *Public interoperability services* include, for example, freely available document format conversion services (voice, video, text, document, presentation, e-book, archive, etc.) on the Internet. Most of these are accessible via a manual user interface, but many service providers also provide programmed access, in the form of web services.[9] These may be free or pay-per-use cloud-based services. In case of public services, safety considerations must also be taken into account as the information to be transformed becomes accessible to the service provider.

Closed interoperability services are a safer solution provided by internal providers under the control of a particular user group, or by trusted external service providers. The availability of services can be restricted to closed networks or controlled by access rights. Closed interoperability services may be needed, inter alia, for public administration, the defence sector and the cooperative IT systems of the European Union or NATO. In case of European and national public services, closed service can be provided by the previously mentioned interoperability service public utility.

Users of Interoperability Services

Users of interoperability services are cooperating actors, who exchange information with each other and wish to create the conditions of the meaning-preserving information exchange using the services provided by service providers.

The ***benefits of interoperability services for users*** are essentially the same as the benefits of services in general. Services provide capabilities, perform activities that their users cannot, or they would only at an expense, compared to which the service is more economical.

The basic type of interoperability services is a meaning-preserving transformation between information representations (data), ranging from transforming certain data elements, to transforming messages, and connecting information exchange protocols. This is accomplished through software components that can also be obtained as a product, so the question arises why software components that can be embedded in your system are not worthy of use as services.

The traditional reasons for the use of services in general are also true for interoperability services: their total costs are lower, they can be used timely, without preparatory tasks, the service levels can be guaranteed, operational and maintenance tasks are not the users responsibility. Because of the information exchange standards change from time to time, newer versions will be introduced, special expertise, software modification and development will be required to track these, but this is the responsibility of service providers rather than users.

In case of interoperability services, there are also ***user tasks.*** As interoperability services are expected to relate to more widely used, standardized representations, they support the use of meaning-preserving transformations between such representations, specific transformations need to be implemented by users between user specific internal representations and

[9] For example, ZamZar Online file conversion, online-convert.com, ConvertAPI.

representations known by interoperability services. Let us examine where they are needed, and where they are not and where services are probable.

The number of different representations of the *first group of general data elements* (such as numbers, logical values, dates, times) is relatively low, less dependent on the application area, the transformations that can be made between them are well formalized and can be easily implemented so that they can be provided as adequate interoperability services.

Different representations of *another group of general data elements* (character strings, unformatted texts: names, short descriptions, remarks etc.) can differ in two ways: the character set used and the language. The range of the former is also limited, so transformation services between them exist, and will exist in the future. Furthermore, to resolve language differences, there already exist— in fact not yet perfect—services in the form of machine translation capabilities.

Finally, interoperability services already exist in the form of easy-to-use conversions between different formats of *audio, video and video information.*

In case of *classification data elements (categories or types),* interoperability services between the different versions of these are required only for widely used standard versions. To develop such a transformation, and a service implementing it are made more difficult by the fact that there is usually no unambiguous mapping between the different classification systems, working in both directions. Nonetheless, when exchanging such information, accepting some loss of information, through the use of an "other, cannot be classified" category, the transformation could be done with preserving the most possible information.

The meaning-preserving transformation between *different formats of data sets* (messages, composite documents) is a complex task, including the necessary transformation of data elements that constitutes the data-set, as well as their relationship structure, the data describing this structure. The questions related to data elements we have been discussing above and in case of data structures, based on the fact that a significant part of these structure formats[10] is of general purpose, standardized, widely used, and interoperability services are already expected to appear.

Providers of Interoperability Services

Interoperability services cannot exist without service providers, so there should be actors that create these services, maintain the conditions for their provision and make it available to the consumers who use the service. The benefits of implementing interoperability functions in the form of a service include the concentration of the capabilities required for the functions, the wider availability of functions and therefore the more economical operation and the more efficient maintenance of functions.

Interoperability providers according to their type may be third party market-based providers working independently of the consumers of their services, or may be internal service providers supervised by some user community. *Third-party service providers* may offer interoperability services in the public domain, mainly on syntactic and elementary

[10] Nowadays, these formats are primarily at the elementary level, the XML; at the upper levels are the different message format or document format standards.

semantic level, but may also operate interoperability gateways if there are user needs. In case of the former, service providers use these services to promote their other similar products, while in case of the latter it is more likely to sell interoperability gateways as products, complemented by a service package that includes further development.[11] In my view, in case of organizational actors, the use of external service providers will be limited due to security, reliability and availability considerations.

Internal service providers typically provide closed services (available to a particular user community), and their services, less frequently, could be open. They serve organizational purposes, the information exchange within a stable cooperating community, the integration of heterogeneous IT systems. The implementation of functions supporting the meaning-preserving information exchange as a service enables the functional separation of the functions and tasks of the organizations involved in the operation of IT systems and of the organizations, organizational elements providing interoperability services.

The ***capabilities necessary for interoperability services*** in case of syntactic level services are easier to develop and do not require deep application area expertise. Conversely, much of the information needed for the transformation at the semantic level is not readily produced. Among them, the transformations between different classifications are a top priority.

The *reasons for different classifications* lie in the different needs and perspectives of their users. Different application communities can group the same objects into different classes, according to their own interests, to their own criteria. There may be a difference between the range of objects to be categorized, and a user community can also create classes for objects that are not in the interest of other communities. Differences between classifications cannot usually be eliminated, in the vast majority of cases there is no way to create and apply a single classification system that is equally suitable for all users.

The *transformation between the different classification systems* means practically a conversion between classification characteristics: based on the source side classification value the target side classification value should be determined. The result of the conversion may be that for the source classification does not exist an appropriate classification value on the target side (or, if there is, it is only the "other"). Therefore, conversion requires further knowledge, for example other attributes describing the source object. Depending on the nature of the relationships and differences between the two classification systems, from the point of view of the source, a transformation may be a one-to-one mapping, it may require additional information (knowledge of other characteristics) and may not be feasible. Conversion between two classification systems, in many cases, is not symmetrical: it can be performed in one direction (e.g. from a more detailed classification into a more comprehensive classification) and in the other it cannot, or only partially.

Service providers that provide transformations between classification systems may be the organizations responsible for the definition of classification systems, or may be independent service providers. The former, of course, has better capabilities and opportunities to determine the content of the meaning-preserving transformation. In case of modification of the classification system on the same application domain, the responsible organization is

[11] For example, in the military application, the IRIS MTF Gateway and IRIS Information Mapping of the Systematic company, as well as the Oracle EDI Gateway products in civil application.

able and is entitled to define the rules of the conversion.[12] In case of a transformation between a classification system supervised by two different organizations, the definition of rules may be the result of joint work, or may be done by one party that is more interested in ensuring the possibility of conversion from another classification system to its classification system.

Interoperability Services in Cybersecurity Information Exchange

Today's social, economic, and everyday activities are increasingly dependent on the services provided by the interconnected, decentralized IT systems and networks that make up the cyberspace. Increasing dependence also means a growing vulnerability and risk, as the breach of the security of IT systems, networks and of information and data that they manage will also result in harm to security of these services. Every state, and every organization must be ready to manage the risks and handle the threats in cyberspace to ensure an adequate level of cyber security. The creation and maintenance of cybersecurity requires a wide cooperation involving several actors, based on the exchange of cybersecurity information.

The cybersecurity information exchange, like other areas of expertise, is hampered by differences and heterogeneity between the actors involved and the IT systems they use, due to their different purposes, approaches and solutions, which require an interoperability solution. One of the possibilities of creating and maintaining interoperability between the actors' IT systems is the implementation of interoperability functions in the form of services.

In the following I will first summarize the basics of cybersecurity information exchange and its interoperability problems and solutions; next, I identify the possible types and content of the syntactic level and then the semantic level of cybersecurity interoperability services.

Cybersecurity Information Exchange, Interoperability Problems

For the purpose of exploring and analysing interoperability services supporting cybersecurity organizations in the following, based on two of my previous publications, I first summarize the framework for cybersecurity information exchange, [15] then the interoperability problems and solutions for information exchange. [16]

Cybersecurity information is all the information that actors involved in cybersecurity[13] are using to perform their tasks. This information can be divided into four major groups (information related to events, to vulnerabilities, to threats, and other information).

Information related to cybersecurity events consists of primary raw event information and evaluated event information. These include the information about the person, organization reporting, the dates and the description of the event; its classification; the components involved, the consequences and effects of the event; and its roots, causes and course. Cybersecurity organizations are continuously receiving, analysing, and, where necessary,

[12] For example the Hungarian Statistical Classification of Economic Activities (TEÁOR).

[13] Cybersecurity emergency response organizations, cybersecurity operations centres, other cybersecurity organizations (providing information, detecting and analysing threats) and vendors of IT products.

transmitting information about the events to the organizations under their responsibility (constituents), and to the cooperating organizations.

Cybersecurity actors maintain and use global and organizational level databases about *cybersecurity vulnerabilities* for their activities. These databases contain the identification and description of vulnerabilities; the components involved, the consequences, and the assessment and severity of the exploitation; the possible ways and methods of exploitation, and its tools already known; as well as the solutions that eliminate, or minimize their impact.

Information on cybersecurity threats are analysed, evaluated, synthesized information about potential security events, potential actors, attackers threatening security, and the methods and procedures they employ, which are used in cybersecurity risk management. While vulnerability-related information belongs to the "own/internal side" part of malicious security events, threat information belongs to the "attacker/external side".

The main types of *cooperation relationships between cybersecurity organizations* include:

- cooperation between a cybersecurity event management centre[14] and the cybersecurity operations centres (IT system operators) under its jurisdiction;
- cooperation between superior and subordinated cybersecurity event management centres with wider and narrower responsibilities (e.g. national and sectoral; or international, regional, federal and national organizations);
- cooperation between cybersecurity event management centres on the same level with non-overlapping responsibilities (e.g. different national or different sectoral organizations);
- cooperation between cybersecurity event management, or operations centres, and vendors of IT products;
- and finally, connections between cybersecurity event management, or operations centres, and military, law enforcement, or national security organizations.

The conditions for sharing cyber security information—within the legal framework—are determined by the information sharing policies of the individual organizations and the trust relations between the organizations.

The basic purpose of exchanging information between cybersecurity organizations is to enable each organization the access to information necessary to their decisions. For this purpose, it is necessary to share and provide information that is necessary and sufficient for the organization using the information. These are called "actionable information" by ENISA documents. [17: 2–4]

The role and significance of the ***interoperability of cyber security organizations*** is of paramount importance, as cybersecurity threats in global cyber space do not have organizational boundaries, and the network boundaries (even in case of distinct networks) are not impermeable. Although cybersecurity organizations sometimes produce new cybersecurity information, their activity is based on information, notifications, announcements, alerts, coming from outside the organization. Lack or lower level of interoperability means that organizations affected can only perform their activity with less information, or the processing of received information requires extra work, takes more time.

[14] Computer Security Incident Response Teams (in the EU), or Computer Emergency Response Teams (in the USA).

Technical level problems of interoperability are related to the data transmission (if necessary secure) links. Today these problems—apart from the potential problems of the secure connection—are relatively easy to solve. *Syntactic level problems* can occur during the exchange of unstructured (typically free text) data, related to the message formats used and the formats of each data element. The necessary transformations to solve these problems are also available, or feasible.

The *semantic level problems* in the field of cybersecurity are also a key issue for ensuring and maintain interoperability, and the provision of meaning-preserving information exchange. In this area there are a variety of taxonomies for different purposes, there are sets of controlled values sets, some of which are used in wider, others in a narrower scope of cooperation. In the future, it is expected that more cybersecurity classifications will remain in use, so their possible alignment or meaning-preserving transformations remain a task for actors involved.

Syntactic Level Interoperability Services for Cybersecurity

The meaning-preserving information exchange between the cooperating cybersecurity organizations—in order to resolve the existing differences—may require a number of syntactic level transformations. In the following, I will examine what types of syntactic level transformations may be required, and in which cases may they occur, and for what reasons the providing of this functionality occurs in the form of services provided by a third party.

The first group of syntactic transformations consists of ***transformations of data elements.*** Among these, the syntactic transformations of numeric, logical, date and time data are well formalized, algorithmised and can be solved on their own. In case of transformations of textual data (names, denominations, descriptions) between different character sets, formats (especially in case of names) and translations between languages the use of services may occur.

For systems that identify certain things (such as hardware or software components affected by security incidents or vulnerabilities) with names, the format for naming the same component may be different in two systems. For this reason, it may be necessary to convert from one format to another, or to split into a different number of name elements, or to make minor translations.[15] In case of textual descriptions, the necessity of translation does not need explanation.[16]

The implementation of these transformations in the form of a service may be justified by the wide, dynamically changing and expanding range of information, and expertise

[15] For example “Adobe Flash Player for Microsoft Edge és Internet Explorer 11 - 31.0.0.108 és korábbi verziói (Windows 10 és 8.1)” (govcert.hu, Hungarian Government Incident Response Team) ~ “Adobe Flash Player for Microsoft Edge and Internet Explorer 11” + “31.0.0.108 and earlier versions” + “Windows 10 and 8.1” (Adobe Security Bulletin)

[16] For example „A sérülékenységet a Cisco Umbrella API interfészéhez tartozó hitelesítés nem megfelelő konfigurációja okozza. Ezt kihasználva, egy hitelesített, távoli támadó olvashatja a saját és más szervezetek adatait, valamint módosítani is tudja azokat.” (govcert.hu) ~ “A vulnerability in the Cisco Umbrella API could allow an authenticated, remote attacker to view and modify data across their organization and other organizations.” (Cisco Security Advisory)

required (related to the formats used), the general nature of the task (machine translation), or the special domain knowledge related to translation of cybersecurity related texts.

The other group includes ***syntactic transformations between groups of data, and data structure representations.*** Basic tools for exchanging cybersecurity information are texts that meet simple structural and formal rules,[17] as well as XML and JSON formats. Transformations between these formats affect the parts describing the structure: in case of text, the order of components and the headings; and, in case of markup languages, the tags used. To transform the complete composite data format (representation), it is also necessary to convert data elements of the source format to data elements of the target format, which belongs to the previous set of transformations.

For transformations of groups of data, the source format may not contain all the required data for generating the target format, or contains data that is not included in the target format (are not of interest to the target user). The latter does not constitute an interoperability problem; it can be considered a realizable filtering that can be solved by the service. Missing data for syntactic level services in some cases may optionally be added, or the result will only be partial. This may be done by the omission of data, or using the "unknown" value. In case of mandatory data, successful transformation requires human, expert involvement. However, compared with a "manual" transformation, this can still be a very useful service.

One of the likely broadly useful services may be the transformation of the above-mentioned structured text data using a markup language (e.g. XML format) describing the structure and the type of data elements. The resulting format can now be further easily transformed to other, for example standard formats, or can be used to convert to a native, inner format of the cybersecurity actor's IT system.

Semantic Level Interoperability Services for Cybersecurity

During the exchange of information between the cooperating cyber security actors, the most important and most difficult to resolve differences are the correct interpretations of the transmitted data. The features of cybersecurity events, vulnerabilities, threats, and other entities of interest are represented by all actors in a manner appropriate to their own goals and tasks.

Differences on the semantic level may, for example, appear in the parties' classification of different things into a concept (e.g. what they consider as a security event); when things are categorized by different criteria, or with different details; the characteristics are described with different value sets; relationships between things are recognized differently. Much of these differences can be traced back to classifying and categorizing things, so I will focus on two questions of implementing transformations between different classifications.

Services performing the transformation between classifications can be implemented in "wired" form, using formalized conceptual systems, or in a complex way. In case of a *wired solution*, the party using the service must provide the source and destination classification identifier and the source classification value, and the service determines the classification

[17] For example the Hungarian Government Incident Response Team vulnerability list (database), or security bulletins, advisories, notifications provided by different organisations.

value according to the target classification. This solution can be used to convert between two specific classifications.

For *services based on formalized conceptual systems* (taxonomies, ontologies), the service provider implements the transformation with a general-purpose interpreter engine using semantic relationships (identity, is-a, etc.) between the classification values, as concepts. The advantage of this solution is that its capabilities can be expanded and improved by incorporating new classification concepts and conceptual relations without software modifications.

Using existing transformations between classifications, new *transformations built on successive steps* can be created. The disadvantage of this solution is that there may be a case in which there could be a one-to-one mapping between two classifications, but this is not possible through the intermediate classification (for example, because its detail is lower than that of the two others).

Organizations responsible for particular classifications can play a prominent role among ***service providers of transformations between cybersecurity classifications.*** They are able and even entitled to define the mapping in the most appropriate way between different versions of their classification systems. An example is the Top 10 vulnerability category system of the Open Web Application Security Project (OWASP), where there are four changes from 2013 to 2017.

An organization responsible for widely used detailed classification system may also be able to provide transformation from its own classification to a less detailed classification system. An example is the Common Weakness Enumeration (CWE) software security weakness categorization that is part of the US National Vulnerability Database, for which a mapping has been defined for different versions of OWASP Top 10 categories (2013, 2017).

Conclusion

The starting point for this publication is that the services provided by globally interconnected, decentralized IT systems and networks, the cyberspace, play a prominent role in our world. The dependence on these services requires the high-level security of cyberspace that can be ensured by a broad cooperation of different organizations, actors. Successful and efficient cooperation cannot be achieved without a similar level of information exchange between the actors, and their IT systems that requires interoperability of these systems.

Functionality ensuring interoperable information exchange between IT systems can be realized using own resources, or using services provided by third parties. The term interoperability service in the literature is described in several different forms, mostly without precise definition. The suggested definition of IT interoperability service is a service by which the service provider supports interoperable (meaning-preserving) data exchange between the information systems, tools and applications of service consumers, cooperating actors. Interoperability services can be implemented as middleware services, web services, and cloud-based services.

Interoperability services can be categorized according to different criteria: their level, nature, and availability. The benefits of using interoperability services are obvious, but there remain tasks that the service consumers (users) should do on their own. Interoperability

service providers can be third party market-based providers, or internal providers, serving organizational, or cooperating community interests. Some interoperability services do not require application domain specific knowledge, but others (primarily on semantic level) do require.

Cybersecurity information exchange has special requirements for interoperability services. They require support for interoperable exchange of data about cybersecurity events, vulnerabilities, threats and other objects of interest. Syntactic level interoperability services can provide transformations of data elements, transformations between groups of data and data structures. Among semantic level interoperability services, the transformations between different classifications play an important role. Ideally, these can be provided by the organisations responsible for classifications.

References

[1] MUNK S.: *Katonai informatikai rendszerek interoperabilitásának aktuális hadtudományi kérdései.* (DSc-értekezés) Budapest: Magyar Tudományos Akadémia, 2007.

[2] MUNK S.: Az adaptív interoperabilitás fogalma és szükségessége katonai informatikai rendszerek esetében. *Bolyai Szemle,* 1 (2006), 28–39.

[3] MUNK S.: Changes in the military information interoperability environment. *Revista Academiei Forţelor Terestre,* 4 (2005), 39–51.

[4] WIEDERHOLD, G., GENESERETH, M.: The Conceptual Basis for Mediation Services. *IEEE Expert,* 5 (1997), 38–47.

[5] BUSSLER, C.: B2B and EAI with Business Process Management. In. CARDOSO, J., ALST, W. van der (eds.): *Handbook of Research on Business Process Modeling.* Hershey & New York: Information Science Reference, 2009. 384–402.

[6] CHARALABIDIS, Y., PANETTO, H., LOUKIS, E., MERTINS, K.: Interoperability Approaches for Enterprises and Administrations Worldwide. *The electronic journal for e-commerce tools and applications* (eJeta), 3 (2008), 1–10.

[7] LI, M. Sz., CABRAL, R., DOUMEINGTS, G., POPPLEWELL, K. (eds.): *Enterprise Interoperability, Research Roadmap Final Version (Version 4.0).* Information Society Technologies, 2006.

[8] *Content Management Interoperability Services (CMIS) Version 1.1 Plus Errata 01.* OASIS, 2015.

[9] *C3 Taxonomy Baseline 2.0* – AC/322-D(2016)0017 Enclosure 1, NATO Consultation, Command and Control Board, 2015.

[10] BISHOP, T. A., KARNE, R. K.: A survey of middleware. In. *Proceedings of the ISCA 18th Conference Computers and Their Applications.* Honolulu, 26–28 March 2003. 254–258.

[11] *Web Services Architecture.* W3C Working Group Note 11, 2004.

[12] *AC/322-D(2004)0040 Annex 1, NATO C3 System Interoperability Directive. Version 2.* NATO C3 Board, 2004.

[13] *Healthcare Gateway: Services.* https://healthcaregateway.co.uk/services/ (Downloaded: 05.10.2018)

[14] DESAI, P., SHETH, A. P., ANANTHARAM, P.: Semantic Gateway as a Service architecture for IoT Interoperability. In. *Proceedings of the 2015 IEEE International Conference on Mobile Services.* 313–319.
[15] MUNK S.: Kiberbiztonsági szervezetek közötti interoperábilis információcsere megoldások (sérülékenységek kezelése). *Bolyai Szemle,* 1 (2018), 54–77.
[16] MUNK S.: A kiberbiztonsági információcsere interoperabilitási kérdései. *Hadmérnök,* 3 (2018), 422–434.
[17] *Actionable Information for Security Incident Response.* Heraklion: European Union Agency for Network and Information Security, 2014.

AARMS Vol. 17, No. 3 (2018) 149–164.

Technical Dimensions of the Development of Unmanned Aerial Systems and Their Impact on Public Service Uses

András NÉMETH[1]

Due to the processes and specialized research of the revolution in technological and scientific information of the last few decades, the development of Unmanned Aircraft Systems (UAS) has now reached the state where it may become a defining factor in the market of civil technologies. In the wake of efforts to enhance aviation safety since the first generation of multicopters, hobby and professional tools have become available that—provided that statutory requirements are flexible enough—could be used in corporate and government sectors alike.

However, the use of such equipment to improve public services would require a strategic-level policy change. Due to rapid technological changes, the speed at which drones are developing is unprecedented, and such equipment is becoming dated significantly faster than, for example, the planned life-cycle of military equipment. These circumstances call for a solution that breaks away from existing procurement principles, and is able to continuously provide government organizations with equipment that meets the latest technical standards, and supports the efficient execution of the most diverse specialized tasks.

This publication aims to present the complexity, technical dimensions and development trends of "drone science", along with suggestions on how their use could be efficiently integrated into the toolbox of public service tasks.

Keywords: *Unmanned Aircraft Systems, drones, system of public-service tasks, development trends*

Introduction

The term "global drone market" has only emerged in the last five years, and the related market research and preparation of various forecasts has already grown into an independent business segment. This fact alone shows that the use of unmanned aerial vehicles (UAVs) and the associated technology is skyrocketing, bringing about a potentially significant change in many areas within only a few years. Since the emergence of the first similar forecasts, all analyses show a dynamic expansion of this market segment, propelled both by Unmanned Aircraft Systems, and by activities related to civil purpose equipment (e.g. design and manufacture of components and equipment, system integration, sensor systems, data processing solutions and insurance). Some variations do exist between individual

[1] Ph.D., National University of Public Service, Faculty of Military Sciences and Officer Training, Department of Electronic Warfare; e-mail: nemeth.andras@uni-nke.hu
The research has been supported by the ÚNKP-17-4-3-NKE-71, the New National Excellence Program of the Ministry of Human Capacities.

forecasts—in terms of the extent and rate of extension—however, they all agree that the time of the forecasted breakthrough is still uncertain. This is basically caused by sluggish attempts to adapt to statutory requirements. Taking a closer look at the data of a much-referenced analysis published in June 2016 (Fig. 1), [1] it becomes clear that for at least the forthcoming years, the hegemony of military expenses remains unchallenged. At the same time, attention may be drawn to the fact that the 9 percent of the entire market spent on civil uses (mostly by the government) in 2016 is forecasted to double to 18 percent within five years (by 2021). For the market of civil uses this means USD 1.8 billion globally, which translates to a 2.25-fold increase. For 2024 this amount—primarily due to the intense expansion of public service and corporate uses—will increase to a 3.3-billion-dollar scale, almost doubling in three years. It will cover slightly more than one quarter of the entire market, exceeding 12 billion dollars. While the entire market will expand by 70 percent in eight years, due to the dynamic growth of the civil—mostly government—use, this segment will show a result of more than 400 percent.

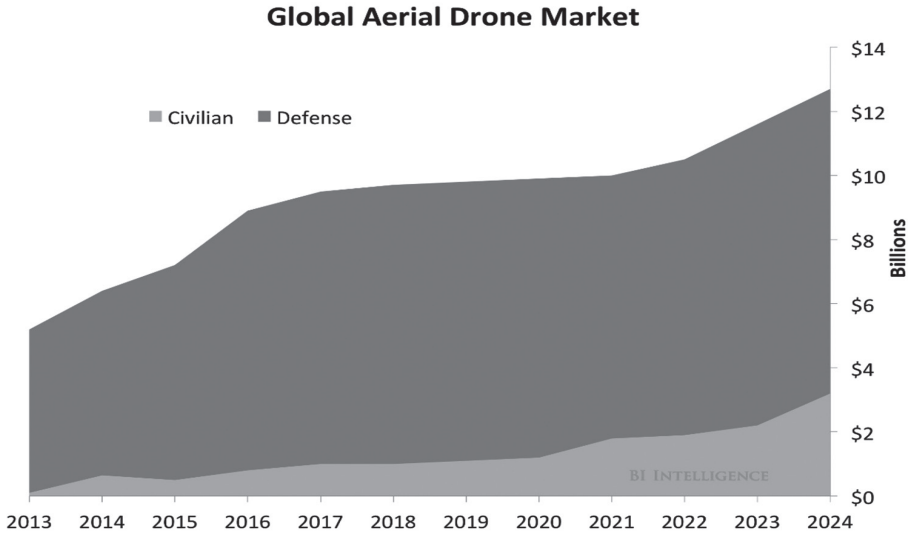


Figure 1. *Global Aerial Drone Market.* [2]

The results of a significantly later study were published in 2018. Though the methodology shows significant variations, it is still obvious that analysts are expecting a turnover of more than 20 billion dollars for this year, which—if the average annual growth rate (CAGR) exceeds 14 percent—will exceed 52 billion dollars by 2025. For this year they primarily expect a growth in the fixed-wing UAV market as opposed to the multicopter market, as the former possess better parameters in terms of military, public service and commercial/delivery use (flight time, payload, etc.). Based on this, the largest segment will be covered by the medium- and high-altitude and medium- and long-range UAVs' turnover, dominated by North American companies (45 percent). The European share will be low by all calculation criteria (20 percent), which is partly explained by the lack of unified European legislation on the matter. Considering this, the list of the top players, General Atomics (USA), Northrop

Grumman (USA), Textron (USA), Boeing (USA), DJI (China), Parrot (France), 3D Robotics (USA) and Aeryon Labs (Canada) is no surprise. [3]

To fulfil these long-term forecasts, legislation attempts aiming to simplify the use of UAV systems (mainly in Europe), and the technological developments allowing for a large-scale and safe airspace use, will need to be promptly realized.

The primary goal of this publication is to provide an overview of the underlying linkages of the scientific and technological developments and their impacts and expected results, while integrating those in attempts to improve the efficiency of the public service task system.

Drones and Science

The terminology used for unmanned, remotely operated aircraft has changed several times in the last decades. Today, official documents issued by international professional organizations belong to one of two main schools: the International Civil Aviation Organization (ICAO) opted for Remotely Piloted Aircraft System (RPAS), also used by EUROCONTROL, the European Aviation Safety Agency (EASA) and several national aviation organizations. As opposed to this, the Federal Aviation Administration (FAA) and the British Civil Aviation Authority (CAA) uses the term Unmanned Aerial/Aircraft System (UAS). The most important connection between the two terms is the approach to perceive such aircraft as a system. The term "drone" is used in French-speaking territories; thus, this is the term preferred by the French Civil Aviation Administration (DGCA) in its communications. It is also the term used by civil and recreational users, along with the media. [4] [5] In this publication, the terms UAS, UAV and drone are used in a quasi-interchangeable manner, as synonyms of the official "unmanned aerial vehicle" preferred by operational Hungarian legislation.

Back to the system approach, despite several sensor systems and other components essential for the operation of the vehicle, the UAV is regarded only as a subsystem (aerial subsystem), for the operation of which, amongst other things, a ground-based subsystem is essential, with the functions of remote control and a communication subsystem enabling data transfer between the two. Expanding the definition even further, the human resources necessary for the operation can also be regarded as a subsystem (operators), even so the procedures associated with the safe operation of the system (e.g. checks, inspections and maintenance).

In order to understand the importance of handling Unmanned Aircraft Systems as a strategic industry by government players—as the largest prospective drone users—it is worth identifying the disciplines in the Hungarian Academy of Sciences (MTA)[2] nomenclature [6] that are directly or indirectly used or affected by this dynamically growing market segment.

The relation system between science and Unmanned Aircraft Systems is more complex than it seems at first glance. At first, the development of *natural non-life sciences, mathematics* and technology-enabled creation of the systems we know as UAV today, appeared. At the same time, the rapid emergence and widespread use of such equipment also had an impact on *life sciences, humanities, and social sciences.* In the future, it will bring about changes in the very basics of many disciplines and their approaches. Through agricultural applications—based on the discipline nomenclature—the most affected life sciences are some areas of *agrarian sciences,*

[2] Magyar Tudományos Akadémia – the Hungarian Academy of Sciences.

while within humanities and social sciences it would be *archaeology, law, economic sciences, war sciences, and regional sciences* that are increasingly affected. These are the sciences that, amongst other things, discuss the government task systems falling directly or indirectly under the umbrella term of public services. Figure 2 shows the system of non-life sciences that can be associated with UASs, based on the MTA's nomenclature.

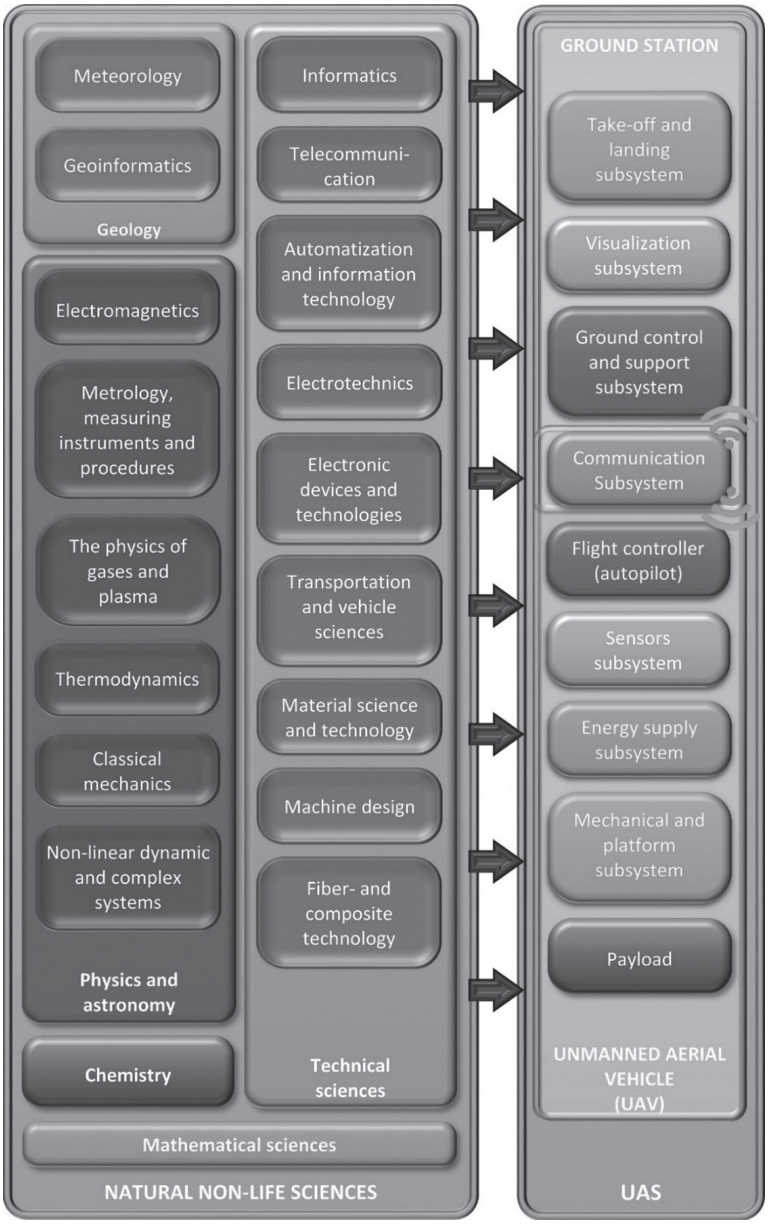


Figure 2. *The Relation of Science and UAS.*
[Created by the author.]

If aviation itself is our starting point, we have to start our study in the field of *physics and astronomy.* An important segment of *classical mechanics* is fluid mechanics and gas dynamics, which are essential to modelling the motion of heavier-than-air objects in the air, and to the design and construction of aircraft. Examining the stability, the forces or the physics of changing the direction of movement of aircraft would require us to use Newton's mechanics, the physics of solid objects, hydraulics, or applied mechanics. If we handle all UAV subsystems as a complex entity, we deal with *thermodynamics, the physics of gases and plasma, non-linear dynamic and complex systems,* or even *electromagnetics.* This latter is the basics of radio frequency-based remote control and wireless communication. The knowledge of several fields of *chemistry* is necessary to design and manufacture energy sources generating energy from chemical transformations (for example batteries), and to examine their features. *Mathematical sciences* establish the framework of natural sciences' activities, and provide them with a calculation tool system, while any other academic field and discipline also uses several achievements of mathematics. The connection of *geology* and drones is not only a broad, indirect connection: *geoinformatics* provide the theoretical background of the functions of air navigation, flight planning and independent flight. For several applications, the achievements of this discipline are used for evaluation and digital map imaging of the results. Similarly, *meteorology* directly affects flight safety, which can be enhanced with aviation meteorology research.

At the same time the design, functional modelling, simulation, manufacturing, testing or compliance verification of Unmanned Aircraft Systems or their subsystems, components or parts, primarily and directly rely on *technical sciences. Informatics,* amongst other things, provide us with the software and hardware necessary for the above processes (for example design and testing platforms) and applications ensuring access to the services of the *ground control and support, visualization, and communication subsystems* necessary for the safe operation of UAVs. *Telecommunication* gave us the means of radio communication between the UAV and the ground-based subsystem in the form of wave shapes, modulation, encoding, and cyphering processes. *Automatization and information technology* ensures the control and adjustment functions and solutions enhancing autonomy and the adequate operation of the *integrated flight control subsystem* (autopilot). *Electrotechnics* provides the theoretical background of all electronic circuits in the system, while their practical realization and manufacture of electric parts, sensors and batteries necessitate the *electronic devices and technologies* discipline. Research of air navigation procedures and technical solutions necessary for their safe operation—such as handling UAVs as an aircraft, and integration of UAVs in the same airspace—falls under the *transportation and vehicle sciences* category. *Material science and technology,* and *fibre- and composite technology* have also contributed to the creation of several subsystems. Research of structural material is worth mentioning here, which aims to enhance the resistance, reduce the weight and increase the life-span of all structural elements and moving parts *(mechanical and platform subsystem).* Efforts to increase the energy density of batteries are to be emphasized, as part of the *energy subsystem.* The results of *machine design,* as part of the *mechanical subsystem,* both affect the shaping of airframes and propulsion units.

UAS Technology and its Technical Parameters

Moving on from the scientific aspects to the technical dimension, it is practical to examine the effects of the innovation and development of the drone industry on the technical parameters of individual pieces of equipment. This is the basis of evaluation of the equipment's suitability for the given purpose. For a given system of public-service tasks, knowing the requirements of the user organizations, a comparison of such parameters will help to establish the type and quantity of the necessary UAVs, and the conditions of a minimum-level, the optimal, or an "oversized" operation (provision of backup equipment, transportation capacity, operators, fuel supply, other necessary support and servicing, etc.), or the fields to be developed and the direction of development.

The technological development of several academic fields witnessed in the last few decades generated revolutionary changes, as a result of which the costs of the initial investment of several modern technical solutions have reduced, allowing for a cost-efficient creation of complex systems. As a result of these processes, in addition to the primarily fixed-wing, bulky, costly UAVs of exclusively military purpose (MQ–1 Predator, [7] RQ–4 Global Hawk, [8] MQ–9 Reaper [9]), civil equipment (mostly government use) has also emerged, giving rise to commercial and recreational uses. At the same time, development has to date been propelled by the market of multirotor, electric engine equipment emerging from RC modelling. This significantly affects fixed-wing constructions and opens up new perspectives in terms of applications, including government uses.

Figure 3 shows a schematic structure of a UAS version. Logically, Unmanned Aircraft Systems can be broken down into two large subsystems, which contain further, distinct functional blocks. The features and operational characteristics of these individually affect the equipment's technical parameters and their limitations. At the same time, it is the quality of their synergy that determines the system's actual capabilities and features that are important for its practical use. However, in terms of reliable and safe operation, the human operator is also part of the system in a wider sense, though often regarded as secondary, along with elements of maintenance technical service (maintenance, repair and provision of backup equipment). These latter two factors are significant, especially for government use, as usually equipment is available through procurement or own development and manufacture, and its technical parameters are known, but efficiency of its operation is determined by the knowledge, skills and experience of the operators and the logistical background responsible for availability.

The development direction of the individual subsystems is basically determined by the technical opportunities and users' needs, along with the associated characteristic market trends. Emphasizing one of the most important technical dimensions, namely *nanotechnology*, it is worth mentioning that it is the most dynamically growing and miniaturizing segment of material sciences and technology. [10] [11] It contributed to the reduction in size of electric spare parts and sensors, the enhanced complexity of integrated and programmable circuits, and the opportunity to use solid, resistant, yet light structural materials. At the same time, it significantly affects the development of power sources, as using nanostructure materials with targeted design, manufactured under controlled circumstances and built from various atoms, allows for the manufacture of greater energy density and lower specific weight batteries, with more beneficial electric

features (for example life-cycle, charging time, environment-resistance). [12] Using such materials gives UAS designers more flexibility, for example when optimizing flying time and weight for a given task. For all subsystems, material science and technology are significant and increasingly dominant. Even more so, if during the development process we consider the cycle of creation of prototypes both in terms of time and costs. Due to ongoing revolutionary changes in the field of *3D printing*, the methods used for not only the manufacturing of prototypes, but also for the end products, has become increasingly efficient. [13] These opportunities may propel the research of identical structure mini-drone swarms, even with a large number of drones. [14]

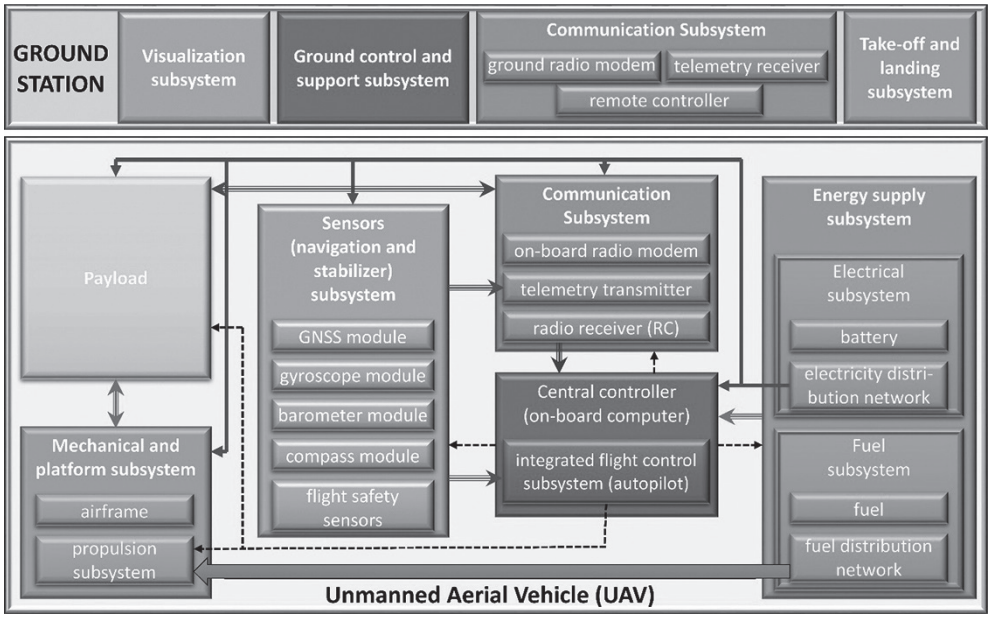


Figure 3. *A generalized UAS structure.*
[Created by the author.]

However, the practical use of mini-drone swarms requires advances in another area, as well. The use of automation and information technology toolkits is also essential for the ability to create a collective intelligence for the drone swarms. Task sharing at the highest possible level of autonomy is allowed by research results in the field of neural networks, *artificial intelligence,* and machine learning methods. [15] [16] Additionally, *increasing computing and data storage capacities* affects the control of UASs, by increasing quantities of real time access, and processing data provided by the increasingly complex sensor system (e.g. multi-direction ultrasound and optical sensors, range indicators, compasses, accelerometers and barometers). [17] On the other hand, information coming from on-board devices and surveillance systems (e.g. ultra-high-resolution cameras, highly sensitive heat cameras, radio frequency surveillance equipment) have to be continuously saved and transmitted to the ground-based subsystem's data processing centre, along with the telemetric data, through a *broadband high frequency datalink.* [18]

And adequate technical background for the latter functions, including remote control by a reliable and secure radio frequency, is provided by the continuous development of telecommunication technologies, and the development and integration of new wave forms and modulation, encoding and cyphering methods. The goal is to transmit as much information as possible within a given amount of time, as independent as possible from the electromagnetic environment and weather conditions. For the ground-based subsystem, the most important software factors are data processing, analysis, evaluation and imaging. Efforts are made in the direction of the highest possible automation of processes. As it is about aircraft, establishment of the exact geographical location of the equipment is vital for both the control of the UAV, and for efficient execution of tasks. Detailed fight planning and routing, even considering meteorological conditions, may significantly reduce the time used for reconnaissance of a given area. This facilitates coverage of larger areas with one flight, for example with a given battery capacity. By using Global Navigation Satellite Systems (GNSS) receivers [19] and ground-based or satellite differential supplementary solutions, this will be a reality in the near future, possibly with a centimetre-scale accuracy, facilitating flight planning or linking measurement information to geographical location points and graphic imaging through Geographic Information System (GIS) applications. [20] [21] At the same time, significant progress is needed to efficiently process the increasing volume of information collected by drones, with the least human intervention possible.

Spreading of practical applications is affected by the level of aviation safety, improvement of which requires accurate navigation and significant development of the autopilot and sensor systems. This is essential to minimize risks by increasing autonomy, by using technologies to prevent, detect and avoid emergencies, and by enhancing the security and reliability of datalinks, even under the following circumstances: low-altitude, below-the-horizon operations (terrain following, obstacle avoidance); flights in busy airspaces (collision avoidance); night flights; flying above people or masses of people; flying among buildings; or a combination of the above. Of course, this would necessitate a change of generations in airspace management, airspace oversight and air traffic control, just like in the broadband mobile communication (5G) services and cloud-based storage services responsible for the transmission of data.

Another large and complex impact area affecting several subsystems is flight time. For example, for a multicopter, increasing the volume of the on-board battery will also increase the available electrical power. But the increased weight will result in increased use of electrical power by the engines, in other words, the additional power will be used up faster. This latter will decrease the effects of the first factor, therefore the flying time will increase in a limited way, but engines will depreciate faster. The goal is to increase the energy density of power sources (e.g. fuel cells [22]) and decrease the total weight of the UAV (use of low specific weight material), reduce the power consumption of the engines, and optimize flight controlling algorithms (reduction of the number and extent of interventions). Primarily, for fixed wing constructions reduction of drag is also an important challenge. Use of solar panels would increase flying time further.

Classification of Unmanned Aircraft Systems with Special Regards to Public Service Uses

Unmanned Aircraft Systems can be classified by several criteria, but usually it is done by the physical characteristics or flying parameters of the aerial subsystem, i.e. the UAV, such as maximum take-off weight, range, cruising altitude, or flying time. Based on the above parameters, one of the most accepted classifications was put together by the Unmanned Vehicle Systems International (UVSI) non-profit international association, in which they attempted to blur the line between civil and military use equipment. The tactical level contains 10 subcategories (nano, micro, mini, Close-Range – CR; Short-Range – SR; Medium-Range – MR; Medium-Range Endurance – MRE; Low Altitude Deep Penetration – LADP; Low Altitude Long Endurance – LALE; Medium Altitude Long Endurance – MALE), with the upper limit of 1,500 kg, a range of 500 m or higher, cruising altitude of 14,000 m, and a flying time of 48 hours. Strategic level UASs entail the categories High Altitude Long Endurance (HALE) and Unmanned (or uninhabited) Combat Air Vehicle (UCAV) (12,500 kg, a range of 2,000 km or higher, cruising altitude of 20,000 m and a flying time of 48 hours), while the group of special purpose equipment features the combat Lethal (LETH) and Decoy (DEC) UAVs. [23] [24] [25] [26] In terms of Hungarian use, the lower five categories of tactical level are potentially relevant for public service uses.

A further potential basis of classification is: structure (fixed wing, rotary wing, hybrid), engine type (piston, gas turbine, electric), method of control (remote control, programmed, combined), method of launching, and landing or purpose. [23] Figure 4 shows a generally accepted classification.

Based on the trends emerging in the last five years, it can be stated that due to the development of flight control systems, the share of multirotor constructions on the market of recreation equipment has drastically grown. This growth is induced by their beneficial features, and mostly their simple operation. The accurate GNSS receivers and modern complex sensor systems ensure unprecedented stability and excellent flying characteristics for such equipment. Automatic collision avoidance, obstacle avoidance, and emergency landing solutions significantly enhance the safety of operations, even for untrained operators. GIS-based flight planning and control systems, broadband radio frequencies (full High Definition [HD] video signals, telemetry, remote control), flexible flight parameters configurable during flight, the limitations and services, all offer an increasingly wide range of uses. With batteries available in commercial circulation, a flying time of more than 30 minutes is achievable, subject to volume, type of payload, method of use (such as increased speed, continuous UHD video capture) and environmental factors (wind). Depending on financial limitations, users are free to choose a 6-, 8-, or even a 12-rotor UAV for a few thousand dollars, which are able to carry a 10–20–30 kg payload, [27] or continue flight and/or land with one or even more unserviceable rotors.

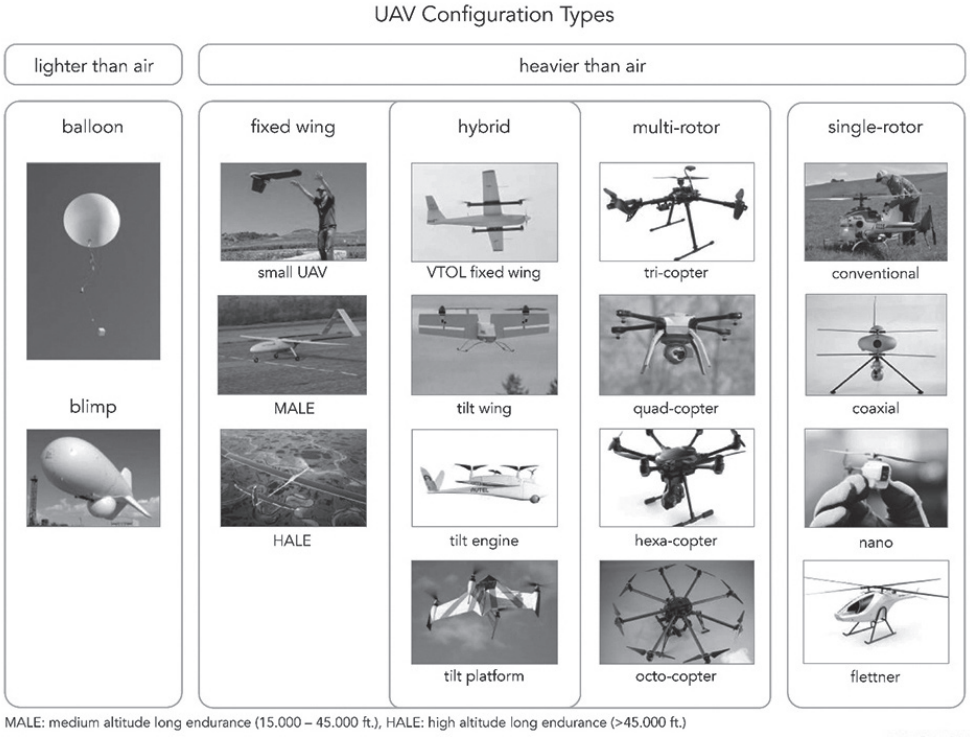


Figure 4. *UAV configuration types.* [28]

In this price category, flexibly configurable constructions are available that are optimized for the given task. They can carry ultra-zoom cameras, multispectral reconnaissance equipment, radio relays, decoys, transportation containers, or even battery blocks to extend flying time.

The use of electric multicopters is supported by the fact that take-off and landing is done vertically, and does not require a special launching pad or lengthy preparation, while also being low-maintenance. They reach cruising altitude at an even 5–10 m/s climbing rate, which combined with a low noise level allows for stealth, even from a few hundred meters of altitude and/or distance.

At the same time, fixed solutions exist that allow for an unsupervised and permanent presence at an altitude of 80–100 m, even for hours [29] or days, with only one launch. In addition to the cumbersome and expensive balloon-based solutions, it can provide an option for law-enforcement where the task involves infrared surveillance of longer river or border segments, provision of relay services above an area uncovered by communication services, or monitoring of mass events, festivals, or objects.

Moving on to the possibilities of public functions, the following reasoning proved to be practical: the government tasking system laid down in the applicable Hungarian law and the organizational structure responsible for the execution of such tasks, shall always efficiently respond to the challenges of the era and to arising security threats. The equipment system used to carry out these shall always be based on the services provided by the latest technologies,

methods and procedures. Based on the above requirements, public service use of drones is obvious, and is in line with international trends. At the same time, considering the forecasted volume of this market and the scale of future uses, handling of this field shall be escalated to a strategic level to provide government players with a customized equipment fleet at all times. Analysing the features of UAS categories, it can be established that except for a few special applications—for example long-range reconnaissance or military cartography, or air defence decoy missions, highway monitoring or firefighting—due to their positive features, it is practical to focus on multicopters. Multicopters are able to rapidly change directions and positions, hover over one spot, or follow moving targets. Thus, they can be put to good use in urban or other complex environments. They are capable of operating without emissions or other harmful effects, and with negligible noise volume, which ensures that such operations remain stealthy. These characteristics are of a universal and great importance. Yet, they are mostly appreciated for their policing, national security, or environmental protection uses.

In the task system of law enforcement, the use of drones could be very practical and efficient. [30] In crime prevention, patrol over endangered areas can reduce the risk of crime, while for crimes already committed, investigation can be supported by drones. At the same time, there are various arguments for the use of drones for crime or accident scene investigations, or other investigations, evidencing procedures, or covert data collection. Further potential areas of use are various police operations, securing venues or events, deployment of troops, preparation of raids, or the border patrol or oversight functions mentioned earlier, and the complex task system of combating illegal immigration and human trafficking. In connection with this, the circle of users is expanded to the staff of the Counter Terrorism Centre, who play an important role in combating terrorism. In the future, the equipment system could be expanded by ultra-small size UAVs for indoor flights for, for example, reconnaissance in closed areas prior to freeing hostages, for diverting attention during the operation itself, for carrying communication devices or other equipment preserving the lives of hostages in the closed area, or for remotely launching smoke grenades. The task system of some units of the National Tax and Customs Administration are similar to these activities, thus similar uses are also within our scope. Important tasks in prisons could be to secure such institutes against escape, prevent transportation of illegal objects into the building, or monitor the working sites outside of the facility. In the future, such tasks could be supported by drones for enhanced efficiency.

Possibilities of using UAS solutions for a wide spectrum of operations open up in the fields of disaster prevention and response, and the associated firefighting, industrial security and civil protection and water-related activities. [31] [32] In addition to reconnaissance, security and search and rescue tasks, UASs can be used for several other special purposes during activities in connection with nuclear or industrial accidents, accidents involving hazardous cargo transport, forest fires, or mass traffic accidents. For example, searching for sources of fire, analysis of fire spread parameters, evaluation of the condition of dams, filtering risk factors, use of firefighting containers, release of neutralizing material, or evaluation of the conditions of infrastructure elements and networks.

As for the support of authority tasks, the potential areas for UAS use would be environment protection and animal and forest management, or uses associated with local government work. In the former case, it is worth mentioning cost-efficient assessment of swamp areas or flooded areas that are otherwise difficult to access, protection of the borders

of protected areas, for example in the vicinity of cultivated lands via photometric comparison of photos captured during programmed flights. [32] The use of drones has the potential to offer efficient remote control solution for combating a wide range of unlawful activities, such as depositing waste, wastewater handling, campfires or timber mining, hunting, fishing, or other environmentally damaging activities. It can also be used to observe the movement of animal herds, count their population, or observe natural habitats without considerable disturbance of the environment. In urban areas, to verify compliance with the requirements of the construction authority or reconnaissance of illegal constructions, to prepare energy-efficiency assessments, even verification of heating systems operating with fossil-based or other fuel in winter (emission-level). Over industrial areas or dangerous facilities, deploying chemical, biological, or optical sensor systems would facilitate verification of compliance with permitted emission-levels, both regularly and randomly. Images captured by drones and the electronic measurement reports can serve as evidence in criminal procedures. In the field of frequency management, drones can prove useful in finding and identifying unauthorized radio frequencies. Multicopters can penetrate dangerous, otherwise inaccessible areas, while carrying special payloads to carry out chemical or physical sampling with low risk.

Though the above list is not complete, it clearly shows the unbelievably wide range of non-military use UASs are offering. In connection with the issue of usability, it should be noted that the emphasis is nowadays shifting from the carrier platform to payloads and the automated processing of real time information they produce, thus governments should also put more emphasis on these factors. Establishment and updating of categories of individual task systems, and the associated technical requirement system, is a more complex task than it appears at first. For Hungarian circumstances, almost all deployed versions have to fit in the weight category comprising UAVs below 150 kg, but with compromises and with the continuous development of such equipment, this weight limitation can even be reduced to 25 kg. One consideration has to be applied by all means, namely that efficient execution of the government's task system is based on the close cooperation between bodies, which also affects the use of UAV systems. Therefore, cooperation during the establishment of categories is paramount.

Summary

Based on both the military and commercial purpose forecasts, the next decades will bring about a widespread use of unmanned aerial vehicles. In addition to military applications, this growth will be propelled by other government and public service uses, along with the expansion of industrial uses associated with strategic industries (energy).

However, due to the exponential and complex technical development processes (e.g. increased autonomy levels, use of collective group intelligence), costly military developments (and not only in this field) are gradually losing their technological benefits, and demands are growing for the adaptation and integration of cost-efficient civilian technology and equipment.

In order for government players to keep up with these processes, a drastic change of view and concepts is necessary, allowing significantly greater flexibility and cooperation between stakeholders. The long-term solution should be presented by a system of associations,

which is based on a broad scale cooperation bringing strategic level users, industrial and other market players, authority bodies and university research workshops, on a mutual and unified national platform. This "Unmanned Aircraft Systems Information, Support, Knowledge and Education Center" would mean not only a formal cooperation, but would present us with a strategic, planning, decision-preparation and development organization that handles associated legal and technical issues as a complex problem, considering the needs of government users (defence, law enforcement, disaster response). A "testbed", an experimental platform, would be created under the auspices of the Center, allowing industrial stakeholders to promptly examine their latest developments, free of significant administrative burdens. It would also facilitate integration of individual subsystems and continuous testing of equipment. The same platform would give room to carry out experiments necessary for the authorization processes associated with authority activities. The centre's workshops would also establish the guidelines and priorities of the "National Drone Strategy", laying down the basic framework for future developments.

To support developments, an extensive central database and the associated multi-level decision preparation system would be set up, which includes all complete UASs available on the market, with their technical parameters, flying characteristics, and ownership and supplier backgrounds. Additionally, it would feature the latest information about international developments, available modules for each subsystem (autopilot, batteries, engines, sensors, communication systems, airframes, etc.), with all physical parameters, characteristics, limitations, and other supplementary data. When entering filter conditions in a special search engine, it will offer solution alternatives for the individual components or the complex system, just like an online catalogue, assessing relevance.

This solution would support customers in laying down the realistic requirements towards the UAS to be used for the given purpose, while developers would be able to choose the most efficient technical solution.

This same organization would also lay down the technical requirements and realize an experimental system of a high autonomy traffic management and traffic control, facilitating the safe management of, for example, an urban drone airspace. The principle would be based on radio communication between UASs, transmitting their identifiers and telemetric data to the system's regional processing center, following each equipment and estimating their trajectories. To avoid emergencies (running out of battery power, malfunctions, or collisions), the system would be able to intervene in the control of individual equipment (e.g. avoidance manoeuvers, stop and hover, land), considering their priority levels (for example government, commercial, recreational use), their type (fixed wing or rotary wing), and their flying characteristics. Such solutions would of course require a substantial infrastructure (radio stations, emergency landing strips, meteorological stations), a standardized UAS equipment fleet, and communication protocols. But in the light of current development trends, this might be necessary within a few decades, provided we intend to exploit the opportunities UASs offer.

References

[1] The Drones Report: Market forecasts, regulatory barriers, top vendors, and leading commercial applications. *Business Insider Intelligence*, 10.06.2016. www.businessinsider.com/uav-or-commercial-drone-market-forecast-2015-2 (Downloaded: 10.10.2017)

[2] TOSCANO, M.: *Global Aerial Drone Market.* Teal Group, BI Intelligence Estimates. s.d. https://static.businessinsider.com/image/54ad8f0269bedd7078ba7175/image.jpg (Downloaded: 02.03.2018)

[3] Unmanned Aerial Vehicle (UAV) Market by Application, Class, System (UAV Platforms, UAV Payloads, UAV GCS, UAV Data Links, UAV Launch and Recovery Systems), UAV Type, Mode of Operation, Range, Point of Sale, MTOW, and Region – Global Forecast to 2025. *Research and Markets*, February 2018. www.researchandmarkets.com/publication/mquzwge/4464352 (Downloaded: 06.06.2018)

[4] *Unmanned Aircraft Systems (UAS).* International Civil Aviation Organization, AN/190 (2011). www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf (Downloaded: 31.12.2018)

[5] Drone, UAV, UAS, RPA or RPAS… *AltiGator* (online), s.d. http://altigator.com/drone-uav-uas-rpa-or-rpas/ (Downloaded: 31.12.2018)

[6] Tudományági nómenklatúra. Budapest: Magyar Tudományos Akadémia, Doktori Tanács, 2017. http://mta.hu/doktori-tanacs/tudomanyagi-nomenklatura-106809 (Downloaded: 07.06.2018)

[7] *Aircraft Platforms.* www.ga-asi.com/aircraft-platforms (Downloaded: 07.05.2018)

[8] *RQ-4 Global Hawk.* www.military.com/equipment/rq-4-global-hawk (Downloaded: 07.05.2018)

[9] *Predator RQ-1 / MQ-1 / MQ-9 Reaper UAV.* www.airforce-technology.com/projects/predator-uav/ (Downloaded: 07.05.2018)

[10] IONESCU, A. M.: Nanotechnology and Global Security. *Connections*, 15 2 (2016), 31–47. www.jstor.org/stable/26326438 (Downloaded: 03.04.2018)

[11] TIWARI, A.: Military nanotechnology. *International Journal of Engineering Science & Advanced Technology (IJESAT)*, 2 4 (2012), 825–830. http://ijesat.org/Volumes/2012_Vol_02_Iss_04/IJESAT_2012_02_04_09.pdf (Downloaded: 03.11.2017)

[12] JUN, L., ZONGHAI, C., ZIFENG, M., FENG, P., CURTISS, L. A., AMINE, K.: The role of nanotechnology in the development of battery materials for electric vehicles. *Nature Nanotechnology*, 11 (2016), 1031–1038.

[13] CHEE, L. C., KAH, F. L.: 3D printing and additive manufacturing: principles and applications (Fifth Edition of Rapid Prototyping). *Nanyang Technological University*, (2017), 272–278.

[14] KOSLOW, T.: Pentagon to Deploy 3D Printed Mini-Drone Swarms for Surveillance and Attacks. *3Dprint.com*, (2016). https://3dprint.com/153572/pentagon-mini-drone-swarm/ (Downloaded: 07.05.2018)

[15] PARPINELLI, R. S., LOPES, H. S.: New inspirations in swarm intelligence: a survey. *International Journal of Bio-Inspired Computation*, 3 1 (2011), 1–16.

[16] BÜRKLE, A., SEGOR, F., KOLLMANN, M.: Towards Autonomous Micro UAV Swarms. *Journal of Intelligent & Robotic Systems*, 11 1–4 (2011), 339–353.

[17] FASANO, G., ACCARDO, D., MOCCIA, A., CARBONE, C., CINIGLIO, U., CORRARO, F., LUONGO, S.: Multi-Sensor-Based Fully Autonomous Non-Cooperative Collision Avoidance System for Unmanned Air Vehicles. *Journal of Aerospace Computing, Information, and Communication*, 5 10 (2008), 338–360.

[18] MIKÓ, GY., NÉMETH, A.: SCFDM based communication system for UAV applications. In. *"Radioelektronika". 25th International Conference*, (2015), 222–224.

[19] SABATINI, R., MOORE, T., HILL, C., RAMASAMY, S.: Assessing avionics-based GNSS integrity augmentation performance in UAS mission- and safety-critical tasks. In. *International Conference on Unmanned Aircraft Systems (ICUAS)*, 9–12 June 2015. 157–166.

[20] MANGIAMELI, M., MUSCATO, G., MUSSUMECCI, G., MILAZZO, C.: A GIS application for UAV flight planning. *IFAC Proceedings Volumes*, 46 30 (2013), 147–151.

[21] GEOSYSTEM GmbH: Processing, cataloguing and distribution of UAS images in near real time. *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, XL–1/W2 (2013), 339–342.

[22] VERSTRATETE, D., LEHMKUEHLER, K., GONG, A., HARVEY, J. R., BRIAN, G., PALMER, J. R.: Characterisation of a hybrid, fuel-cell-based propulsion system for small unmanned aircraft. *Journal of Power Sources*, 250 (2014), 204–211.

[23] BÉKÉSI B.: Pilóta nélküli légijárművek jellemzése, osztályozásuk. In. PALIK M. (szerk.): *Pilóta nélküli repülés profiknak és amatőröknek*. 2. jav. kiad. Budapest: Nemzeti Közszolgálati Egyetem, 2013. 65–109.

[24] *U.S. Army Unmanned Aircraft Systems Roadmap 2010–2035.* www.rucker.army.mil/usaace/uas/US%20Army%20UAS%20RoadMap%202010%202035.pdf (Downloaded: 10.11.2017)

[25] CROUCH, C. C.: Integration of mini-UAV at the tactical operations level: implications of operations, implementation, and information sharing. Monterey: Naval Postgraduate School, 2005. www.e-education.psu.edu/geog892/sites/www.e-education.psu.edu.geog892/files/Collier_Crouch_thesis_a435680.pdf (Downloaded: 15.02.2018)

[26] WATTS, A. C., AMBROSIA, V. G., HINKLEY, E. A.: Unmanned Aircraft Systems in Remote Sensing and Scientific Research: Classification and Considerations of Use. *Remote Sensing*, 4 (2012), 1671–1692.

[27] *Top 10 Heavy Lift Drones.* https://filmora.wondershare.com/drones/top-heavy-lift-drones.html 2018 (Downloaded: 10.06.2018)

[28] *UAV Configuration Types.* Drone Industry Insights, 2016. www.droneii.com/wp-content/uploads/2016/06/UAV-platform-configurations-compr.png (Downloaded: 10.09.2017)

[29] *Vezetékes táplálású drón.* Rotors & Cams, s.d. https://rotorsandcams.com/drotosdron/ (Downloaded: 05.06.2018)

[30] PETRÉTEI D.: A drónok kriminál technikai és rendészeti felhasználása. *Magyar Bűnüldöző*, VI 1–3 (2015), 70–81.

[31] BODNÁR, L., RESTÁS, Á., QIANG, X.: Conceptual Approach of Measuring the Professional and Economic Effectiveness of Drone Applications Supporting Forest Fire Management. *Procedia Engineering*, 211 (2018), 8–17.

[32] RESTÁS Á.: Az UAV közszolgálati alkalmazásai. In. PALIK M. (szerk.): *Pilóta nélküli repülés profiknak és amatőröknek*. 2. jav. kiad. Budapest: Nemzeti Közszolgálati Egyetem, 2013. 241–280.

AARMS Vol. 17, No. 3 (2018) 165–170.

Roadblock: Is it an Effective Tool Against a Car Bomb?

The History of Road-Blocking

Luděk RAK[1]

This article serves as a short preview to the history of roadblocks (road obstacles), and also as an outlook to modern and future technologies, and challenges they face in this particular field of science. At this moment, it is a real problem to stop the car immediately (if possible), before it causes damages, or threats any civil or military objects. It does not necessarily have to be only an accident, it can be a terrorist attack, which can cause enormous collateral damage and also life losses. The contemporary problem is not only the combat with fire explosive systems, but it is also important to focus on avoiding damaging of important devices, road objects or spots called "soft targets". All this combined presents the essential challenge for roadblocks development.

Keywords: *roadblock, car bomb, soft target*

The history of road-blocking dates back to the times of the Roman Empire expansion, and is associated with its quickly spreading road network. During the existence of ancient Rome, 80,000 km [7] of paved roads and over 400,000 km of roads in total were constructed. The roads were supplemented with numerous structures, bridges and viaducts, the formation line led in side-hill cuttings and trenches, and the roadbed comprised several layers. The layers, methods of construction and the width of the roads were prescribed by law. As basically all Western Europe, the Mediterranean, and the Near East were linked, road security became an issue. Roadblocks were rarely used then, only in frays and combats. Protection more often consisted of the construction of fortification objects on access roads or the roads themselves. On crossroads, villages were founded that were gradually fortified. Where the Roman dominion lasted longer, wooden palisades were turned into stone walls. In border areas, military garrisons were maintained, and the roads passed by fortified buildings—later called "Limes Romanus".

As the roads could easily be bypassed, road obstacles were not considered practical. In addition, the roads were mainly used for driving cattle and carts or by military units and horsemen. This belief, however, proved false in the late Roman Empire as Teutonic tribes used the roads to move rapidly between provinces raiding various places.

After the fall of Rome, the quality of roads and the highly developed art of constructing and engineering declined. In the following centuries, the transport among newly established feudal states was conducted using the remainders of the Roman roads and mostly earth trade roads. At that time, road obstacles mainly had the form of abatis due to dense forests. In the Czech lands, several cases, when enemy forces were directed, using abatises, to places convenient for the defenders (compare with source [1]), were documented. In mountainous

[1] Ph.D., Captain, assistant professor, Department of Tactics University of Defence; e-mail: ludek.rak@nob.cz

border areas, felled trees (cut at the height of approx. 1 m), mutually stuck and not completely separated from the stumps, meant a significant obstacle for the attacker's movement. Hence, the enemy could only attack along the trade routes, which were protected by lines of fortified settlements, later castles. (A modified variant of this non-demolishing obstacle is used even today.)

All along the history of medieval warfare, both temporary and permanent military organisations were established, whose purpose was to construct roads for carts conveying military materials; these, however, were far from the quality of ancient road constructing.

Between the 15th and 17th century, the quality of road maintenance, construction of bridges and military engineer support improved in Russia first. In the 17th century, due to the transport boom and the invention of explosives other than gun powder, the rest of Europe followed. Only then was the ancient standard of road construction overcome. The need for movement of large military units across Europe led to the establishment of forces dealing with both the construction and the destruction of roads and bridges. Permanent fortifications and bastion forts proved to be inefficient (Franco–Prussian War in 1871), and armies were forced to increasingly manoeuvre, which could be prevented using suitably located obstacles mainly on roads. Also, first fougasses, i.e. predecessors of mines and the first efficient representatives of a later very large group of demolishing obstacles, occurred (Russo–Turkish War 1828–1829). Compare with source [6]. Their massive development came in the late 19th century due to the invention of dynamite and the establishment of factories producing the dynamite, blasting and ammonium nitrate gelatines, burning fuses, explosives and the explosive most important in military terms—Trinitrotoluene (TNT). [8] The use of non-demolishing obstacles boomed during World War I, when road-blocking became one of the crucial engineering tasks. Barbed wire in combination with wooden poles, electric barriers, concertina wires or Czech hedgehogs became the commonly used non-demolishing obstacles that were not only placed between trenches, but were also used for road-blocking on a large scale. The extent of road destruction was classified as:

- demolition—the engineering forces destroyed a line of communication including road structures in order to render the road unserviceable for a certain period of time. After bridges had been demolished by full demolition section, supporting and retaining walls had been destructed, and craters had been placed on roads, it took weeks or even months to restore the road.
- interruption—meant the destruction of minor road structures, damaging of the road formation. The consequences could be remedied within hours or days.

Moreover, abatis, stone barricades, or jammed vehicles with dismounted wheels were still used as barriers.

For the personnel destruction so-called underground torpedoes were mainly used, which were initiated by means of an electric detonator (compare with source [1]), (e.g. Russo–Japanese–War 1904–1905). These were used as separate barriers in the terrain, or as roadblocks preventing the enemy from conveying the ever-heavier cannons, ammunition and other materials. After World War I, anti-tank and anti-personnel mines became one of the main types of demolition obstacles. The first improvised anti-tank mines were introduced around 1917 in the form of artillery ammunition and boxes filled with explosives hidden underground. The charges were usually activated using a hand grenade placed on the top.

The fact that "5,500 km of roads, more than 1,000 bridges and viaducts and 1,000 km of railroads were destroyed" [1: 12] using explosives during the German army retreat shows the extent of the use of demolition obstacles in World War I.

The construction of permanent fortification structures in the inter-war era meant another stage of significant development of non-demolishing obstacles. Forts and strong points were interconnected using wide systems of non-demolishing obstacles in the form of either anti-personnel obstacles—steel needles with the bases embedded in concrete and interconnected by barbed wire—or anti-tank obstacles—Czech hedgehogs, anti-tank ditches. Roads in border areas were blocked using solid reinforced concrete barriers, and were also guarded by weapons placed in the fort casemates. The trend of heavy fortification structures construction is still apparent at the remainders of Mannerheim, Maginot, so-called Stalin line, Czechoslovak border-area fortification line etc. The demolition obstacles also went through a considerable development. There were two specifically separated ways of anti-tank and anti-personnel mines development, in consequence of which the mines became resistant to removal, i.e. the inventing and upgrading of so-called anti-personnel bounding mine, which exploded after clearing from the casing, and hard-to-remove non-metal mines continued during World War II and afterwards.

When the benefits of forts proved to be considerably limited with regard to the modern tactics, the development of non-demolishing obstacles began to stagnate. In particular, after World War II, modern influence mines were developed, which were gradually fitted with specific functions using electronics. Non-demolishing obstacles, which had been originally developed for purely military purposes, started to be used in the civil sector due to a growing amount of road transportation and in order to increase road safety. Obstacles, that were to prevent the use of roads, have turned into safety elements aiming to keep a crashing car on the road and reduce the loss to property and lives. Today, crash barriers, shock absorbers [2] and further road equipment must comply with strict standards, and various types of obstacles are particularly important in the field of road safety. Unfortunately, the development of efficient military roadblocks has almost ceased recently, and older types of roadblocks are only being modified. What is more, the obstacles used by the police are usually incapable of stopping a vehicle immediately.

Only the current operations in Afghanistan, Syria and Iraq are proving that the absence of road block development poses a considerable risk in terms of protection against Vehicle-Borne Improvised Explosive Device (VBIED). "A device placed or fabricated in an improvised manner on a vehicle incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. Otherwise known as a car bomb or VBIED." [9: GL-11] For requirement this article only in self-propelled vehicle, which attacked with momentum of mobility and explosive impact (or other lethal possibility).

According to the statistics, the VBIED is the fifth (compare with source [5]) most common method of terrorist attacks in asymmetric operations worldwide. The lack of effective defence makes the terrorist targets quite vulnerable, and accelerated development or the used road elements seem inefficient. (Compare with source [4].)

The use of demolishing obstacles is unjustifiable due to the risk of collateral losses. Furthermore, it cannot be identified in advance, if a moving car diverting from its direction has become a tool of a terrorist attack, or it is an ordinary car accident caused by e.g.

a driver's acute health problem. Using explosives in that case would be rather inhuman. In addition, maintaining a functional system of demolishing obstacles around a soft target is a utopian and unrealistic concept that means a threat rather than protection.

The non-demolishing obstacles appear to be more appropriate in this case. Yet, today's society pays dearly in a number of incidents of this type all over Europe for having neglected the development of non-demolishing obstacles.

In the worldwide context, the VBIED attacks in Europe have been conducted in an inefficient manner. The terrorists only made use of the kinetic energy of moving vehicles in a "crowd" of people, their acting was not coherent enough, and they had not preselected the locations of their attacks at all, or very randomly. It can be said that if they use explosives in the future, armour their vehicles to secure them against small arms at the minimum, or drive the vehicles using remote control units, the number of casualties will grow dramatically, unless the attack is stopped efficiently. Furthermore, it is clear that the terrorists are capable of producing and using explosive charges even in Europe, as for example in Paris, France close to the "Stade de France" stadium on 15 November, 2015.

In order to prevent such attacks, the process of VBIED preparation must be interfered with, which means the intelligence service shall be involved from the very start, and the police shall conduct their investigation through all stages of the process. All this effort, however, might prove inefficient when it comes to preventing an isolated attack. For that reason, threatened locations of soft targets must be protected using effective non-demolishing obstacles. Due to a great number of soft targets, the obstacles must be cheap, easily transportable, and must have at least partial absorbability as the scatter of splinters during an explosion and their damaging effect is the general substance of the attack. In particular, the ability to stop a vehicle as soon as possible, and the absorbability of the material fragments scattered by an explosive form the limit of survival within the perimeter of the target under attack.

A theoretical chance of an uncovered person standing in an open terrain of surviving a blast wave without the primary and secondary splinters effect is expressed as follows:

$r = K(m).\sqrt[3]{Q}$; (compare with source [3])

- r—radius from the exploding charge, beyond which the eventuality given by the critical factor K(m) occurs;
- $K(m)$—the critical factor of a person's survival 10; for civil buildings the critical factor of destruction is set to 70, etc.;
- Q—the TNT equivalent of the exploding charge in kg.

Example: When a charge of 10 kg TNT equivalent explodes, the blast wave lethal radius is 21 m from the epicentre of the explosion.

Should the obstacle fail to catch the splinters, the zone of lethal effect due to the splinters penetrating targets would expand to:

$R_{(f)} = 109.62 \times Q^{0,164}$ [compare with source (3)]

- $R_{(f)}$—Hazardous Fragmentation Distance Range (m);
- Q—the TNT equivalent of the exploding charge in kg.

Considering the above-described case, the distance would be 159 m.

Hence, even partial absorbability increases the chance of survival within a soft target by more than seven times. The protection against the effects of a blast wave grows considerably with the distance, at which the vehicle is stopped. If, in the case described above, the vehicle is stopped at the target area perimeter at the distance from its centre equal to the radius of destruction, the areal impact on a target area having the size of 2*r* will decrease to less than 40%. An explosion within the target would destroy 80% of the area. Thus, with 100 people evenly distributed within a target having the area of 2*r,* only half of the people would be killed by the blast wave effect if compared to an explosion at the target centre.

On these grounds, a specific research is being conducted at the University of Defence, Brno (UNOB) aimed to come up with a project of a non-demolishing obstacle preventing a VBIED attack and to verify its feasibility. The input conditions comprise simple construction, high resistance to VBIED, low price, good transportability and variability. At this stage, steel has been selected as the basic material; in the future, it will be replaced with modern composite armoured plastic. The core of the obstacle is formed by wire ropes with excellent toughness when catching a vehicle and high tearing strength.

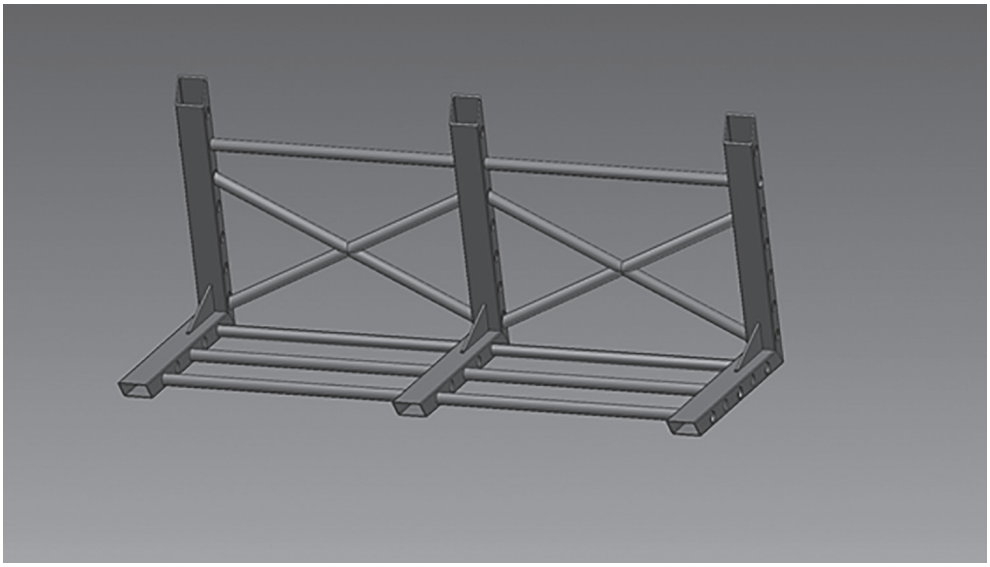


Figure 1. *Anti VBIED Obstacle developed by the University of Defence.*
[Edited by the author.]

References

[1] DOLEZAL, L., KROUPA, L.: *Ženijní vojsko, historie a současnost*. Praha: Ministerstvo obrany ČR, 2003.

[2] STRIEGLER, R.: *Řešení kritických míst na pozemních komunikacích v extravilánu.* Brno: Centrum dopravního výzkumu, 2013.

[3] *Explosive ordnance disposal procedures (FM60A–1–1–4). Tech. Manual*, US ARMY, 2003.

[4] Can concrete barriers protect against truck attacks? Germans stage crash test to find out. *RT Question More (online)*, 22. 03. 2017 www.rt.com/news/384461-truck-attacks-concrete-test/ (Downloaded: 20.11.2017)

[5] *Intercenter.com*, 18.01.2017. https://intelcenter.com/icd/ / (Downloaded: 18.11.2017)

[6] ŠEVČUK, M. K.: *Zdolávání zátarasů.* Praha: Naše Vojsko, 1956.

[7] KUCERA, V.: *Architektura inženýrských staveb.* Praha: Grada Publishing, 2011.

[8] AKHAVAN, J.: *The chemistry of explosives.* 2nd Edition. Cambridge: Royal Society of Chemistry, 2015.

[9] NATO: *Joint Security Operations in Theater (JP-3-10).* NATO Standardization Office, 2006. www.bits.de/NRANEU/others/jp-doctrine/jp3_10%2806%29.pdf (Downloaded: 30.01.2018)

AARMS Vol. 17, No. 3 (2018) 171–188.

Seven Pieces of Advice to Improve Your Information Security

Best Practices from the Enterprise's Point of View[1]

Gergely SZENTGÁLI[2]

Establishing and operating an effective information security management system within an organization is never an easy job. Organizational culture, management support, budget restrictions and many other factors affect the security efforts of a company. Although the information security academic literature is growing, there is no clear guidance in several fields of the topic, therefore the life-tested best practices can be a useful aid in operating such systems. The aim of this paper is to provide a short guidance regarding the basic steps of a beginner information security manager, and maybe to give some useful thoughts to the experienced officers, as well.

Keywords: *information security, ISMS, cyber security, risk, incident, management*

Introduction

Information security practices and methodologies are evolving every day. The threat environment is constantly changing, forcing the companies and security professionals to learn, improve and adapt. There may be a lot of differences between the public and private sector, still I believe that the following information security practices can be used on both sides. In the following, I am going to introduce seven pieces of advice regarding information security which are coming from my managerial and auditor experience, serving as a guidance for a minimum standard what every information security manager should do in order to improve their organizational defence capability, and to review their taken steps to achieve this goal.

Don't be a Lone Wolf: Gain Management Support

Supporting and auditing companies worldwide, my experience was that the common reason of failed information security management systems (ISMS) was the lack of senior management support. Information security managers who are trying to build and operate ISMS without management sponsorship will find themselves alone. However, gaining

[1] Edited version of a presentation in *Cyber Security in Public Sector* international scientific conference.

[2] Information Security Manager, IT Services Hungary; e-mail: gergely.szentgali@t-systems.com

the management's approval is not easy: the information security manager has to make the board understand why security is so important.

The members of the leadership of companies talk a unique language, the IT jargon should be avoided if you communicate to them. The regular root cause of miscommunication is that the members of the senior management are usually not IT experts, and the security manager is not a business leader. It is not easy to bridge the gap between the strategic priorities and day-to-day operational governance concerns: the board is focusing on brand reputation, financial revenue and business objectives, whereas the (security) governance is dealing with daily challenges. [1] Therefore, in order to fill this gap, one of the mandatory elements of the General Data Protection Regulation (GDPR) is the basic information security education of the board members. [2]

Using a business case, including cost and benefits (not just financial), to present your ideas is always a good choice. Let them know that the IT and the information security itself are serving the business, and your goals are always aligned with the objectives of the business.

To achieve success, you have to involve the proper stakeholders: explore and draw your stakeholder map, get familiar all the "players" within your organization. Involvement has many aspects: organize steering committees, security meetings and maintain reporting channels. With a well-established relationship between the board members and the information security manager, many security incidents can be prevented and the budget of the security program can be secured year by year.

Know Your Next Steps: Implement a Security Strategy and Governance

Knowing that the management supports your efforts, you should have a vision and a structure to achieve your goals. Without a clear target, even a brilliant strategy will fail. Creating an information security strategy will guide you and your employees regarding how to achieve the desired state. Be realistic, set up accountable, and—maybe it is the most important—measurable goals. Use key performance indicators (KPIs) in order to track your progress.

The well-established governance structure comes from a proper strategy and the connecting policy. Compliance to the policy and policy changes is always a challenge. Employees resist changes in most cases, and this noncompliance results security risk. An information security policy should be enforceable, but still, the communication and popularity of the security policy has to be the cornerstone of the ISMS: a positive attitude toward a mandatory security change leads to greater intention to comply. [3]

Regarding the governance structure, build up information security roles depend on the size of your organization, such as Chief Information Security Officer (CISO), Business Continuity Manager, Chief Data Privacy Officer, security administrators, and so forth. Due to the defined roles, accountability and separation of duties come true, and it will be also helpful to create and maintain escalation channels. Through the identifying the process and data owners, proper asset classification and the level of the linked controls can be successfully determined.

The information security governance system should be led by the CISO who is ideally directly reports to the Chief Executive Officer. In some cases, the Chief Information Officer can be the direct supervisor of the CISO. A well-trained and experienced information security team is important in such structure, and operates as a consultancy and guidance point for the business. To achieve this goal, the team should be visible and reachable from the business functions, what can be done if information security is a respected value and priority of the organization. [4] A well-built information security management system is transparent, hierarchical, understandable and executable for every employee.

During building up your governance system, do not be afraid to use international standards and best practices. You do not have to reinvent the wheel, there are several good solutions what you can use. For an example, ISO 27001 standard[3] [5] is a cornerstone of today's ISMS, supported by many others, such as ISO 22301 for business continuity management, [7] or ISO 31000 for risk management. [8] One of the biggest advantages of using an international standard is that your organization can be audited and certified. This is a clear statement for the outside world, and also can be a contract requirement from the customer's side. Regarding IT service management, besides ISO 20000, [9] ITIL [10] can be a reliable source, even only some part of it: if your organization is focusing on IT system operation and you are facing budget restrictions, than implement just the operation phase of the IT service lifecycle.

See the Big Picture: Use a Tool

A tool, which here means a software, can make the information security manager's life easier with providing dashboards, tracking status, maturity level, etc. With a universal product, you are able to manage your audits and track the findings; record the results of risk assessments; perform a business impact analysis; set up a strategic program management and many more.

The IT security market is growing, and new products appear every day. Besides antivirus programs, firewalls, intrusion prevention and detection systems—information security management software should be also the part of a security management's portfolio. Since every organization is different, the tuning and tailoring capability (e.g. self-releasing) should be a primary condition of such product.

The reports produced with this tool can be a status snapshot, identifying the strengths and weaknesses, and also fits for audit purposes: the internal or external auditor can get a picture quickly on the organization's maturity and compliance compared to the chosen standard. In the age of GDPR, this capability will worth to invest in, but will be helpful for those who are out of the GDPR's scope, as well. The senior management can also require risk management status, or compliance reports.

As an example, Figure 1 shows a spider graph regarding an organization's ISO 27001 maturity and compliance.

[3] The number of ISO 27001 certified entities is growing every year, in 2017 more than 39,000 organizations were holding this certificate. [6]

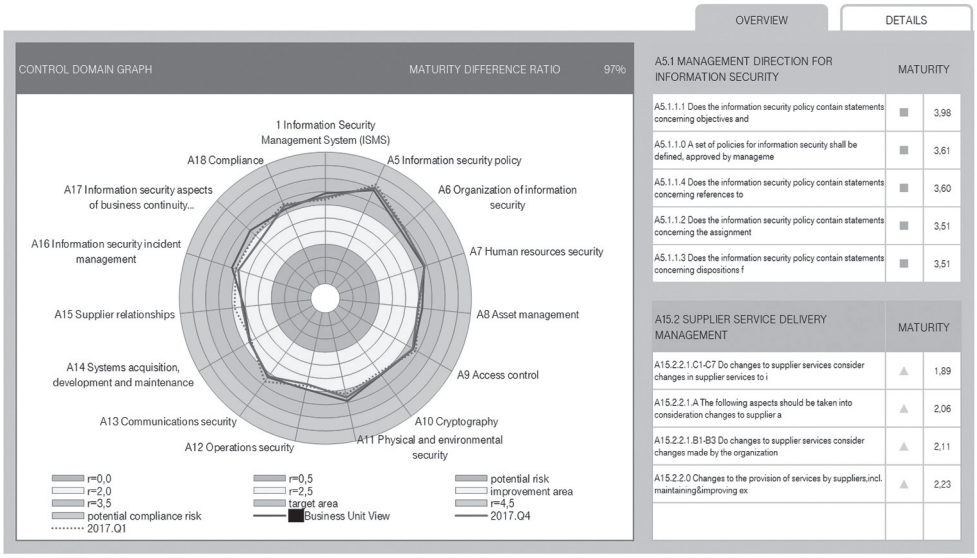


Figure 1. *Spider graph of ISO 27001 maturity with the highlight of the strongest and weakest fields.* (Screenshot by the author from [11].)

This spider graph is made with a few clicks, and operates perfectly for showing the current status of ISO 27001 compliance. The graph can be created for every international standard, or even customer requirements which are uploaded in the system as a control assessment.

Focus on the Whole Lifecycle of Risks and Incidents: Tracking is the Key

Performing risk assessments periodically is one of the basic tasks of an information security manager. Exploring the new threats is the first thing to do in preparation for protecting the organization's information assets. As in so many other cases, there are no new tricks on the field of risk management, as well—you have to follow the classic lifecycle: identification, analysis, evaluation and treatment. [12] A tool—mentioned in the previous chapter—can be a useful ally regarding the tracking of your incidents and risks. This is a core point, because in several cases, the information manager is just opening the ticket, but does not manage it through, losing the possibility to see the big picture and find connections between events. It is also the information security manager's overall responsibility to maintain the risk and incident database.

Always give time for post-incident reviews. In most cases, after analysing the root cause, the risk can be eliminated and the incident can be closed for a lifetime. Involve the stakeholders, give time for a brainstorming in order to improve your security. Inform your management about the improvements and the current threat status. Always be honest, do not play with the numbers—transparency is a long-term basis of management sponsorship.

Get Comfortable with the Uncomfortable: Test Yourself and Be Prepared

Incident management is a core activity of information security management. The preparedness, response time and tools are vital parts of the survival capability of an organization. It may happen that your company's daily operation or even its reputation will depend on how good your readiness is.

As an information security officer, it is your responsibility to create, maintain and test your incident management plan and processes. You have to train your colleagues, test their knowledge and preparedness. Do not underestimate the utility of incident management exercises. Drills and regular tests will create reflexes which pay off in a stern situation.

Build up your own incident management team. Resourceful companies are able to operate a Computer Emergency Team (CERT) or a Security Operations Center (SOC), working in 24/7, employing IT security experts in shifts. But money cannot be an excuse: take your organization's head of IT operation and a technician from that department, an IT technician with security experience, somebody from the management (with the right to make decisions), a communication expert, train them, build up escalation channels and procedures, and your very own incident response team is ready. Of course, it will not be equal with an SOC or a CERT, but an information security manager has to adapt to the limits of the organization. You have to win the management for the cause because in the long run it will not be a solution due to the rising number of cyber-attacks, and the fact that lots of roles have to be shared among less people. [13]

Business continuity and disaster recovery strategies, plans and scenarios also should be tested on a regular basis. It does not matter if you are working for a bank or in the public sector, service outages can cause financial and reputational loss, and in some cases can escalate into a national security risk, as well. When the time comes, success will depend on your employees' preparedness. Just like on some other fields of information security, during the creation of these plans, the business (especially the business process owners) should be deeply involved since the requirements are coming from their side.

Communication and its channels are vital. In case of the public sector, it has to be a must to maintain an active dialogue between the organization and the Government Incident Response Team (GovCERT) since its basic task is the incident handling of central and local government agencies. [14] It is not only essential for the updated information, but to reach the GovCERT as quickly as possible in a case of a serious and/or high priority incident. Communication plays a central role in public relations (media, customers, etc.), your organization should be prepared for crisis communication: train appointed employees to communicate to the media in order to control the situation.

Strengthening the Human Factor: Security Awareness

It became a cliché, that the weakest link in information security is the human factor, the user itself: high percentage of successful attacks is starting with social engineering. Moreover—according to the IBM 2016 Cyber Security Intelligence Index [15]—60% of attacks came from the inside, showing clearly that insider threats continue to pose the most significant

risk to organizations.[4] Despite the international trend, employees believe information security attacks are external factors, therefore do not consider themselves a threat. [17]

A trained employee is the first line of defence in protecting the company's information assets. With a well-established awareness program, a person's awareness becomes a (preventive and detective) control. The goal of the awareness activities is to make the employees understand the importance and implications of information security, moreover the safe behaviour, aligned with the organizational information security policy. [18]

These kinds of trainings should be mandatory in online or in-door form. After you identified the needs and goals of your organization, create a steering committee to assist in planning, executing and maintaining the awareness program. The information security strategy will be a compass to understand the connection between awareness targets and business objectives. Shaping the awareness program, you should focus on four domains: people (the right employee in the right role), technology (up-to-date technology with implemented security features), processes (role-based and effective), and policies (clear and high-level statements). [19]

Tailor your training to your audience, use everyday examples for better understanding. In addition to trainings, there are many other practices for raising information security awareness: posters, intranet news, e-mail campaigns, etc.[5] The goal is to make the employees understand: security is not just a management issue, security is everybody's business. The final goal is to organize the quickest training possible that has the greatest impact on target groups. Use your employees and the awareness steering group to review your program at least annually.

The result of an awareness program should be tracked and tested on a regular basis. Controlled phishing campaign, fake calls and many other tests will prove the awareness level of the organization. After this, the information security manager has to communicate and explain the results for all the employees. In lessons learned sessions, they have to understand what would happen in a real-life situation. Facing the actual consequences is one of the best methodologies to shape a user's behaviour.

And Finally: Be Emphatic

Be emphatic, because sometimes security can be viewed as a burden: most of the employees consider security controls a nuisance and unwanted obligations. Every security officer knows the typical questions: "Why do I have to change my passwords again?" or "Why do I have to keep my desk clean?" Such questions usually lead to uncooperative attitude.

---

[4] Regarding insider threat we have to make difference between the malicious insiders and inadvertent actors. In the 2016 IBM report, behind the 44.5% of the 60% attacks were actors with malicious intent. However, in the latest, 2018 IBM X-Force Threat Intelligence Index [16] considers insider incidents as hot topic, as well. The report concludes that in the age of bring-your-own-device, everyone is an insider threat, and the errors of inadvertent employees (e.g. weak passwords, unsecured personal devices, etc.) could lead to serious security incidents.

[5] Alternative solutions can provide cost-optimized tools for smaller organizations. Being creative is the key regarding an awareness campaign. Focusing on such methodologies could change the current trend which shows that big size companies (with higher security budget) have higher awareness level, while the smaller ones have lower. [20]

The solution is the engagement: just like in case of the senior management, employees have to understand why security and their participation are important.

Starting from their first day at the office, employees should be trained regarding security. Help them with easy-to-understand materials, for example create a one-pager from your information security policy or rule base. As I stated before, employees' compliance to the security policy often fails, and in several cases, it comes from the size and the poor structure of the document. Nonetheless, security policy has to be the basis of the ISMS; still there is no clear guidance on how to design such a document. However, at the end of the day, it is the information security manager's responsibility to make the security policy a useful tool for the organizational governance and employees, as well. [21]

Motivate your employees through awards for their awareness, e.g. after a successful clean desk audit. Make good practice as an example to follow, and spread via the organization's communication channels such as the corporate intranet.

Working as a security manager will give a very specific perspective on your organization, but it still remains just one point of view. Therefore, require input from employees regarding information security, because sometimes they see better the everyday risks and potential threats in their personal environment. It is worth making exit interviews in order to reveal what kind of failures they have seen in the organization's information security system during their employment.

Summary

Discussing minimum information security standards is always subjective. In this paper I summarized and aligned with my experiences seven pieces of advice to improve your information security, but this is a highly personal point of view. An information security manager should be aware of the changes in this field, train himself/herself and always be ready to respond to the upcoming threats and security challenges. At the end of the day, the senior management has to understand the importance of information security, and with the support of a security team, the business and security goals can be achieved.

There is no hundred percent security, so this cannot be the final goal—a well-configured ISMS' aim is to manage the risks on an acceptable level. As I stated before, you do not have to reinvent the wheel: methodologies, tools and best practices are public and available. It's your turn now.

References

[1] KELLY, T. S.: Building Bridges with the Board—Innovation in Information Governance. *ISACA Journal*, 3 (2018), 34–38.

[2] TÓTH, A.: Future Information Security Threats to the Defense Sector. *Hadtudományi Szemle*, 10 4 (2017), 246–257.

[3] BÉLANGER, F., COLLIGNON, S., ENGET, K., NEGANGARD, E.: Determinants of early conformance with information security policies. *Information & Management*, 54 7 (2017), 887–901.

[4] THARAKAN, D. J.: Protecting Information—Practical Strategies for CIOs and CISOs. *ISACA Journal,* 3 (2016), 34–36.
[5] *ISO/IEC 27001:2014 Information technology—Security techniques—Information security management systems—Requirements.*
[6] CHARLET, L.: *ISO Survey 2017.* www.iso.org/the-iso-survey.html (Downloaded: 06.01.2019)
[7] *ISO 22301:2012 Societal security—Business continuity management systems—Requirements.*
[8] *ISO 31000:2018 Risk management—Guidelines.*
[9] *ISO/IEC 20000:2005 Information technology—Service management.*
[10] *What is ITIL Best Practice?* www.axelos.com/best-practice-solutions/itil/what-is-itil (Downloaded: 05.10.2018)
[11] avedos *risk2value* software, special release for T-Systems International GmbH.
[12] SZÁDECZKY, T.: Risk Management of New Technologies. *Academic and Applied Research in Military and Public Management Science,* 15 3 (2016), 279–290.
[13] HÁMORNIK, B. P., KRASZNAY, Cs.: Prerequisites of Virtual Teamwork in Security Operations Centers: Knowledge, Skills, Abilities and Other Characteristics. *Academic and Applied Research in Military and Public Management Science,* 16 3 (2017), 73–92.
[14] FEHÉR, J.: Incident management of central and local government agencies. *National Security Review,* 2 (2016), 78–92.
[15] IBM: *Reviewing a year of serious data breaches, major attacks and new vulnerabilities. Analysis of cyber-attack and incident data from IBM's worldwide security services operations.* www.autoindustrylawblog.com/wp-content/uploads/sites/8/2016/05/IBM_2016-cyber-security-intelligence-index.pdf (Downloaded: 23.05.2018)
[16] IBM: *IBM X-Force Threat Intelligence Index 2018. Notable security events of 2017, and look ahead.* https://microstrat.com/sites/default/files/security-ibm-security-solutions-wg-research-report-77014377usen-20180329.pdf (Downloaded: 03.01.2019)
[17] BAUER, S., BERNROIDER, E. W. N., CHUDZIKOWSKI, K.: Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security,* 68 (2017), 145–159.
[18] PARSONS, K., CALIC, D., PATTINSON, M., BUTAVICIUS, M., MCCORMAC, A., ZWAANS, T.: The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security,* 66 (2017), 40–51.
[19] DAHBUR, K., BASHABSHEH, Z., BASHABSHEH, D.: Assessment of Security Awareness: A Qualitative and Quantitative Study. *International Management Review,* 13 1 (2017), 37–58.
[20] SASVÁRI, P., NEMESLAKI, A., WOLF, R.: Old Monarchy in the New Cyberspace: Empirical Examination of Information Security Awareness among Austrian and Hungarian Enterprises. *Academic and Applied Research in Military and Public Management Science,* 14 1 (2015), 63–78.
[21] KARLSSON, F., HEDSTRÖM, K., GOLDKUHL, G.: Practice-based discourse analysis of information security policies. *Computers & Security,* 67 (2017), 267–279.

AARMS Vol. 17, No. 3 (2018) 179–186.

Nonverbal Communication of Prison Subculture through Criminal Tattoo Symbols

Barbora VEGRICHTOVÁ[6]

The paper discusses the importance of tattoo in the criminal environment and prison subculture. Special attention is paid to the function of tattoos, especially in the area of identification and communication. Frequently used symbols have a considerable explanatory value. They reflect the criminal past of the wearer, expressing religious or ideological beliefs, indicate a process of radicalisation, membership in a criminal group or gang. With the help of analysis of the selected tattoo symbols, it is possible to collect valuable information about the personality profile of a particular individual. The findings presented in the paper are based on the original research project realised in the prison facilities in the Czech Republic.

Keywords: *communication, convict, criminal, prison, symbol, tattoo*

Introduction

Prison environment is a unique space accumulating different individual with various personal characteristics, behavioural models and sets of opinions, beliefs, attitudes and criminal experiences. Inmates in correctional facilities all over the world represent specific subculture developing and maintaining internal hierarchy, structured system and a so-called convict code of conduct. Convict code or inmate code refers to the unwritten rules and values developed inside prison facilities among convicts as an integral part of a specific social system. Concerning this phenomenon, it needs to be highlighted that informal rules followed by convicts vary with every country, governmental system or legislation background. These norms could only be effective in small populations, where reputations could provide information at a low cost. [1]

Prison subculture fulfil without any doubt the above-mentioned characteristics. Some rules are original and typical only for selected groups of offenders or groups of gangs respecting ethnical, national, cultural or ideological differences. Other rules can be considered traditional norms representing the social standards of the inmate's behaviour, no matter if it relates to correctional facilities in the United States or European Prisons. American sociologist and criminologist Gresham Sykes with a certain generalisation formulated major norms with stable roots almost in all prisons:

- *Don't Interfere with Inmate Interests.* Never rat on an inmate, don't be nosy, don't have loose lips and never put an inmate on the spot.
- *Don't Fight with Other Inmates.* Don't lose your head and do your own time.

[6] Ph.D., MBA, assistant professor, Faculty of Law and Public Administration, University of Finance and Administration; e-mail: barbora.vegrichtova@gmail.com

- *Don't Exploit Inmates.* If you make a promise, keep it, don't steal from inmates, don't sell favours, and don't go back on bets.
- *Maintain Yourself.* Don't: weaken, whine, cop out. Be a man and be tough.
- *Don't Trust Guards or the Things They Stand For.* Don't be a sucker, the officials are wrong and the prisoners are right. [2]

Among academic sources, this inmate code emphasizes oppositional values to conventional society in general and to prison authorities in particular. The most serious offence against this code of conduct is for an inmate to cooperate with the officials as a *snitch*.[7] Incarcerated persons, after their imprisonment, understand very quickly that the most serious contravention of internal norms of prison subculture is cooperation with the prison staff or even denunciation. Loyalty and conformity to the prison subculture is one of the most highly valued rules among the inmates. In simple terms, convicts live by a system of certain tenets inherited with their incarceration, and carried an "us against them" mentality no matter the odds. Loyalty, honour and respect are priceless within the inmate community.

Respect is a value that represents an inmate's sense of masculine standing within the prison subculture. If convicts are disrespected, they are honour-bound to avenge that disrespect or considered weak by other inmates. Any failure to preserve their sense of respect will lead to a question of the inmates' manhood and their ability to handle the time period in a correctional facility. [3]

Nonverbal Communication in Prisons

Convicts communicate on a daily basis with other inmates, but also with prison staff, educators, pedagogues, attorneys, their family members and relatives. This form of verbal communication is usually under strict control of prison wardens and constantly monitored. Incarcerated persons need to communicate in a secret way, hidden from the permanent monitoring in order to solve their internal matters, transfer important messages, news or warning signs in the daily inmate-to-inmate interaction. Prison slang, used primarily by criminals or incarcerated individuals, is a significant attribute of prison subculture as well, but it is not the paper's purpose to discuss it.

Inmates develop interesting systems of hidden communication which involve different forms and methods of nonverbal expressions. Patterns of demeanour, dress, symbols or gestures are vital in the function of correctional facilities. Convicts use nonverbal communication during their visit when they need to convey something that they do not want the others to hear or understand. They communicate non-verbally when they are ready to start a fight or initiate a prison business. The arrangement of hair, jewellery, clothes, self-touch, short eye contact, changing position of the whole body or crossed arms may symbolise various messages or even instructions for the recipients.

Prison nonverbal code communication were in use from the time prison systems were established and are always developing despite all efforts to combat it. In some cases, the use

[7] A snitch is the label given to an inmate who reveals the activity of another inmate to authorities, usually in exchange for some type of benefit within the prison or legal system.

of symbols and other methods of nonverbal communication is applied outside correctional facilities as well, especially among street gangs and organised crime syndicates. Infamous and very violent street gangs Crips or Bloods use different hand signs, colour symbols or graffiti on a daily basis. They are used to distinguish the members within the gang but it can also be used to deliver messages to rival gangs. Graffiti signs on the walls serve as a means to intimidate the rivals, to mark the territory or memorialize the death of a gang member. It is a very well-known fact that terrorist and extremist organisations are in connection with different security threat groups and gangs. Ideologically motivated movements use symbols and nonverbal communication as an integral part of their propaganda and violent actions.

The use of secret language of codes and symbols in correctional facilities enable the convicts to traffic in drugs and improvised weapons, to smuggle various contraband items into the prison, to intimidate other inmates, to prepare an escape or riot, to recruit or radicalise the individuals or to plan other criminal and illegal activities.

Methodological Background

Tattoos are important symbols used by criminals all over the world and in many cases function as a clear and definite indication of gang membership. The explanatory value of tattoo symbols is in real much more complex and represents a helpful tool in the profiling procedure and consequent risk evaluation.

This concept laid the foundation of research project focused on prison environment in the Czech Republic.

In the followings, a brief sum up will be presented of the key methodological background of the project and research environment in the correctional facilities of the Czech Republic.

The population of the Czech Republic is over 10 million and at the beginning of this year the number of prisoners was about 22,000; out of that 1,775 were pre-trial detainees and roughly 1,800 prisoners had a foreign nationality.

In total, there are 35 prisons in the Czech Republic and each prison has its own governor. Approximately 11,000 employees work within the Prison Service of the Czech Republic. The central management is operated by the Prison Service General Directorate under the Ministry of Justice.

There are 4 basic types of prisons in the Czech Republic. They can be classified as follows: minimum, medium, high and maximum security. Those convicts are placed in the minimum-security prisons who are sentenced for the least severe offences. Convicts sentenced for the most severe offences are placed in the high and maximum-security prisons. There are more than 11,000 convicts in the high security prisons. In the maximum-security prisons there are roughly 1,000 convicts. There are 48 convicts sentenced to life imprisonment, 45 male and 3 female convicts.[8]

All research subjects (incarcerated persons) were informed of the potential risks and benefits of their participation; they received enough clear information to make a voluntary decision. Conscious consent and voluntary participation are fundamental ingredients of an ethical research. The inmates in the Czech prisons were interviewed by the author and

[8] For more information see www.vscr.cz.

during these procedures the tattoos symbols were documented. Information gathered from respondents was put down in questionnaires prepared in advance. All dates were compared, analysed and the final findings interpreted with regard to content analysis of relevant tattoo symbols, tattoo application methods, tattoo purpose and importance and other causalities.

Data was gathered from a sample of more than one thousand interviewed inmates in 14 correctional facilities, including prisons for female convicts. The findings, which are based on content analysis of tattoo symbols and structured interviews confined in all types of prison facilities, provide substantial support for the theoretical expectations and bring remarkable findings. Concerning expected outputs, the ambition of the research team is the innovation of the information system used by the Czech criminal police and investigation service related to the database of criminal tattoo symbols. The research team have developed an electronic database of criminal tattoo symbols, logically categorizing the relevant symbols in specific groups accompanied with adequate description and risk assessment. Criminal tattoos were evaluated as one of the indicators of potential radicalisation processes and were included in the list of indicators, which are detected and assessed by the Prison Service of the Czech Republic. The Police Academy of the Czech Republic organises and performs a 3-days special course for the employees of the Prison Service entitled *Identification of Radicalisation Indicators in Prison Facilities.* At the same time, an analytic tool is also developed for detection of radicalised inmates in prisons, with the objective to implement this programme in all correctional institutions in the Czech Republic and other affected security institutions.

Selected Research Findings

Specific categories of tattoo symbols are characteristic for inmates with notorious criminal background with a tendency to recidivism. For these inmates typical symbols are standing for loss of freedom, stylisation of the role of an incorrigible criminal, adoration of local or foreign personalities of the underworld.

Choosing of a concrete tattoo is of course affected by other inmates and their personal influence. Especially *newcomers* are affected by the attitudes and social behaviour of prison life. This complicated process of adoption to prison conditions or assimilation into the inmate society is called prisonisation. This term is possibly understood as the process of being socialized into the prison culture. This process occurs over time as the inmate or the correctional officer adapts to the informal rules of prison life.

The process of prisonisation is related and in some cases directly influenced by the individual's radicalisation. Personal trauma accompanied by social isolation, problems in the family and private life, frustration, fear of the uncertain future and existential issues can function as radicalisation drivers. Negative and pessimistic opinions can be manifested and expressed through different tattooed quotations, sayings or sentences.

Typical and very frequent phrases among the convicts in Czech correctional facilities are: *Only God can judge me! Live outside the law! Life is a bitch! God forgives, I don't! God gives me a sign! Never give up! Killer! Public enemy number One!* etc.

It needs to be highlighted that these sentences are tattooed in various languages, ethnic dialects and criminal slang.

Figure 1. *Quotation in Latin language.* [Picture made by the author.]

The above presented photo illustrates the popularity of famous quotations among the inmates in Czech correctional facilities. "Non omnia possumus omnes" is a Latin quotation form Virgil, which can be simply translated as: "Not everybody can do everything."

Tattoos simultaneously symbolize a group-organizational association and the hierarchical status of an individual. Prisoners use tattoos to represent their strength and status, to mark their belonging to a certain group, to create a unifying symbol and to define their status and position within their group. [3]

Symbols used by criminals with a rich criminal past in the Czech prison facilities usually prefer symbols with morbid, frustrating and gloomy motifs. Heavily spread are symbols of death, especially sculls with crossbones and figures of Death. The meaning of these motifs have a multiple meaning. Some convicts present their rough nature this way and chosen symbols serve as intimidation tools. Death motifs in different cases refer to the form of crime they committed, most frequently murder or some similar violent act. The symbol of sculls is also very popular among members of Neo-Nazi movements or various outlaw motorcycle clubs. The scull motif with wings is a traditional symbol of the international one-percenter gang, Hells Angels. From the perspective of right-wing extremism, the motif of scull in the traditional design is a well-known symbol of SS units, the infamous paramilitary organisation in Nazi Germany. Right wing extremists using this symbol express this way their loyalty to the Nazi ideology and related attributes. Tattoos are very popular among right wing

extremists and in some cases could represent a deep fanaticism of the tattoo wearer or even acceleration of a radicalisation process. The phenomenon of radicalisation in prison facilities poses serious security threats not only in correctional facilities but also for the external world.

Figure 2. *Symbol related to death and morbid topics.* [Picture made by the author.]

Radicalisation is usually defined *as a process of adopting an extremist belief system, including the willingness to use, support, or facilitate violence, as a method to effect social change.* [4] Prisons are often said to have become the breeding grounds for radicalisation. This should come as no surprise. Prisons are "places of vulnerability", which produce "identity seekers", "protection seekers" and "rebels" in greater numbers than other environments. They provide near-perfect conditions in which radical; religiously framed ideologies can flourish. Overcrowding and understaffing circumstances amplify the conditions that lend themselves to radicalisation. Badly run prisons make the detection of radicalisation difficult, and they also create the physical and ideological space in which extremist recruiters can operate at free will and monopolise the discourse about religion and politics.

Certain tattoo symbols documented in correctional facilities may show the individual's transformation or a change in his/her ideological or religious belief.

Extremism and terrorism are among the security threats for the Czech Republic, on the other hand, in comparison with West European countries this threat is less immediate. The level of extremism in the Czech society is rather low, revealed cases of radicalized individuals willing to commit politically or religiously motivated criminal acts e.g. foreign

fighters, are rather exceptional. But in conformity with the current situation in Europe, Czech inmates are getting radicalised or are imprisoned already being radicalised and contrary to the social situation it is not exceptional. [6]

Politically oriented extremists represent an integral part of the Czech prison subculture. Sentenced and imprisoned followers of extremist ideologies are usually intensively supported by the extremist scene. From this perspective, they are introduced and presented as martyrs, heroes or even so-called *prisoners of war (P.O.W).* Following this concept, Czech extremists are engaged in fund-raising, organise and attend public assemblies and write different comments on the internet and social media in order to help and support their fellows. Such efforts can be detected in the correspondence of classical written communication, as well.

Tattoo symbols can represent the extremist's resistance against the penitentiary system; it is a way of hostile attitude toward prison staff. The most frequently used tattoo symbol in the Czech prison facilities is an anti-police acronym *ACAB (All Cops Are Bastards),* manifested in countless designs and coded variations.

These symbols and other threatening and hateful symbols can be assessed as serious warning signs of an ongoing radicalisation process or as an indicator of a violent individual.

Conclusion

Higher awareness or even professional knowledge about nonverbal communications and symbols related to different ideologies, movements, extremist organisations and gangs could contribute to the effective prevention in this field. The basis of successful tattoo analysis is educated prison staff and mutual sharing of information among the security bodies and academic sphere. The constructive approach to this issue and reciprocal cooperation as a basis makes prevention and intervention as effective and successful as possible.

Criminal tattoos as a way of nonverbal communication in correctional facilities play a multiple role in the process of appropriate detection of dangerous persons and individuals involved in gangs, radicalised inmates or even members of extremist or terrorist groups. The early warning system based on professional and correct detection, together with adequate security measures, constitute the fundamental pillars of crime and terrorism mitigation.

References

[1] SKARBEK, D.: *The Social Order of Underworld.* New York: Oxford University Press, 2014.

[2] CLEAR, T. R., RESIG, M. D., COLE, G. F.: *American Corrections. Seventh Edition.* Boston: Cengage Learning, 2006.

[3] HANSER, D. R.: *Introduction to Corrections. Prison Subculture and Prison Gang Influence.* Chapter 10. www.sagepub.com/sites/default/files/upm-binaries/50421_ch_10.pdf (Downloaded: 11.07.2018)

[4] SHOHAM, E.: *Prison Tattoos. A study of Russian Inmates in Israel.* New York: Springer International Publishing, 2015.

[5] *HR 1955 (110th): Violent Radicalisation and Homegrown Terrorism Prevention Act of 2007.* Homeland Security Institute, *Radicalisation: An Overview and Annotated Bibliography of Open-Source Literature. Final Report* (Arlington: HSI, 2006), 2–12. "The term 'violent radicalisation' has been defined as the process of adopting or promoting an extremist belief system for the purpose of facilitating ideologically based violence to advance political, religious, or social change." www.govtrack.us/congress/bills/110/hr1955/text (Downloaded: 24.10.2007)

[6] VEJVODOVÁ, P., KOLÁŘ, O.: Radicalisation in Czech prisons: empowering of prison staff as "must" for effective facing the issue. In. *17th Annual Conference of the European Society of Criminology.* Cardiff, September 13–16, 2017.

AARMS Vol. 17, No. 3 (2018) 187–188.

Authors' Guide

AARMS is a peer-reviewed international scientific journal devoted to reporting original research articles and comprehensive reviews within its scope that encompasses the military, political, economic, environmental and social dimensions of security.

Manuscripts and editorial correspondence should be addressed to

Prof. Dr. József PADÁNYI, Editor-in-Chief
National University of Public Service
P. O. Box 15, H-1581 Budapest 146
Hungary
E-mail: aarms@uni-nke.hu

Manuscript Submission Form. All manuscripts should be accompanied with a completed Manuscript Submission Form signed by the author who will be responsible for all correspondence and proofreading ("Corresponding Author"). Manuscript Submission Form can be requested from the Editorial Office through mail, fax or e-mail or can be downloaded from the website of the journal.

Form of the manuscript. Manuscripts (text, tables and illustrations) should be submitted in triplicate. Although every effort will be made to guard against loss, it is advisable that authors retain a copy of all materials submitted. Text (in English only) should be typed double spaced on one side of a good quality paper, with generous margins, and bear the title of the paper, name of the author(s), and the institute where the work has been carried out. An abstract of 50 to 150 words should precede the text of the paper stating briefly the main results and conclusions of the work. It should be suitable for use by abstracting services. Authors are encouraged to use descriptive headings, e.g. Introduction, Methods, Results, Discussion, Conclusion, Acknowledgements (if any), Appendix, Notes, References, etc. The paper should preferably not exceed 32 typewritten pages (about 40,000 characters) including tables and references. The approximate location of tables and figures should be indicated on the margin.

Tables and Figures. Tables, each bearing an informative title, should be self-explanatory and numbered consecutively. Black-and-white or gray scaled illustrations should be selected carefully and the number kept to the essential minimum. The author's name, the title of the paper, and the serial number of the figure should be written on the back of each print. Figure captions should be brief and collected on a separate sheet.

References. References should be peer-reviewed literature whenever possible, so technical reports, conference proceedings, and other "gray literature" should be referenced only when no other source of the material is available.

References should be numbered in order of occurrence in the text, where the numbers are given in square brackets as, e.g. [12]. In the References section, the bibliographic elements of the numbered references should be given according to the following examples:

For a journal article
[1] WRIGHT, S.: Surfaces of Selective Value Revisited. *The American Naturalist,* 131 1 (1988), 115–123.

For a book
[2] WALLACE J. M., HOBBS P. V.: *Atmospheric Science: An Introductory Survey.* Cambridge: Academic Press, 1977.

For a chapter in a book or monograph
[3] KAUFMANN, S. A., JOHNSEN, S.: Co-Evolution to the Edge of Chaos: Coupled Fitness Landscapes, Poised States, and Co-Evolutionary Avalanches. In. LANGTON, C. G., TAYLOR, C., FARMER, J. D., RASMUSSEN, S.: *Artificial Life II, SFI Studies in the Sciences of Complexity,* 325–369. Boston: Addison-Wesley Publishing Company, 1991.

Web references
As a minimum, the full URL should be given and the date when the reference was last accessed. Any further information, if known (DOI, author names, dates, reference to a source publication, etc.), should also be given. Web references can be listed separately (e.g., after the reference list) under a different heading if desired, or can be included in the reference list.

[4] NULAND, V.: *2012 Conference on a Middle East Zone Free of Weapons of Mass Destruction (MEWMDFZ), Declaration of USA Department of States.* Washington D.C., 23 11 2012. www.state.gov/r/pa/prs/ps/2012/11/200987.htm (Downloaded: 14.04.2013)

Submission in electronic format. Definitely no electronic version of the manuscript is supposed to be attached to the original submissions. Such attachments will not be archived or kept for later use by the Editorial Office. In case of acceptance, the authors are kindly asked to send an electronic version of the final, accepted manuscript (on magnetic or optical media or via e-mail). In case of any doubt, always the printed paper copy of the manuscript is considered authoritative.

Copyright Transfer Form. Accepted manuscripts cannot be published unless a Copyright Transfer Form is completed and signed by the Corresponding Author. Copyright Transfer Form can be requested from the Editorial Office through mail, fax or e-mail or can be downloaded from the website of the journal.

AARMS Volume 17, Issue 3 (2018)

Contents

ISSN 2498-5392