MILITARY NATIONAL SECURITY SERVICE

Issue 1. 2019.

NATIONAL SECURITY REVIEW

BUDAPEST

Scientific Periodical of the
Military National Security Service

Responsible Publisher:

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

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

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

TABLE OF CONTENTS

JÚLIA FELEGYI

GERMANY'S RESPONSES TO THE CHALLENGES OF TERRORISM AND MIGRATION

Abstract

The aim of the author is to illustrate the changes generated by the refugee wave arriving in Germany regarding migration policy, national security measures and the prevention of terrorist acts. The German migration situation, the powers available to the authorities and innovations to tackle the challenges of terrorism and migration will be described.

***Keywords*:** Germany, migration, national security, terrorism.

Even before the 2015 European migration wave, Germany was a popular destination not only for those from third countries but also from the continent. Since 2015, more than one and a half million asylum seekers have been registered in the country.[1] Given the failure of cultural and labour market integration, worrying figures show that by 2018, 25.5% of the country's population will have an immigrant background.[2,3] In 2016, several terrorist attacks were reportedly committed by asylum seekers and thus linked to the 2015 migration crisis.[4] Following the deadly attacks in Germany and throughout Europe, the federal government has stepped up its security and anti-terrorism laws. In my essay, I present the powers and innovations available to the German authorities to tackle the challenges of terrorism and migration.

Asylum procedure

The reception procedure for asylum seekers is currently governed by the Asylum Procedures Act of 2016. Asylum seekers who are authorized by the authorities to enter the Federal Republic of Germany or found in the country without a residence permit are transported to the nearest reception centre of that state. Initially distributed using the national system, they are distributed among the reception centres of each German state according to the quotas set out in the Asylum Procedures Act. Subsequently, their application for asylum is submitted to the competent branch of the Federal Office

1 Germany sees drop in asylum claims in 2018; https://www.dw.com/en/germany-sees-drop-in-asylum-claims-in-2018/a-47190013 (downloaded 19 October 2019)

2 Resident in Germany whose at least one parent has not become a German national by birth.

3 MTI: Németországban már a lakosság több mint negyede migrációs hátterű; https://www.origo.hu/nagyvilag/20190821-nemetorszagban-meghaladta-a-25-szazalekot-a-migracios-hatteru-lakossag-aranya.html (downloaded 17 October 2019)

4 Grafing bei München, München, Würzburg, Ansbach, Berlin.

for Migration and Asylum (BAMF[5]) for examination and consideration. Asylum seekers are granted a residence permit which entitles them to stay for the duration of the asylum procedure. The asylum interview is the same as the Hungarian and the European procedure, the interview is recorded and translated into the language of the asylum seeker, and the decision is based on the hearing and any further examination required.

Asylum seekers are notified in writing of the decision and informed of the remedies available.[6] If neither asylum nor any other status can be granted, BAMF examines whether there is a prohibition on return during the asylum procedure.[7] Asylum seekers whose application has been denied usually have to leave the country. At least that is the decision, but the practice is the same as the European average in general: in 2018 alone, out of the 236,000 people waiting to be deported, a total of 25,000 were returned, but 31,000 deportation procedures were unsuccessful. Deportations were often not possible due to the identity documents issued to the persons concerned under different names. Since April 2019, authorities have been able to impose different sanctions on them: they cannot apply for employment, they can live only in their designated place of residence and they can be fined. Deportation of deportees may be carried out under simpler conditions prior to their return. The 14-day detention facility serves to clarify the identity of those involved and to assure their presence at any necessary official controls. Anyone who has previously been deported may be taken into custody.

Of those who have committed crimes, those sentenced to one year or more in custody have been deported. Nowadays, people sentenced to six months in prison have to face expulsion from the country. Repeat offenders may be subject to a permanent entry ban. Anyone who cannot be expelled (in the absence of cooperation from the country of origin) can be monitored more closely by the authorities.
There is also an effective new tool for the authorities, they can now reduce the social benefits of asylum seekers who do not produce their documents, do not reveal their other financial resources, apply for asylum late or do not cooperate with the German authorities. The main reason for the withdrawal of social benefits is that many have already been granted refugee status in other European countries, but have moved on to Germany. In the future, they will be supported to the maximum extent possible by returning to the country where they have been granted refugee status.[8]

National security aspects of migration

In the Federal Republic of Germany, the legal framework for the national security system was established by the 1949 Fundamental Law and, following

5 Bundesamt für Migration und Flüchtlinge
6 Asylum and refugee policy; https://www.bmi.bund.de/EN/topics/migration/asylum-refugee-protection/asylum-refugee-policy-germany/asylum-refugee-policy-node.html (downloaded 15 October 2019)
7 Non-refoulement law.
8 JOÓB, Sándor: Kemény szigorításokat vezet be Németország a menekültek kitoloncolására; https://index.hu/kulfold/2019/04/17/nemetorszag_menekultek_kitoloncolas_szigoritas_kiutasitas_horst_seehofer_buntetes_orizetbevetel/ (downloaded 16 October 2019)

reunification in 1990, by the laws relating to national security services. Today, the Federal Constitutional Office (BfV[9]), the Federal Intelligence Service (BND[10]) and the Military Counter-Defense Bureau (MAD[11]) are responsible for national security. In addition, the provinces maintain separate offices for response and security tasks[12].

It is also important to mention the Joint Counter-Terrorism Centre (GTAZ[13]), which is under the authority of the BfV. Since 2004, the centre has been coordinating the activities of federal and provincial organizations, combining and analyzing information obtained there. The organization also includes staff from all three national security services, law enforcement agencies, customs, and the Immigration Service.[14] The role of all three national security services is in some way related to migration. The BfV, as a civilian response service, is responsible for CT and CI operations, preventing the spread of extreme Islam and preventing Islamic terrorism. MAD's activities include combating extremism and terrorism, which may be related to migration-related issues. The BND's Directorate for Combating Terrorism and Organized Crime is responsible for controlling illegal migration and preventing Islamic-based international terrorism. Interestingly, intelligence and analysis are done together within one organizational element to increase efficiency.

Practical work of BND on migration

Founded in 1958, the Hauptstelle für Befragungswesen (HBW) was used to interview incoming migrants. It used covert BND agents, and even allowed the British and American services to question asylum seekers. The BND unit was based in Berlin. It was also active in refugee camps in Germany, where BND had undercover operatives. The migrants interrogated were typically from conflict zone countries. The organization came into focus, when a German newspaper reported in November 2013 that information gathered from migrant camps was also used to target US drone attacks. The newspaper also reported that asylum seekers were sometimes promised more favourable treatment in order to glean information about Islamic groups or other dangers in their own country. Subsequently, the government announced the closure of HBW.[15]

Information provided by the Syrian, Iraqi or Eritrean people is a treasure trove for intelligence services. This is not only a problem in Germany: while intelligence services collect information from as many sources as possible, migrants can also pose a national security risk.

---

9 Bundesamt für Verfassungsschutz
10 Bundesnachrichtendienst
11 Amt für den Militärischen Abschirmdienst
12 Landesbehörde für Verfassungsschutz
13 Gemeinsame Terrorismusabwehrzentrum
14 The concept corresponds to the aims and structure of the Hungarian National Directorate-General for Aliens Policing
15 Balkananalysis: Exclusive: Germany's BND Investigating Migration Risks and Russian Influence in Greece; http://www.balkanalysis.com/blog/2016/03/07/exclusive-germanys-bnd-investigating-migration-risks-and-russian-influence-in-greece/ (downloaded 18 October 2019)

According to balkananalysis.com, BND agents are present in several migration issuing countries (eg Eritrea, Syria, Pakistan), as well as in Turkey, Greece and major international organizations. But there is no need to weave conspiracy theories behind them, they are working within a regulated framework to prevent terrorism, extremism and crime, as most European countries do.
Due to new security challenges (terrorism, migration, radicalization etc.), the budget of the German National Security Services has been steadily increasing in recent years, and the BfV and BND have also expanded their staff.[16] In 2015, the domestic intelligence services were reformed and the BfV became the central leader. The innovations are designed to allow closer collaboration between federal and state authorities while regulating the use of paid informants who report regularly to agency staff.[17]

The Joint Centre for Illegal Migration Analysis and Policy (GASIM[18])

In Germany, a special group was set up in 2006 to analyse uniform information on illegal migration. The Joint Analysis and Strategy Centre on Illegal Migration (GASIM) recruits experts from the Detective Agency, the Police, the Immigration Service, the Labour Inspectorate, the BfV, the BND and the Ministry of Foreign Affairs. At the professional level, the fight against illegal migration has become a key issue in terms of operational activities and the analysis of the resulting information.[19] At the time of its establishment, it had 36 employees and by 2007 it had 40 employees. In July 2011, a total of 18 people worked permanently at GASIM. The current staff is staff of the Federal Office for Migration and Asylum (five), the Federal Criminal Police (two), the BND (one), the Federal Police (nine) and the Customs (one). The Federal Ministry of Foreign Affairs and the BfV represent themselves occasionally. First headquartered in Treptowers, Berlin, it moved to Potsdam, the federal police centre, in August 2009.[20]

Illegal migration and illegal residence are punishable under Article 95 of the Residence Act as they undermine the overall purpose of the German Residence Act, which is to manage immigration in the light of Germany's economic and labour market needs and its capacity to accommodate and integrate immigrants. Anyone staying in Germany without the necessary residence permit must leave the country (Article 50 (1) and (2)). [21]

---

16 Dr. János, BÉRES: Külföldi nemzetbiztonsági szolgálatok; HM Zrínyi Nonprofit Kft, ISBN:9789631295481, pp. 107-113.

17 Marcel FÜRSTENAU: Opinion: Reforming Germany's domestic intelligence service; https://www.dw.com/en/opinion-reforming-germanys-domestic-intelligence-service/a-18560391 (downloaded 17 October 2019)

18 Deutscher Bundestag: Das Gemeinsame Analyse- und Strategiezentrum illegale Migration – Sachstand 2011; http://dip21.bundestag.de/dip21/btd/17/067/1706720.pdf (downloaded 15 October 2019)

19 Balázs, LAUFER: A migráció jelensége, valamint egyes külföldi biztonsági (elhárító) és hírszerző szolgálatok ezzel kapcsolatos kommunikációja; Felderítő Szemle, 2010. Issue 2. p. 59.

20 Gemeinsame Analyse- und Strategiezentrum illegale Migration; op. cit.

21 Act on the Residence, Economic Activity and Integration of Foreigners in the Federal Territory Residence Act, 2017; http://www.gesetze-im-internet.de/englisch_aufenthg/index.html (downloaded 17 October 2019)

National measures against illegal immigration and smuggling of human beings:

- Border checks at international airports in Germany;
- Controls across borders, railway areas and trains;
- Different forms of cooperation between Federal Police, State Police and Federal Customs, such as Joint Investigation Teams, Police and Customs Co-operation Centres;
- Effective investigation and situation analysis by the Federal Police, Federal Criminal Police (BKA) and responsible state-level authorities;
- Comprehensive, inter-ministerial and inter-institutional analysis of illegal immigration, human smuggling and related crimes through GASIM, the Federal Customs Service (Unit for Investigating Illegal Work), the BfV and the Federal Ministry of Foreign Affairs.[22]

International measures against illegal immigration and smuggling of migrants

- Federal police officers for irregular migration in major countries of origin and transit, such as the European Border Agency (FRONTEX[23]); Bilateral and multilateral cooperation on illegal immigration with EU Member States and countries of origin and transit;
- Federal police cooperation with partners in neighbouring countries, such as joint patrols;
- Border Police Liaison Officers in selected countries;
- Cooperation with the European Police Office (Europol[24]), Police Assistance with Targeted Analysis and Evaluation;
- Cooperation with Eurojust[25], judicial assistance in individual cases;
- Cooperation with FRONTEX, for example in the area of strategic evaluation and analysis;
- Assistance in Interpol operations and analyses.[26]

Migration restrictions

As a result of the continued and later the drastic increase in the number of asylum seekers (2012: 77,000, 2014: 202,000, 2016: 745,000), the German government and the legislature have repeatedly opted for a correction of the

22 Illegal entry; https://www.bmi.bund.de/EN/topics/migration/illegal-entry/illegal-entry-node.html (downloaded 15 October 2019)
23 Frontières extérieures
24 European Police Office
25 The European Union's Judicial Cooperation Unit
26 Illegal entry; op. cit.

regulations (Asylpaket I - 2015, Asylpaket II - 2016).[27] The most important changes, which included some tightening, but also some facilitations for more effective integration:

- Unlimited residence permits for successfully integrated minors (§ 25a, § 26a).
- Residence permit for periods of school or dual education (§ 60a).
- Facilitating the conditions for family reunification (§ 27).
- For the first time in modern German refugee law, the possibility of deportation detention was created (§ 62b).
- Automatic ban on entry and stay for rejected asylum seekers from safe third countries, provided they do not leave the country voluntarily (§ 11 Abs. 7).[28]
- The declaration of Albania, Bosnia and Herzegovina, Northern Macedonia, Kosovo, Montenegro, Ghana, Serbia, Senegal and, from 2018, Algeria, Morocco, Tunisia and Georgia as safe countries of origin.[29]
- The concerned individual is financially rewarded for complying with the law: € 800 for those who leave the country before the deadline (30 days or 1 week) in the event of a negative decision. Those who decide to leave Germany before the decision of the authorities before the decision will receive EUR 1200 "start-up aid".[30]
- In order to speed up procedures, 5 special closed reception centres have been set up for those with little chance of acquiring refugee status. (For example, if they refused to cooperate, provided false information, came from a safe country of origin, or came from a third country.) (§ 30a). [31]
- Increase the capacity of integration and language courses. At the same time, the introduction of a partial cost burden for asylum seekers.
- Re-regulate the distribution of asylum seekers between the provinces and between the provinces and the federal state.
- Expulsion procedures can only be halted for health reasons in particularly serious cases.[32]

---

27 Jenny GESLEY: Germany: Proposed Tightening of Asylum Rules; http://www.loc.gov/law/foreign-news/article/germany-proposed-tightening-of-asylum-rules/ (downloaded 16 October 2019)

28 Act on the Residence, Economic Activity and Integration of Foreigners in the Federal Territory Residence Act; op. cit.

29 Demokrata: Bővül a biztonságosnak tekintett országok listája Németországban; https://demokrata.hu/vilag/bovul-a-biztonsagosnak-tekintett-orszagok-listaja-nemetorszagban-106538/ (downloaded 16 October 2019)

30 Starthilfe Plus Programm; http://www.bamf.de/DE/Rueckkehr/StarthilfePlus/starthilfe-plus-node.html (downloaded 16 October 2019)

31 Asylum Act; op. cit.

32 Dr. Szabolcs, PETRUS: Német menekültügyi eljárás – A szabályok szigorúbbak, mint gondolnánk; https://jogaszvilag.hu/vilagjogasz/nemet-menekultugyi-eljaras-a-szabalyok-szigorubbak-mint-gondolnank/ (downloaded 16 October 2019)

- Establishment of a pre-existing Federal Register of Foreigners (AZR[33]) to which federal, provincial and municipal authorities in the field of asylum have access. [34]
- In spring 2019, two proposals from the Ministry of Labour and Social Affairs were adopted at the Cabinet meeting. On the one hand, the financial support for asylum seekers is reduced: for single adults, the total grant is reduced from € 354 to € 344. On the other hand, they will increase their participation in integration courses that include language and social studies.[35]
- In the summer of 2019, a migration policy package was adopted to facilitate the return of rejected asylum seekers and the labour market integration of migrants. The package included the "Ordered Return Act", which extends the powers of police and immigration authorities with regard to the removal of asylum seekers. Horst Seehofer, president of the Bavarian Christian Social Union, said this was a turning point in German migration policy.[36]

Fight against terrorism

The Federal Criminal Police (BKA) in Germany has the prime responsibility for internal security and the fight against terrorism, while intelligence work is split between the BfV and the BND. All three organizations were granted significantly expanded licenses in 2017.

- In June 2017, due to the increased terrorist threat, the government took tougher measures on public surveillance and the Internet, as set out in the German Criminal Code. As a result, the number of security cameras installed in cities has increased significantly. The BfV is responsible for monitoring unconstitutional and extremist activities by screening data sent through telecommunication networks such as e-mails, telephones and text messages. You can also do this by requesting data from your telecommunication service provider, which you can store for up to six months. BND uses preventive intelligence to identify potential threats. As the world's largest internet access point is located in Germany, BND's capability provides particularly strong access to international intelligence. BND may also share information with foreign agencies.
- With the exception of Bavaria, every German state can hold a suspect without charge for up to 14 days. In 2017, Bavaria introduced laws that allow suspects to be pre-arrested for up to three consecutive months. However, every three months the judge must review whether the suspect is released or not.

---

33 Ausländerzentralregister

34 BAMF: Data collection; http://www.bamf.de/EN/DasBAMF/Aufgaben/Datenerhebung/datenerhebung-node.html (downloaded 16 October 2019)

35 JOÓB op. cit.

36 Judith MISCHKE: Germany passes controversial migration law; https://www.politico.eu/article/germany-passes-controversial-migration-law/ (downloaded 18 October 2019)

- The German government's list of banned organizations mainly includes neo-Nazi and Islamist groups. Anyone who is in contact with such groups, whether through the dissemination of propaganda material or the use of their symbols, can be prosecuted. The law on symbols of anti-constitutional groups lists Nazi symbols, and in 2014 the flag used by the so-called "Islamic State" was added to the list.
- While Germany is a member of the Schengen area, which allows the free movement of goods and people within EU borders, in 2015 the federal government introduced controls at the country's borders in response to the migration wave to Europe. According to the European Court of Justice, authorities may require identification within 30 kilometres of an international border, provided that the measure is proportionate and prevents illegal entry into the country.[37]

Summary

The German example shows that migration is a complex challenge that requires in-depth information security services, even as part of an analytical-evaluation cooperation forum, in order to increase efficiency. In addition to counterterrorism and police forces, continuous improvement of the national security sector – financially, headcount, and legislation – is also needed to maintain its effectiveness. As with organized crime, international cooperation is needed to successfully combat acts of terrorism, extremism and illegal migration. Migration to Europe, Germany has not ceased and high-intensity waves continue to be expected due to the demographic explosion in Africa and worldwide civil wars, fallen states and natural disasters. There is a link between migration and terrorism and Germany, with its population of 25% with migrant background, with more than 1.5 million refugees, faces major challenges. Germany's patience is running out. In 2019, more and more migration restrictions were introduced month by month, for example, at the border reinforcing controls and actually rejecting applicants back to their countries of origin. To my mind, further strict measures can be expected in the future.

[37] David MARTIN: Preventing terrorism: What powers do German security forces have? https://www.dw.com/en/preventing-terrorism-what-powers-do-german-security-forces-have/a-40546608 (downloaded 17 October 2019)

Bibliography:

- Asylum Act; http://www.gesetze-im-internet.de/englisch_asylvfg/index.html (downloaded 15 October 2019)
- Asylum and refugee policy; https://www.bmi.bund.de/EN/topics/migration/asylum-refugee-protection/asylum-refugee-policy-germany/asylum-refugee-policy-node.html (downloaded 15 October 2019)
- Act on the Residence, Economic Activity and Integration of Foreigners in the Federal Territory Residence Act, 2017; http://www.gesetze-im-internet.de/englisch_aufenthg/index.html (downloaded 17 October 2019)
- Balkananalysis: Exclusive: Germany's BND Investigating Migration Risks an Russian Influence in Greece; http://www.balkanalysis.com/blog/2016/03/07/exclusive-germanys-bnd-investigating-migration-risks-and-russian-influence-in-greece/ (downloaded 18 October 2019)
- BAMF: Data collection; http://www.bamf.de/EN/DasBAMF/Aufgaben/Datenerhebung/datenerhebung-node.html (downloaded 16 October 2019)
- Dr. János, BÉRES: Külföldi nemzetbiztonsági szolgálatok; Budapest, 2018, HM Zrínyi Nonprofit Kft, ISBN: 9789631295481
- Demokrata: Bővül a biztonságosnak tekintett országok listája Németországban; https://demokrata.hu/vilag/bovul-a-biztonsagosnak-tekintett-orszagok-listaja-nemetorszagban-106538/ (downloaded 16 October 2019)
- Deutscher Bundestag: Das Gemeinsame Analyse- und Strategiezentrum illegale Migration – Sachstand 2011; http://dip21.bundestag.de/dip21/btd/17/067/1706720.pdf (downloaded 15 October 2019)
- Marcel FÜRSTENAU: Opinion: Reforming Germany's domestic intelligence service; https://www.dw.com/en/opinion-reforming-germanys-domestic-intelligence-service/a-18560391 (downloaded 17 October 2019)
- Germany sees drop in asylum claims in 2018; https://www.dw.com/en/germany-sees-drop-in-asylum-claims-in-2018/a-47190013 (downloaded 19 October 2019)
- Jenny GESLEY: Germany: Proposed Tightening of Asylum Rules; http://www.loc.gov/law/foreign-news/article/germany-proposed-tightening-of-asylum-rules/ (downloaded 16 October 2019)
- Illegal entry; https://www.bmi.bund.de/EN/topics/migration/illegal-entry/illegal-entry-node.html (downloaded 15 October 2019)

- Sándor, JOÓB: Kemény szigorításokat vezet be Németország a menekültek kitoloncolására; https://index.hu/kulfold/2019/04/17/nemetorszag_menekultek_kitoloncolas_szigoritas_kiutasitas_horst_seehofer_buntetes_orizetbevetel/ (downloaded 16 October 2019)
- Balázs, LAUFER: A migráció jelensége, valamint egyes külföldi biztonsági (elhárító) és hírszerző szolgálatok ezzel kapcsolatos kommunikációja. Felderítő Szemle, 2010. Issue 2.
- David MARTIN: Preventing terrorism: What powers do German security forces have? https://www.dw.com/en/preventing-terrorism-what-powers-do-german-security-forces-have/a-40546608 (downloaded 17 October 2019)
- Judith MISCHKE: Germany passes controversial migration law; https://www.politico.eu/article/germany-passes-controversial-migration-law/ (downloaded 18 October 2019)
- MTI: Németországban már a lakosság több mint negyede migrációs hátterű; https://www.origo.hu/nagyvilag/20190821-nemetorszagban-meghaladta-a-25-szazalekot-a-migracios-hatteru-lakossag-aranya.html (downloaded 17 October 2019)
- Dr. Szabolcs, PETRUS: Német menekültügyi eljárás – A szabályok szigorúbbak, mint gondolnánk; https://jogaszvilag.hu/vilagjogasz/nemet-menekultugyi-eljaras-a-szabalyok-szigorubbak-mint-gondolnank/ (downloaded 16 October 2019)
- Starthilfe Plus Programm; http://www.bamf.de/DE/Rueckkehr/StarthilfePlus/starthilfe-plus-node.html (downloaded 16 October 2019)

KRISZTIÁN JÓJÁRT

RUSSIAN MILITARY THINKING AND THE HYBRID WAR

Abstract

The goal of the study is to examine hybrid warfare's role and place in the Russian military thought. Hybrid warfare is a Western term and was largely missing from the Russian military literature until 2014. Russian theorists have started to use the notion broadly only after hybrid war has become the popular Western term to label the Russian warfare seen in Ukraine. Ironically, in the Russian understanding it is the West (i.e. the United States) that wages hybrid war, and as such the notion is a synonym for Russian expressions like "new type" or "new generation" war. While Moscow's perception on events of the Arab Spring – which are seen as cases for Western warfare – is distorted, Russian military thinkers probably correctly evaluate how the development of technology (particularly information technology) will change the content of war. Russian forecasts on the primacy of information domain in high-tech future wars preceded Western thinking about the subject. However, today similar thoughts on the preeminent role of information space are widely held by Western military thinkers, too. The paper argues, that in the Russian understanding the so-called hybrid war is the general form of future war.

***Keywords**:* hybrid warfare, Russian military thought, new type war, war in Ukraine

Introduction

The goal of this article is to facilitate a better understanding of the theoretical background of Russia's so-called hybrid war. Russian military thinkers devote great attention to predict what the future war is going to look like and determine the forms and methods to wage it. These ideas were put into practice once Russia launched its war against Ukraine. The study concludes that the hybrid war in Ukraine was not a one-time strategy, but a case for future war. Understanding the lessons Moscow has drawn from the conflict is crucial as they will refine the Russian way of war.

Russia's bold, quick and bloodless military operation in the Crimea has caught the whole world by surprise. The seemingly novel kind of Russian warfare on the one hand, induced Western military thinkers to find a term that best describes this unique warfare. And on the second, to identify its theoretical roots in the Russian strategic thinking. Now we know that the results have become controversial in both quests. As Adamsky points out correctly, "hybrid warfare" – that has become the mainstream term describing the contemporary Russian way of war in the West – is entirely a Western notion that has not even been present in the Russian official lexicon until before the war in Ukraine. Nevertheless, Russian military thinkers refer to hybrid war (gibridnaya voyna) quite often today (see later). The real problem with the notion

however, is that it misguides discussion on the true essence of Russian strategic thought. Hybrid warfare is originally mostly derived from the conceptualization of empirical experiences of wars waged by the U.S. and Israel against state and non-state actors in the Middle East. While there are certain similarities between the blended use of conventional and non-conventional warfare by actors in the Middle East and the war Russia unleashed against Ukraine in 2014, the underlying strategic principles were different. Actors in the Middle East aimed to achieve a "victory by non-defeat" through the application of hybrid warfare whereas the Russian way of war apparently seeks to bring about the defeat of the enemy by mostly non-kinetic and non-military means.[1,2]

Finding the theoretical roots of the "new" Russian warfare has produced not less controversy. Robert Coalson was the first who translated and broadly distributed in June 2014 the now (in)famous article written by Chief of the General Staff, Army General Valery Gerasimov as an "insight" into what happened later in Ukraine.[3] Because of the perceived similarities between the content of the article written in February 27, 2013 and the Ukraine War – the beginning of which was marked by the first appearance of the "little green men" exactly one year later – the paradox that in Gerasimov's understanding it is the West that wages a "new type of war" was easily overlooked. Mark Galeotti, the renowned British Russia expert solved this controversy by claiming that "[t]here is an old Soviet-era rhetorical device that a 'warning' or a 'lesson' from some other situation is used to outline intent and plan. The way that what purports to be an after-action take on the Arab Spring so closely maps across to what was done in Ukraine is striking. Presenting the Arab Spring–wrongly–as the results of covert Western operations allows Gerasimov the freedom to talk about what he wants to talk about: how Russia can subvert and destroy states without direct, overt and large-scale military intervention."[4] Disguising Russian intentions by presenting them as observations on the actions of others is truly a Soviet rhetorical device.[5] Nevertheless, it is more likely that Gerasimov merely meant to

---

1 ADAMSKY, Dmitry: Cross-Domain Coercion: The Current Russian Art of Strategy; Proliferation Papers, No. 54, November 2015 p. 22

2 This analysis uses hybrid war in the lack of a better notion to label the Russian warfare while also bearing in mind that the expression is disputed within military circles.

3 COALSON, Robert: Russian Military Doctrine article by General Valery Gerasimov; Facebook, June 21, 2014, https://www.facebook.com/notes/robert-coalson/russian-military-doctrine-article-by-general-valery-gerasimov/10152184862563597 (downloaded 1 October 2019)

4 GALEOTTI, Mark: The 'Gerasimov Doctrine' and Russian Non-Linear War; In Moscow's Shadows, July 6, 2014, https://web.archive.org/web/20140722003855/https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ (downloaded 1 October 2019) Galeotti has refined and complemented his comments to Gerasimov's article on his blog later. He also apologized in an article for "inventing" the "Gerasimov Doctrine". See: GALEOTTI, Mark: I'm Sorry for Creating the 'Gerasimov Doctrine'; Foreign Policy, March 5, 2018, https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/ (downloaded 1 October 2019)

5 Soviet military thinkers for instance have been discussing the future Soviet battalion tactical formation by seemingly writing about U.S. tactical formations. The weapons and formations presented in Soviet military articles were American but the tactics were actually Soviet. GRAU, Lester: Soviet Non-Linear Combat: The Challenge of the 90s; Soviet Army

describe the operational environment and the nature of future war.[6] As such Gerasimov probably intended to write about what the title of his article suggests: forecasting and predicting the future war which is a crucial component of Russian strategy.

Future war in the Russian terminology: new type, new generation and hybrid

Hybrid war in the Russian understanding seems to be nothing but a synonym for future war. Aleksandr Bartosh, a corresponding member of the Russian Academy of Military Sciences and a retired colonel who writes extensively about hybrid war claims, that it is just another attempt to unify the peculiarities of future war (such as three-dimensional, network centric, contactless, information etc.) into one term. As such, there is "nothing principally new in the understanding of hybrid war" he adds.[7] One can conclude that the terms "hybrid war", "new type war" (favored by Gerasimov and the General Staff) and "new generation war" (coined by retired General-Lieutenant Sergey Chekinov and retired Colonel Sergey Bogdanov, two well-known Russian military theorists) are used interchangeably in the Russian military literature to describe future operational environment and Western warfare. Further – seemingly incoherent – appearance of "new generation" and "new type war" in writings of both Gerasimov and Chekinov and Bogdanov also underscore that the two expressions actually mean the same thing.[8] The content of hybrid war described by Gerasimov and others also seems to be identical with new type and new generation wars.[9]

While officially "new type", "new generation" and "hybrid war" all describe Western warfare in the Russian military literature, it appears that these notions also describe Russian strategy to a certain extent. Timothy Thomas, a distinguished expert on Russian military thought and a former senior fellow at the U.S. Army Foreign Military Studies Office points to this controversy in the context of a speech held by then-Chief of the Main Operational Directorate of the Russian General Staff, Colonel

---

Studies Office, September 1990, https://apps.dtic.mil/dtic/tr/fulltext/u2/a231789.pdf (downloaded 1 October 2019) p. 6

6 BARTLES, Charles: Getting Gerasimov Right; Military Review, January-February 2016

7 БАРТОШ, Александр: Стратегия и контрстратегия гибридной войны; Военная Мысль, No. 10, October 2018a

8 Interestingly, Chekinov and Bogdanov have replaced "new generation" (their own preferred term) with "new type" war later which probably indicates that the authors adopted Gerasimov's and the General Staff's terminology. THOMAS, Timothy: The Evolving Nature of Russia's Way of War; Military Review, July-August 2017. At the same time, Gerasimov used the notion "new generation war" in 2018. ORENSTEIN, Harold: Russian General Staff Chief Valery Gerasimov's 2018 Presentation to the General Staff Academy. Thoughts on Future Military Conflict—March 2018; Military Review Online Exclusive, January 2019, https://www.armyupress.army.mil/Portals/7/Army-Press-Online-Journal/documents/2019/Gerasimov-2019.pdf (downloaded 1 October 2019) Gerasimov's reference to new generation war might be a gesture of tribute to Chekinov and Bogdanov.

9 ГЕРАСИМОВ, Валерий: По опыту Сирии; Военно-промышленный курьер, March 7, 2016, https://vpk-news.ru/articles/29579 (downloaded 1 October 2019)

General Andrey Kartapolov in early 2015.[10] *"It is thus a contradictory view of NTW (new type war – the editor) that Kartapolov presents. He stresses several times how the West, and the United States in particular, uses the concept and does so in a ruthless manner. Then, at the end of his presentation, he clearly states that Russia is preparing to conduct NTW as well in conjunction with the development of asymmetric methods."*[11] The Kartapolov presentation also included a graphic (see Figure 2) which equates the term indirect actions (preferred in the Russian terminology) with hybrid methods (a Western notion).[12] A similar controversy appears in Aleksandr Bartosh's study, in which hybrid is also described as Western warfare. The author emphasizes the non-linear character of hybrid war, while a few lines later he praises the success of Russia's own non-linear strategy in the Crimea and Syria in fending off Western military operations.[13]

Forecasting the war of the future

The obsession with indirect warfare

While Gerasimov wrongly attributes the Arab Spring to Western intelligence services and special forces, he probably correctly assesses the trends of future war. One observation with regard to the trends of current war is the emphasis on the indirect and non-military means which is by no means appeared first in Gerasimov's article. Chekinov and Bogdanov for instance argued for the use of "asymmetric methods" (which should rather be understood as indirect here, as the authors also refer to Liddell Hart in the article) already in 2010 by claiming that *"[t]he danger of catastrophic consequences of hostilities fought on a varying scale with the use of highly effective modern and next-generation weapons, not to say weapons of mass destruction, points to the need for nonmilitary measures of interstate confrontation to be employed more actively to end armed conflicts and local wars, and the role and significance of these measures continues to rise."*[14] Thus, according to Chekinov and Bogdanov it is the unbearable costs potentially arising from the use of direct methods that necessitates the reliance on indirect approaches. This observation is not new either. This was actually the very rationale that drove both the Soviet Union and the United States toward the employment of indirect warfare during the Cold War. In fact – as Michael Kofman notes – Gerasimov's thoughts on the use of non-military means closely

---

10 Kartapolov is currently a Deputy Defense Minister of the Russian Federation and the Chief of Main Directorate for Political-Military Affairs of the Russian Armed Forces. See Kartapolov's short biography on the website of the Russian Ministry of Defense. http://eng.mil.ru/en/management/deputy/more.htm?id=11960036@SD_Employee (downloaded 1 October 2019)

11 THOMAS (2017) op. cit.

12 Ibid.

13 JÓJÁRT, Krisztián: Revising the Theory of Hybrid War. Lessons from Ukraine; Center for European Policy Analysis, April 2019, https://www.cepa.org/revising-the-theory-of-hybrid-war (downloaded 1 October 2019) p. 3

14 CHEKINOV, Sergey – Bogdanov, Sergey: Asymmetrical Actions to Maintain Russia's Military Security; Military Thought, No. 1, 2010

resemble to what George F. Kennan described as overt and covert political warfare in 1948.[15]

The other factor driving warfare toward the use of indirect methods lies in the perception on the contemporary offensive-defensive balance of military technology. Retired U.S. Army Major General David Fastabend argues, that in the physical dimension of conflict defense is becoming the preferred form of war because technology allows for detecting hostile movements relatively easy, making it possible to readily react to them. On the other hand, information domain favors offense as it is relatively easier to infiltrate enemy information systems than fully protecting ourselves from similar intrusions. Thus, it is likely that the future operational environment is going to be a combination of the two, whereby the peer competitor is going to try to set conditions in the information domain so that it could act quickly in the physical one, rapidly making some advantages and then transitioning to defense in order to preserve gains.[16] A similar sequence of operation is reflected in Kartapolov's thoughts on the new-type war.[17] While it is not entirely clear how the Russians perceive the current offensive-defensive balance, the utmost importance they attribute to the superiority in the information domain as a precondition for any conventional military operation suggests their views concur with Fastabend's. Moreover, this might be the rationale Gerasimov sees a disappearing difference between offensive and defensive operations.[18]

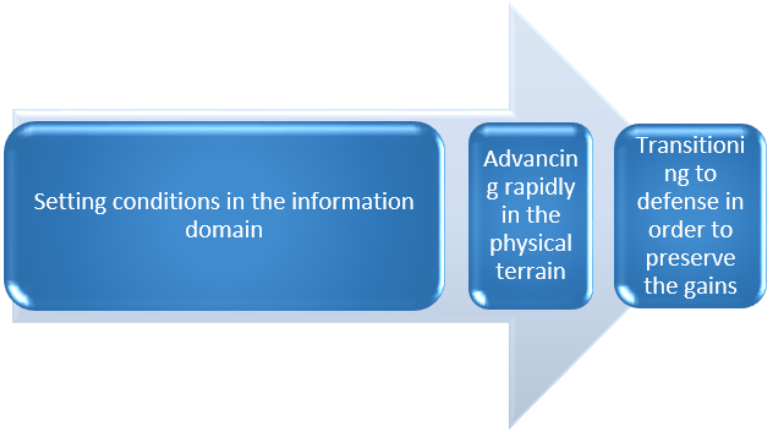

Figure 1: The future operational environment based on Fastabend's thoughts shared in the cited podcast (see footnote no. 15)
(Graphic is prepared by the author)

---

15 KOFMAN, Michael: Russia's Hybrid Warfare and Other Dark Arts; War on the Rocks, March 11, 2016, https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/ (downloaded 1 October 2019)

16 "How Will Technology Change Future Wars?" Modern War Institute Podcast. Episode 66, December 14, 2018, https://mwi.usma.edu/mwi-podcast-will-technology-change-future-wars/ (downloaded 1 October 2019)

17 КАРТАПОЛОВ, Андрей: Уроки военный конфликтов, перспективы развития средств и способов их ведения. Прямые и непрямые деситвя в современных междунардных конфликтах; Вестник Академии военных наук, No. 2 (51) 2015

18 József Holecz in his Hungarian translation and analysis of Gerasimov's well-known article correctly emphasizes the importance to understand why Gerasimov sees a disappearing difference between offense and defense. HOLECZ, József: A Geraszimov-doktrína – egy másik megvilágításban, *Felderítő Szemle,* Vol. XVI., No. 3-4, 2017

Figure 2: Graphic from Andrey Kartapolov's article *(see footnote no. 23).*
Graphic translated by Dr. Harold Orenstein and published in Timothy Thomas' article *(see footnote no. 10).*

The blurring line between offense and defense

Russian discourse about the fading distinction between offense and defense goes back at least until the 1980s' technological change. Analyzing the writings of Soviet military thinkers of the 1980s, Lester W. Grau noted that *"[t]he ability of "defensive" systems to identify deep targets, reach out and destroy them has enabled the modern defense to assume many of the advantages previously enjoyed only by the offense. Thus, in the Soviet perspective of the future battlefield, the distinction between the offense and defense is disappearing."*[19] Further observations of Grau's study on the practical application of this thought in Soviet military planning sound prophetic in retrospect. "In this new environment, the role of conventional artillery will increase. Sufficient artillery must be immediately available to seize fire superiority from the very beginning of the conflict. Revolutionary improvements in munitions, ordnance, reconnaissance and control systems will force the Soviets to shift from their current normative-based firing (which expends vast amounts of ammunition and creates a sizable logistics burden) to accurate, point-target engagements. (…) Since these systems will be more mobile, they will be able to fire at greater depths and service larger areas without having to form into the presently employed large artillery groups. Improved, automated fire control systems will computerize the planning and control of artillery fires to allow effective fires separate from artillery groups and in support of non-linear combat. Artillery will be re-integrated into maneuver battalions to support this non-linear combat."[20] This is another proof that in forecasting the future

[19] GRAU, Lester: Soviet Non-Linear Combat: The Challenge of the 90s; Soviet Army Studies Office, September 1990, https://apps.dtic.mil/dtic/tr/fulltext/u2/a231789.pdf (downloaded 1 October 2019) p. 19

[20] Ibid.

war, Russian military thinkers have been correctly evaluating the likely impacts of technology to warfare. In 2014, the Russian Army fully implemented this theory in practice and unleashed its deadly artillery tactics in eastern Ukraine.[21]

The role of information space

Beyond the concurring views with their Western counterparts that contemporary wars are initiated in the information domain, Russian military thinkers show an almost obsessive interest for information warfare. This is probably best illustrated by a study of two Russian military thinkers, Pavel Doulnev, the head of the Department of Military Art at the Russian Academy of Military Sciences and his colleague professor Vladimir Orlyansky. The 2015 study, titled "Basic Challenges in the Armed Struggle Character of First Third of the XXIst Century" goes as far as to claim, that "in the present circumstances the interrelation between the activity of the highest political leadership and of military formations of different levels will change fundamentally. In other words, politics can exert direct influence not only to the armed struggle of strategic scale but also [to the ones] waged on the operational and tactical levels."[22] [23] This change is driven by our information age. On the other hand, this interrelation is mutual as tactical events can also directly impact the political decision-making – the authors believe. For instance, threatening with the destruction of nuclear or other ecologically dangerous objects during the course of tactical actions can lead to change the entire political goals of a state. This is not only due to the potential dangers of the destruction of these objects but also because of the political demands tied to the threat and the spread of information about it. Thus, the population informed about the threat can force its government to change its political course of action. Information warfare today can often be more effective than kinetic warfare. Therefore, warfare can exclude the latter completely (and consequently armed conflict in general) as information warfare alone can achieve the desired goal.[24] Then-Chief of the Main Operational Directorate of the Russian General Staff, Colonel General Andrey Kartapolov claims that new types of wars consist of 80-90% propaganda and 10-20% actual military violence. However, – unlike Doulnev and Orlyansky – Kartapolov does not envision the disappearance of kinetic warfare and believes it will be still part of any future wars.[25]

Western military experts now also echo very similar ideas – not entirely unrelatedly to the Russian way of war. Colonel Steve Banach, a former director of the U.S. Army's School of Advanced Military Studies writes about what he calls the "Virtual War". The goal of Virtual War is social control, he claims. "The entity that

---

[21] COLLINS, Liam – MORGAN, Harrison: King of Battle: Russia Breaks out the Big Guns; Association of the United States Army, January 22, 2019, https://www.ausa.org/articles/king-battle-russia-breaks-out-big-guns (downloaded 1 October 2019)

[22] Дульнев, Павел –Орлянский, Владимир: Основные изменения в характере вооруженноǐ борьбы первоǐ трети XXI века; Вестник Академии военных наук, No. 1 (50) 2015, p. 45

[23] This might also take us closer to understand why Gerasimov envisions the disappearance of strategic, operational and tactical levels.

[24] Дульнев – Орлянский, 2015 p. 45

[25] Картаполов (2015) op. cit. p. 33

controls the Virtual Domain and masters Virtual War Campaigning first, will indirectly achieve social control, and will win every war they engage in, at pennies on the dollar."[26] No wars in the future will be won without establishing supremacy in the virtual domain first.[27] Banach's thoughts coincide with the ones expressed earlier by his Russian counterparts (for instance Kartapolov or Doulnev and Orlyansky) in as much as they all attribute secondary role to the kinetic battlespace in a future war. As he puts, "[t]he nation-state or actors who can learn the fastest, and optimally frame and reframe their strategies the best, will rule the day in a world that fights predominantly in Virtual Space and only as necessary in Physical Space, as it is too costly on multiple fronts."[28] Once again, is important to emphasize, that Banach's observations are not unrelated to the theory and practice of Russian warfare. He actually emphasizes that both Russia and China are better suited to achieve social control due to their repressive political systems. Indeed, the Russian internet law which aims to secure and insulate the country both from cyber intrusions and what they perceive as hostile information influence is already a step made in Moscow's preparations for a future war scenario.

Theory in practice: the Ukraine War

Ukraine in 2014 has proven to be an ideal target for both Russian military and non-military operations in many respects.[29] However, the strategy used against Ukraine points well beyond the (undoubtedly successful) exploitation of the country's weaknesses of the time. It mirrored what Chekinov and Bogdanov wrote about new generation war in 2013. It also paralleled Fastabend's above described observation (which he formulated five years after the start of the Ukraine War) on the contemporary operational environment and the sequence of future military operations: seizing the initiative in the information domain, then making advancement in the physical one, and consolidating the achieved goals through the quick transition to defense. In the Crimea, Russia has realized this approach in the following manner:

(1) It has launched a full-scale information war against Ukraine which aimed to incite fears from the "fascist Kiev junta" and by that enhancing the secessionist sentiments within the Russian minority.

---

[26] BANACH, Stefan: Virtual War – A Revolution in Human Affairs; *Small Wars Journal*, February 2, 2018, https://smallwarsjournal.com/jrnl/art/virtual-war-revolution-human-affairs (downloaded 1 October 2019)

[27] This almost verbatim echoes Chekinov and Bogdanov as they wrote in their 2013 article that *"no goal will be achieved in future wars unless one belligerent gains information superiority over the other."* Chekinov and Bogdanov's idea is twofold here: gaining superiority both in the spheres of information technology and information and psychological warfare. THOMAS (2017) op. cit. p. 38

[28] BANACH (2018) op. cit.

[29] The factors that made Ukraine an ideal target included Moscow's deep penetration to Ukraine's security services and military, the political chaos in Kyiv, the presence of Russian minority and a Russian speaking population prone to Moscow's soft power influence, and Russia's naval base in Sevastopol and Ukraine's adjacent to Russia geographic situation, the economic dependence of Ukraine on Russia, the Russian presence in different sectors of Ukrainian industry, e.g. in energetics (mainly hydrocarbons), defense sector.

(2) After the decisive move in the information domain, it organized mass protests throughout the peninsula and Russian special operation forces, local and foreign proxies took over the Ukrainian military bases, seized the control over major roads and other key facilities.

(3) The arrival and deployment of defensive – anti-ship, air defense and long-range artillery – weapon systems represented the last phase of the strategy: consolidation of the gains.

All of the above suggest that the warfare may it be called hybrid or else, was not a one-time strategy tailored to Ukraine but the first example of future war. This is underlined by writings of Russian military thinkers who refer to an era of hybrid war. Dmitri Trenin, director of the Carnegie Moscow Center for instance calls the current Russia-West antagonism the age of "Hybrid War" which similarly to the Cold War marks a distinct period in history and has its own rules of game which have not yet been laid down today.[30] Like the Cold War, hybrid war is also accompanied by the revolutionary change in technology and its impact on warfare and society. While it was the appearance of nuclear weapons during the Cold War, today globalization and the development of information-communication technology are the major determinants of hybrid war – argues Aleksandr Bartosh.[31] Since Russian military thinkers apparently regard hybrid war the general form of confrontation in the future, it is of utmost importance to follow and understand the progress of Russian military thought on this subject. The experience of the Ukraine War deserves special attention in that respect.

[30] TRENIN, Dmitri: Avoiding U.S.-Russia Military Escalation During the Hybrid War; Carnegie Moscow Center, January 25, 2018, https://carnegie.ru/2018/01/25/avoiding-u.s.-russia-military-escalation-during-hybrid-war-pub-75277 (downloaded 1 October 2019)

[31] БАРТОШ (2018a) op. cit.

Bartosh and the strategic planning of hybrid war

One writing of Aleksandr Bartosh apparently explores the hurdles of Russian hybrid war strategy in eastern Ukraine. While the author argues (as usual) that it is the West that wages hybrid war, most likely what he really talks about is the lessons of the Russian hybrid war employed against Ukraine. It is quite telling that another writing of his, titled *Strategy and Counterstrategy of Hybrid War* gives actually very few advices on counterstrategy, i.e. how one could defend itself against hybrid war. Instead, it provides a detailed 7-step-strategic-planning of hybrid war. Interestingly, despite the claim hybrid war being a Western strategy, Bartosh's idea on the planning of hybrid war reflects Soviet/Russian strategic planning and not Western one, as it features concepts such as the assessment of the correlation of forces (COF) and forecasting, all typical to Soviet/Russian strategic thought. This again implies that the author actually wants to discuss how Russia could perfect its hybrid methods. Therefore, it is worthy of presenting here the verbatim translation of the seven steps of hybrid strategy:

First: clear formulation of the sense and goal of war.
Second: revealing the weak and vulnerable sides in the fields responsible for the internal and external security of the target country.
Third: formation of the complex of hybrid threats to impact the object of aggression with taking into consideration the local specifics.
Fourth: strategic planning on the basis of concrete assessment of national forces and means, dedicated to exert pressure on bottlenecks and vulnerable spots in the enemy's spheres of political-administrative, financial-economic and cultural-worldview. The expected counteraction (plausible counterstrategy) of the enemy must be also taken into account (This is the assessment of the correlation of forces – the editor).
Fifth: consecutive destructive activity focusing on the victim country's key areas of leadership, concentrating major efforts to the most critical factors guaranteeing the military security of the state (economy, finances, morale of the military and population).
Sixth: carrying out undeclared military movements during which the aggressor country attacks the enemy's state structure and regular army with the help of local insurgents and separatists supported with weapons and money from abroad. The extremist nature of the activities of the "fifth column" plays an important role, as it is used for carrying out ramming strikes against the authorities during one or multiple "color revolutions".
Seventh: declaration of the conditions of ultimatum with regard to the victim state's total capitulation.

Figure 3: Bartosh and the strategic planning of hybrid war[32]

[32] Бартош, Александр: Стратегия и контрстратегия гибридной войны; Военная Мысль, No. 10, October 2018a

The lessons learned from Ukraine

While the annexation of Crimea has been executed smoothly, the Russian hybrid warfare encountered serious difficulties in eastern Ukraine. With the consolidation of the political and military leadership in Kyiv and the decisive advance of the Ukrainian Army and volunteer battalions to regain control over the separatist-held territories, hybrid war protracted and its difficulties have come to surface. Aleksandr Bartosh apparently considers these challenges in his writings in which he underlines the importance of *friction* in hybrid war. According to Carl von Clausewitz, the great Prussian military thinker who first coined the term, friction of war encompasses all the factors due to which actual war deviates from the war on paper. Accidents, lack and unreliability of information and fear are all sources of friction. It is easy to see that a hybrid war's broad range of non-military and military means and its various actors multiply the sources of friction, which enhances chaos. Bartosh claims that the combined use of conventional warfare with irregular methods such as rebel groups or international terrorist organizations increases unpredictability. Proxies are able to block or evade international initiatives dedicated to regulate the conflict and by pursuing their particular interests they drive the conflict toward a free-for-all game.[33] While friction has not been attested during the swift land-grab of Crimea, it caused serious disrupts in the protracted hybrid war in eastern Ukraine. Friction was visible in the presence of different Russia-backed militias in the Donbas (i.e. the so-called Donetsk and Luhansk People's Republics) who have been fighting not only against the Ukrainian Army but oftentimes with each other too. According to a 2015 report, around 2000 fighters were operating within rogue militias at that time, outside the command of Russia or the so-called people's republics.[34] The low morale of the rebel groups and their participation in lootings, extrajudicial killings and human rights violations are broadly documented.[35] It might well be the case that some of the ceasefire violations have occurred contrary to the will of Moscow, underlining Bartosh's claim that proxies can disregard international conflict regulation mechanisms.

---

[33] БАРТОШ, Александр: Гибридная война – переход от неудач к победе; Независимое Военное Обозрение, June 1, 2018b, http://nvo.ng.ru/realty/2018-06-01/1_998_hybryd.html (downloaded 1 October 2019)

[34] JENSEN, Donald: Moscow in the Donbas: Command, Control, Crime and the Minsk Peace Process; NATO Defense College, March 2017, http://www.ndc.nato.int/news/news.php?icode=1029 (downloaded 1 October 2019) p. 4

[35] For an interesting and detailed read on the subject, see Donald Jensen's report.

The tragedy of the MH17 – a case for friction

The shoot down of the Malaysia Airlines flight MH17 is also a case for friction. The Buk air defense complex which has been handed over to the so-called separatists was not the complete system as it included the transporter erector launcher radar (TELAR) vehicle only, and thus missing key components – most notably an acquisition radar vehicle – necessary for the identification of incoming aircraft. Based on phone calls intercepted by the Ukrainian intelligence, it was the Bezler Group – a militia named after its leader and suspected Russian military intelligence (GRU) officer, Igor Bezler – that informed about an approaching aircraft that later turned out to be the MH17.
The intercepted conversation reveals that those who noticed the airplane had no information about its type, role, or even its size, and their observation was purely visual. Another phone call recorded after the rebels have realized they hit a commercial airline testifies, that they were most likely convinced that the airspace was closed for civilian aircraft by the summer of 2014. On the other hand, because Russia consistently denied its participation in the conflict, the world was unaware that the rebels put their hands on advanced air defense systems capable of taking down objects flying at high altitude.
The tragedy meant a turning point in the history of war as it drew the world's attention to the ongoing conflict in eastern Ukraine and Moscow's role in it. Moreover, it pushed the West to accept tough and comprehensive financial and economic sanctions against Russia, after the relatively weak response that followed the occupation of Crimea. Bartosh's statement that tactical events can have strategic impacts in hybrid war is relevant in this respect, in as much as tactical errors can also result (inadvertent) negative strategic consequences.

Figure 4: The tragedy of the MH17 – a case for friction[36]

Moscow has eventually solidified its grip on its proxies thus, decreasing the source of friction. Russian special operation forces and the mysterious Vostok Battalion are suspected behind some of the crackdowns on rogue militias and the violent deaths of certain separatist leaders.[37] Also, separatist militias of the so-called people's republics have been formed into conventional military units under full Russian control. Today, Russian military officers fulfill the ranks of deputy-commander within every military units of battalion size or bigger of the so-called

[36] Read the Bellingcat's report here: https://www.bellingcat.com/news/uk-and-europe/2019/06/19/identifying-the-separatists-linked-to-the-downing-of-mh17/
Listen to the published phone conversation about the observation of the incoming MH17 here: https://www.youtube.com/watch?v=emfVpkBKoow
Listen to the conversation concluded between the militans who investigated the crash site and their commander here: https://www.youtube.com/watch?v=BbyZYgSXdyw

[37] LUHN, Alec: Volunteers or paid fighters? The Vostok Battalion looms large in war with Kiev; Guardian, June 6, 2014, https://www.theguardian.com/world/2014/jun/06/the-vostok-battalion-shaping-the-eastern-ukraine-conflict (downloaded 1 October 2019)

Donetsk and Luhansk People's Republic's (DNR/LNR).[38] This guarantees that no spark in hostilities can happen without the Kremlin's consent.

Implications

One could assume that based on the lessons of the Donbas, Russian hybrid operations would be more centralized and under tighter control in the future. However, decentralized and autonomous activity seems to be a core peculiarity of hybrid war both during the planning and execution phases. Bartosh argues that hybrid war lacks a "formal unified leadership center" and the "general guidelines are worked out and approved on the level of government organizations, leadership of transnational companies, financial and banking structures, different influential persons."[39] This modus operandi is also attested by the work of Putin's Russia in general. About Putin, Mark Galeotti writes that "[h]e (and increasingly often his senior people, too) rarely gives direct instructions, but defines broad objectives and hints as to what he might like to happen."[40] The system – that is comparable to a royal court according to Galeotti – consists of "policy entrepreneurs, seeking and seizing opportunities to develop and implement ideas they think will please the boss, based on hints and guesses."[41,42]

Describing the implementation process, Bartosh writes that "the operational plans of destabilization in the administrative-political, social-economic and cultural-worldview spheres include the creation of various network structures on the territory of the enemy with a high level of independence [samostoyatelnost'] and capability to self-synchronization."[43,44] While independence and autonomy increase friction, the author writes in another study that hybrid war's total lack of legitimacy and subordination to international norms and regulations serve as a *unique oil* which decreases friction. This allows for the "carrying out of the dirtiest provocations with the involvement of terrorist organizations, organized criminal groups, private military companies."[45] Thus, apparently the advantage deriving from the use of a broad range

---

38 JÓJÁRT, Krisztián: Revising the Theory of Hybrid War. Lessons from Ukraine; Center for European Policy Analysis, April 2019, https://www.cepa.org/revising-the-theory-of-hybrid-war (downloaded 1 October 2019) p. 4

39 БАРТОШ (2018a) op. cit.

40 GALEOTTI, Mark, We Need to Talk About Putin. How the West Gets Him Wrong (London: Ebury Press, 2019) p. 20

41 Ibid.

42 A good example to policy entrepreneurship is the failed coup attempt in Montenegro in 2016. According to Bulgarian intelligence, the idea of the coup came first from a Russian businessman, Konstantin Malofeyev. Ibid. p. 25

43 БАРТОШ (2018a) op. cit.

44 Former supervisor of the infamous militia leader and later DNR defense minister, Igor "Strelkov" Girkin states in an interview that Strelkov in 90% acted on his own initiative in Ukraine. МАРТОВА, Марина: Генерал ФСБ: Стрелков в Украине действовал на 90% по собственной инициативе; Независимое Военное Обозрение, December 19, 2014, http://nvo.ng.ru/spforces/2014-12-19/1_interview.html (downloaded 1 October 2019)

45 БАРТОШ, Александр: Гибридная война – новый вызов национальной безопасности России; Национальная Оборона, October 16, 2017 http://www.nationaldefense.ru/includes/periodics/maintheme/2017/1016/154222573/detail.shtml (downloaded 1 October 2019)

of proxies (deniability, execution of provocations) is bigger than the potential disadvantage that is manifested in higher friction.[46] Eventually, Bartosh only calls for the better understanding of friction in hybrid war, and does not advise to eliminate its sources. The heavy presence of the Wagner Group and other Russian private military and security companies in Syria and Libya, and their occurrence in such remote places, like the Central African Republic or Venezuela, also indicate that proxies will play an important part in the Russian way of war and in the Kremlin's foreign policy toolset in general.

Conclusion

While hybrid warfare has not been present in the Russian military literature before 2014, today military thinkers use the term extensively in prominent military journals, like the *Voennaya Misl*, *Voyenno-promishlenniy Kurer* or the *Nezavisimoe Voennoe Obozrenie*. Similarly to the Russian concepts of *new-type* and *new generation wars,* hybrid war describes future operational environment and a perceived Western way of war in these studies. Nevertheless, Russian authors use these notions in a controversial way and often suggest that Moscow should use the same methods to counter Western warfare. Russian military thinkers probably correctly assess what impacts the current technological change and the information society will have on warfare, may it be called hybrid or else. There is a broad consensus within military circles (Russian and Western alike) that no future war will be won without creating a superiority in the information domain first. It seems likely, that future wars will start (and most likely be decided) in the information space and will elaborate in the physical one with the deployment of intelligence services, special operation forces and various proxies. Regular forces will serve as a credible deterrence and shall be deployed only in the closing period to consolidate the achieved goals and defend those from enemy counterattacks. The war in Ukraine has followed this pattern. However, as the war in the Donbas has protracted because of the resistance Ukraine has managed to put up, the numerous proxy actors have increasingly become a burden for Moscow as they tended to pursue their own interests instead of the orders coming from their curators. Insubordinate proxies together with the wide toolset of military and non-military means result that friction is more apparent in a hybrid than in a conventional war. Since in the Russian theory, decentralized and autonomous activity of proxy actors during the early and decisive period of hybrid war is of key importance, the sources of friction are unlikely to decrease in a future hybrid war. The increasing role of Russian private military and security companies play in the facilitation and protection of Russian interests worldwide underscore the theory. Thus, the impact of friction must be taken into account during the planning and execution of a hybrid war in the future.

[46] Moreover: Kartapolov writes that the violation of humanitarian norms and human rights is not a collateral effect but the basic content of the new-type war. This provides a pretext for foreign powers to intervene in the conflict to prevent humanitarian disaster and stabilize the situation. КАРТАПОЛОВ (2015) op. cit. p. 33

Bibliography:

- "How Will Technology Change Future Wars?" Modern War Institute Podcast. Episode 66, December 14, 2018, https://mwi.usma.edu/mwi-podcast-will-technology-change-future-wars/ (downloaded 1 October 2019)
- "Identifying the Separatists Linked to the Downing of MH17," Bellingcat, June 19, 2019, https://www.bellingcat.com/news/uk-and-europe/2019/06/19/identifying-the-separatists-linked-to-the-downing-of-mh17/ (downloaded 1 October 2019)
- "SSU, radio interception of conversations between terrorists, "Boeing-777" plane crash," The SBU's Youtube channel, July 17, 2014, https://www.youtube.com/watch?v=BbyZYgSXdyw (downloaded 1 October 2019)
- "Two minutes before the Boeing-777 tragedy," The SBU's Youtube channel, July 25, 2014, https://www.youtube.com/watch?v=emfVpkBKoow (downloaded 1 October 2019)
- ADAMSKY, Dmitry: Cross-Domain Coercion: The Current Russian Art of Strategy; Proliferation Papers, No. 54, November 2015
- BANACH, Stefan: Virtual War – A Revolution in Human Affairs; Small Wars Journal, February 2, 2018, https://smallwarsjournal.com/jrnl/art/virtual-war-revolution-human-affairs (downloaded 1 October 2019)
- BARTLES, Charles: Getting Gerasimov Right; Military Review, January-February 2016
- CHEKINOV, Sergey – BOGDANOV, Sergey: Asymmetrical Actions to Maintain Russia's Military Security; Military Thought, No. 1, 2010
- COALSON, Robert: Russian Military Doctrine article by General Valery Gerasimov; Facebook, June 21, 2014, https://www.facebook.com/notes/robert-coalson/russian-military-doctrine-article-by-general-valery-gerasimov/10152184862563597 (downloaded 1 October 2019)
- COLLINS, Liam – MORGAN, Harrison: King of Battle: Russia Breaks out the Big Guns; Association of the United States Army, January 22, 2019, https://www.ausa.org/articles/king-battle-russia-breaks-out-big-guns (downloaded 1 October 2019)
- GALEOTTI, Mark: The 'Gerasimov Doctrine' and Russian Non-Linear War; In Moscow's Shadows, July 6, 2014, https://web.archive.org/web/20140722003855/https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ (downloaded 1 October 2019)
- GALEOTTI, Mark: I'm Sorry for Creating the 'Gerasimov Doctrine'; Foreign Policy, March 5, 2018, https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/ (downloaded 1 October 2019)
- GALEOTTI, Mark: We Need to Talk About Putin. How the West Gets Him Wrong, London: Ebury Press, 2019

- GRAU, Lester: Soviet Non-Linear Combat: The Challenge of the 90s; Soviet Army Studies Office, September 1990, https://apps.dtic.mil/dtic/tr/fulltext/u2/a231789.pdf (downloaded 1 October 2019)
- HOLECZ, József: A Geraszimov-doktrína – egy másik megvilágításban; Felderítő Szemle, Vol. XVI., No. 3-4, 2017
- JENSEN, Donald: Moscow in the Donbas: Command, Control, Crime and the Minsk Peace Process; NATO Defense College, March 2017, http://www.ndc.nato.int/news/news.php?icode=1029 (downloaded 1 October 2019)
- JÓJÁRT, Krisztián: Revising the Theory of Hybrid War. Lessons from Ukraine; Center for European Policy Analysis, April 2019, https://www.cepa.org/revising-the-theory-of-hybrid-war (downloaded 1 October 2019)
- KOFMAN, Michael: Russia's Hybrid Warfare and Other Dark Arts; War on the Rocks, March 11, 2016, https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/ (downloaded 1 October 2019)
- LUHN, Alec: Volunteers or paid fighters? The Vostok Battalion looms large in war with Kiev; Guardian, June 6, 2014, https://www.theguardian.com/world/2014/jun/06/the-vostok-battalion-shaping-the-eastern-ukraine-conflict (downloaded 1 October 2019)
- ORENSTEIN, Harold: Russian General Staff Chief Valery Gerasimov's 2018 Presentation to the General Staff Academy. Thoughts on Future Military Conflict—March 2018; Military Review Online Exclusive, January 2019, https://www.armyupress.army.mil/Portals/7/Army-Press-Online-Journal/documents/2019/Gerasimov-2019.pdf (downloaded 1 October 2019)
- THOMAS, Timothy: The Evolving Nature of Russia's Way of War; Military Review, July-August 2017
- TRENIN, Dmitri: Avoiding U.S. – Russia Military Escalation During the Hybrid War; Carnegie Moscow Center, January 25, 2018, https://carnegie.ru/2018/01/25/avoiding-u.s.-russia-military-escalation-during-hybrid-war-pub-75277 (downloaded 1 October 2019)
- БАРТОШ, Александр: Гибридная война – новый вызов национальной безопасности России; Национальная Оборона, October 16, 2017 http://www.nationaldefense.ru/includes/periodics/maintheme/2017/1016/154222573/detail.shtml (downloaded 1 October 2019)
- БАРТОШ, Александр: Гибридная война – переход от неудач к победе; Независимое Военное Обозрение, June 1, 2018b, http://nvo.ng.ru/realty/2018-06-01/1_998_hybryd.html (downloaded 1 October 2019)
- БАРТОШ, Александр: Стратегия и контрстратегия гибридной войны; Военная Мысль, No. 10, October

- Герасимов, Валерий: По опыту Сирии; Военно-промышленный курьер, March 7, 2016, https://vpk-news.ru/articles/29579 (downloaded 1 October 2019)
- Дульнев, Павел – Орлянский, Владимир: Основные изменения в характере вооруженноѓ борьбы первоѓ трети XXI века; Вестник Академии военных наук, No. 1 (50) 2015
- Картаполов, Андрей: Уроки военный конфликтов, перспективы развития средств и способов их ведения. Прямые и непрямые деситвя в современных междунардных конфликтах; Вестник Академии военных наук, No. 2 (51) 2015
- Мартова, Марина: Генерал ФСБ: Стрелков в Украине действовал на 90% по собственной инициативе; Независимое Военное Обозрение, December 19, 2014, http://nvo.ng.ru/spforces/2014-12-19/1_interview.html (downloaded 1 October 2019)

LT. COL. ZSOLT LAKATOS (†) – LT. BALÁZS PÜSPÖK

THE EFFICIENCY OF MILITARY CRISIS MANAGEMENT

Abstract

"Let's speak frankly about military crisis treatments" – was the original title of this thesis, in which we intend to demonstrate the effectiveness of military crisis management by giving examples from some of the current and past peacekeeping operations. Both political and military aspects are demonstrated, highlighting their opposing or similar point of views. After analyzing the duration of peace operations, we only see "*infinite*" and "*interfere and leave*" type missions. Are they the evidences of wrong strategic decisions? How useful and effective these peace operations are from political and military strategic point of view? What is the role of intelligence? In this work we try to find answers to the above mentioned questions.

Keywords: crisis management, peace operations, military interventions, political decisions, responsibility of intelligence

Introduction

Figure 1. clearly shows[1] the decline of developmental supports between the period of presence, and after the leave of US troops from Bosnia and Herzegovina, Haiti, Kosovo, and Iraq. Cordesman would like to emphasize that after the "proclamation" of victory and leaving of troops, the crisis regions and countries "suffered" by peace operations are actually "left alone" with their problems, which is mainly caused by military intervention.

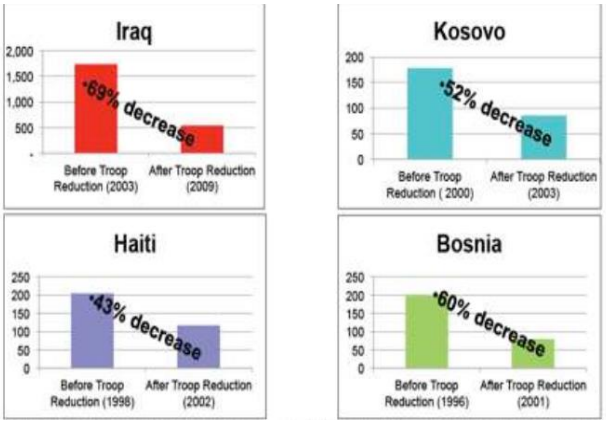

Figure 1: Development assistance levels before and after troop reductions

[1] Anthony H. CORDESMAN: Transition in Afgahnistan: 2009-2013; Center for Strategic and International Studies, Aug 2013, p. 3. http://csis.org/files/publication/130801_transition_afghanistan.pdf (downloaded 02 November 2013)

This statement does not mean that we should not start peace operations because of ethnic conflicts, terrorist threats, humanitarian disasters or because of other reasons, however, without clear identification of strategic planning (the ultimate goals to be achieved: *end state;* and the way leading to it without the determination and support of forces and resources: *force generation*), the failure is almost certainly involved in peace operations.

Missions doomed to failure: "infinite" and "interfere and leave" type peace operations

There are little differences within the goals of a decision-making politician and a soldier, who participates in a peace operation. The most important similarity is, however, the endeavor to survive. Soldiers (from private till general rank) are struggling to return home safe and sound, while politicians are trying to survive the pitfalls in connection with managing political conflict. What can a soldier do, when s/he must accomplish the orders and commands of a politician, who is playing for short-term survival?

Politicians are not almighty; their decisions are influenced by numerous things, whereof public pressure and opinion have crucial importance. Let us remember to George W. Bush American President's speech, narrated on the USS Abraham Lincoln aircraft carrier on 01 May 2003. Behind Bush the "*Mission Accomplished*" text was seen on a billboard, meanwhile the Iraqi security situation progressively worsened, though nobody foresaw the losses suffered by the US Army in the forthcoming years.

In democracies, the fate of politicians is decided in the polling-booths; therefore they take every effort to make favorable or acceptable measures to the public. As long as the suffered losses do not influence significantly their chances for the (re)election (which are often represented by the number of home coming coffins), the support for a peace enforcement operation will be accepted by them. Further important aspect is that the operation should be sustainable in financial and economic dimensions, possibly the UN Security Council's decision should support it, and the army should participate within an alliance or coalition, and not alone.

The peace operations' strategic goal is to reach an "end state" within a determined time-limit, then after the reached status quo the mission terminates and soldiers will be withdrawn. By analyzing the duration of peace operations, we can observe "*infinite*" and "*interfere and leave*" type peace operations on the two ends of the timeline. Both peace operations are the evidences of wrong strategic decisions, because as the first one is extremely stressful and pointless, the second one leaves chaos and often even worse security situation behind after the intervention.

Iraq, Afghanistan, Cyprus, Kosovo, Bosnia and Herzegovina, fight against pirates, ethnic conflicts across the globe. We should count those peace missions for a long time where we have to send soldiers for a shorter or longer period and where we have to devote money, time, energy or even our soldiers' life in order to consolidate the crisis situation or to reach a kind of peaceful solution. However, a question arises: how useful and effective these peace operations are from political and military strategic point of view? Unfortunately, the answer is that in the vast majority of the

cases the tactical, short-term successes are characterized by strategic failures. Although politicians like posing with soldiers in all parts of the world and strengthen their politics by representing them, if we deeper analyse the operations either with UN mandate, or peacekeeping launched by dependent decision without the mandate (UN), crisis managemental (EU definition) or crisis responsal (NATO definition) operations, the strategic failure's admission is sooner or later inevitable. What is the reason for the failure? Who or what is responsible for the unsuccess? Anyway, how to determine the matter of success or failure? What should be done for the peace operations' realization to be more effective? We have plenty of questions, and there are only a few answers leading forward.

First, try to define the concept of success. If this succeeds, then it would not be difficult to create a definition of failure, as it is the opposite of success. In our opinion, success is a kind of condition that accomplishes the determined target. Accordingly, failure means a situation, in which the determined goal is not met. Before starting the strategic analysis of peace operations, it is exceedingly essential to clarify these concepts. Due to the extremely large number of peace operations, the analysis is not complete; in this paper larger operations are emphasized, as well as those, which are more important for Hungary due to geopolitical reasons or participating in NATO/EU coalition missions.

Peace operations in the Western Balkans

Alexander Vershbow − Deputy Secretary General of the NATO − stated in his interview given to the MTI that Hungary did a lot to reach proper security level in the Western Balkans and also in Kosovo. However, according to his assessment, the Western Balkans is an "*unfinished issue*".[2] Bosnia and Herzegovina is one of the best examples, because on the basis of political decision a mission was launched whose strategic purpose and effectiveness is questionable. A Bosnian Serb daily newspaper (Nezavisne Novine) published an article of Milorad Dodik (President of Republika Srpska, the Serb part/entity of Bosnia and Herzegovina) in connection with the 18th anniversary of signing the Dayton Peace Agreement (1995). According to Dodik, Bosnia and Herzegovina "*nowadays is a tragically failed country and a disagreeable place for the inhabitants*." In his opinion, the Balkan state consisting of two entities can no longer keep up, cannot be successful. Dodik in his decisively composed article indicates that "*in Bosnia and Herzegovina everyone is dissatisfied*". "*The Bosniaks because the country is not strong enough, the Croats because they have nothing, and the Serbs because the Republika (Srpska) had been taken away from them, and no one opens their door leading to the independence*".[3] Of course, Dodik is biasing and exaggerating. As the President of the Republika Srpska, his bias and skepticism regarding the future of Bosnia and Herzegovina is understandable. Nevertheless, it must be accepted that his reality-based opinion describes existing problems, political problems, whereupon the military peace operations cannot find a solution. After signing the Dayton Agreement, NATO operations (IFOR and later SFOR) were

[2] A NATO-nak készen kell állnia a jövő válságaira; 24/11/13. Honvédelem. http://www.honvedelem.hu/cikk/41131 (downloaded 24 November 2013)

[3] Csak a daytoni szerződés miatt létezik Bosznia, 20/11/2013; Magyar Nemzet, http://mno.hu/kulfold/csak-a-daytoni-szerzodes-miatt-lezetik-bosznia-1196372 (downloaded 24 November 2013)

launched, and in 2004 they came under the European Union's direction. The ground for this was provided by the Berlin Plus agreement, adopted in 2002. According to it, the EU can use NATO's structures, mechanisms and power sources in order to carry out military operations, if NATO does not intend to participate in them.

Is crisis management a success or a failure in Kosovo? In our opinion, the proper answer is the second one. We must admit that a country was created by a political decision, and such a country cannot survive without the aid coming from the international community. The root of the problem is to be searched in the wrong Dayton Agreement (1995), which established Bosnia and Herzegovina and closed the civil war. As Dr. István Magyar accurately defines: "*During the peace treaty negotiations, contracting parties made an agreement regarding Kosovo without a valuable decision. The agreement – tacitly − acknowledged that ethnic separation is legitimate, and this way those can get the benefits, who can create situations made up for theirselves (even with the methods of ethnic chasing and cleansing).*"[4] The Dayton Agreement did not have the role to arrange the Kosovo case; however, it opened the gate in front of those, who were eager for Kosovo's independence, since the precedent had been given (by establishing Bosnia and Herzegovina). Hungary has been contributing to the KFOR mission since its formation (1999) with sending soldiers to personal staff officer positions, and with deploying contingents. Soldiers serving in Kosovo use every effort to maintain status quo, which was invented by politicians and created by the power of weapons. Nobody is going to acknowledge that this system is not operable, so our soldiers (though in decreasing muster) are going to stay for decades in a country, which is not recognized by several EU countries, therefore Kosovo can be the latest Cyprus from peacekeeping point of view.

Cyprus and the Sinai Peninsula

Cyprus, where the UNFICYP mission was launched in 1964, is one of the oldest peacekeeping activities in which Hungary has been taking part, and one of the best examples of the infinite missions. It is interesting that Hungarian soldiers for the first time ever were sent to peace operation because of a Greek-Turkish opposition, too. In the period of the Austro-Hungarian Empire in 1896, on the island of Crete under the jurisdiction of the Ottoman Empire, the Greeks who made up the majority of the population began to form armed resistance against the invading Turks. The first peacekeeping, peacebuilding mission took three years, after the consolidation of the situation troops returned home. That mission successfully completed its tasks, and serves as a fine example of peace operations because it was short-termed, and effectively implemented the strategic objectives.

On the island of Cyprus, most of the Hungarian contingents serve in the so-called Buffer Zone, but Hungarians also serve at the Nicosia Headquarters (UNFICYP HQ) and in the Nicosia staff officers' group.

The Multinational Force and Observers (MFO) is a UN mission on the Sinai Peninsula. It started on 25 Apr 1982, but it begins to become like the Cypriote

[4] István MAGYAR: A koszovói válságkezelés katonai tapasztalatai; Hadtudomány, 2002, No. 2. http://mhtt.eu/hadtudomany/2000/2_8.html (downloaded 14 November 2019)

mission.[5] The MFO "celebrated" its 30th anniversary in 2012, while the Cyprus mission was 50 years old in 2014. Unlike real peace operations, these missions should not be defined as peace operations, since there is no real strategic goal (end state), only their presence.

Iraq

In case of Iraq, after the military attack on 20 Mar 2003 and the rapid collaps of the regime, the country was characterized by unmanageable political, economic, ethnic, transnational (e.g. terrorism), and other kinds of crises, which are still characteristic today. After the departure of US troops in 2011 and the completion of NATO training mission (Dec 2011), the country sank into total chaos, which was well reflected in the assassinations committed in Oct 2013, during these attacks nearly one thousand civilians were killed.

Sensing the failure of the Iraqi operations, President Obama has decided early enough to withdraw the US troops, leaving alone, however, a previously dictatorship operated country, which did not cause as many headaches to the international community as today's Iraq. For the logistical support to the Polish-led multinational division, a Hungarian logistics transportation battalion served in Iraq in 2003 and in 2004.

Afghanistan

Hungary's participation is multi-faceted in Afghanistan; Hungarian forces has been involved in these operations since 2003, the main objectives are as follows:

- stabilizing Afghanistan;
- establishing the Afghan National Security Forces;
- creating a self-supplying economy;
- improving the living conditions of the population.

The Hungarian participation was intensely wide-ranging during the operations; the Provincial Reconstruction Team (PRT) was the largest, which endeavored to improve the security situation in the province till its withdrawal by regular patrolling in different parts of the province, by facilitating the local security sector's reform, or rather by extending the power of the Afghan central government. In addition, Hungarian forces took part in the defense of Kabul International Airport, in the work of the Afghan Air Force transport helicopter pilots' training and mentoring within the Mi-17 Air Mentor Group, and also in the work of the Afghan Air Force attack helicopter pilots' training and mentoring within the Mi-35 Aviation Training Support Group. The Logistics Mentor Group also helped to increase the level of qualification of the Afghan armed forces. Even today, the special operation forces involved in counter-terror operations provide combat tasks, as well as the Military Advisory Team (MAT), whose duty is to participate in the training and preparation of the Afghan

[5] Attila SELMECZI: Harmincéves az MFO-misszió; 29/05/12. Honvédelem. http://www.honvedelem.hu/cikk/harminceves_az_mfo-misszio (downloaded 10 November 2013)

National Army corps, the Afghan National Police, the Afghan Border Guards, to keep contact with the ISAF units, and to support the formation and implementation of operational planning.

In spite of so many human and material efforts, the international forces' involvement in Afghanistan is doomed to failure. After the twin towers' assault in New York (2001), but prior to the US intervention, Russian strategic analysts and retired generals (who participated in the occupation of Afghanistan) had warned the United States not to intervene with land troops in Afghanistan. Their estimation was grounded on the lessons learned by the failed Soviet invasion. According to the US Department of Defense report, between 2012 and 2013, the loss of the Afghan Security Forces increased by 80%, while the loss of the ISAF and the coalition forces decreased by 60%. What do these numbers mean? The number of Taliban attacks did not change considerably; meanwhile the international forces are gradually withdrawn from the fight. Instead of them, the Afghan Security and Police Forces are trying to hold their ground in the fought battles against the Taliban and other resisting forces. Their qualifications, morale, and equipment do not reach the level of the Western forces', thus their losses are greater.

It is expected that a similar Iraqi situation is about to emerge in Afghanistan. The military action against al-Qaeda and the Taliban were not accompanied by the consolidation of the country. Politicians cannot expect the soldiers to gradually leave the country with dignity, as it is operating under tribal basis and under the warlords' decisions, and which is undoubtedly going to fall back to the period before the ISAF intervention.

Libya

In order to restrain Gaddafi's regular army and militias, NATO led an intervention in Libya with naval and air forces in 2011 under the Operation Unified Protector. The purpose of the 222 days lasting sea and air operation was to protect civilians against Gaddafi's terror.[6] The fact that resistance fighters have killed Gaddafi and have taken over control of the country should mark the operation's success. However, the reality is absolutely different. The National Transitional Council and later the General National Congress were not able to take the country under their control, a permanent source of conflict emerged between the national and local authorities.

On 27 Aug 2012, the US State Department issued a travel warning, indicating the possibility of a conflict, which can break out anywhere and at any time in the country between militias. The arsenals got into the hands of the Islamists, thus different kind of weapons may appear in any country in North Africa in the future. The system is successfully defeated, the dictator is removed, but we cannot speak

[6] Péter BALOGH: Az Operation Unified Protector felderítő tapasztalatai; Hadtudomány, XXII. Vol 1. 2013. http://mhtt.eu/hadtudomany/2013/2013_elektronikus/2013_e_Balogh_Peter.pdf (downloaded 15 November 2019)

about consolidation at all. It is to be feared that the country gets into deeper chaos, from where it will not be able to emerge for decades.

EU missions

Based on the above-mentioned Berlin Plus agreement, next to the current EUFOR operation in Bosnia and Herzegovina, the characteristics of "purely" EU-led operations is that the EU military missions are trying to avoid the UN practice of "infinite" operation formations. Owing to this, they expect during the planning that another operation - especially operations led by the African Union or by the UN - take over the management of peace operations, or simply they do not define a strategic goal. In such cases, the period is turning into goal, according to the EU's practice; it is generally one year which may be extended if necessary. For example, the EUNAVFOR Atalanta mission, launched against the Somali pirates, is continuously extending since 2008. Owing to the operation, piracy is far not so profitable in Somalia like a few years ago, but we should not have illusions: as piracy in the Gulf of Aden became increasingly general, merchant vessels began to steer well clear of the Somali coast, and this has required the Somali pirates to operate further out to sea and they have developed the “mother ship” strategy. In addition, intensive naval operations in the area have drove piracy to another less protected area, thus piracy have spread through the Indian Ocean and created a new “High Risk Area”.[7]

Design models

The North Atlantic Treaty Organization, the European Union, and the United Nations have also developed their own operational planning models, which operate relatively effectively, and provide space for the flexible strategic planning. Regarding the “infinite” and “interfere and leave” type peace operations we can notice that not unique incidents, but rather system failures occurred. By extremely simplifying, the process is the following: [8]

- intelligence has the responsibility to report predictions and warnings in the crisis management process; in case of NATO and EU, the reports of the military and civilian intelligence services are set together by a serious analytical apparatus into an all-risk and all-hazard threats analyzing document;
- this document is the basis of the assessment of military strategy, which defines those military options, whereby the ambitions can be carried out;
- after choosing the appropriate option, the operation’s planning begins;
- after the operation’s approval the period of implementation starts;
- during the period of implementation they evaluate the operation at certain intervals, and apply various modifications (fine-tuning) in order to succeed.

---

7 Balázs PÜSPÖK: Az EU első haditengerészeti missziója, Fókuszban az Európai Unió; 2014, p. 100.

8 Crisis Management in NATO’s Strategy, 16/15/03. pp. 1-8, 1-9.

The failure of missions and peace operations at the strategic level can be deduced from two main reasons. First: political leaders assign bad strategic targets; and second: military strategic planning is made on the basis of faulty goals. These two matters are closely related, but still different. Let's see, how do politicians and soldiers think about these problems: „*War is too serious a matter to entrust to military men*", said Georges Clemenceau, French politician, who carried through the First World War as a victorious prime minister. Sun Tzu Chinese general saw the following errors in case of "politicians": "*There are three ways in which a ruler can bring misfortune upon his army:*

1. *by commanding the army to advance or to retreat, being ignorant of the fact that it cannot obey: this is called hobbling the army;*
2. *by not understanding the particular roles of an army, and handle it as a simple governing: this causes confusion in the officers' minds;*
3. *by attempting to govern an army in the same way as he administers a kingdom, being ignorant of the conditions which obtain in an army: this way the officers' will not know what to do.* [9]"

Sun Tzu said: when a prince entrusts the leadership of an army, military leaders must take over all responsibility, and prince shall not intervene in the governance of it. Against Sun Tzu, Clemenceau wanted to narrow the soldiers' space. The golden mean – as so often – Clausewitz, who declares: "*war is merely the continuation of policy by other means*".[10] Thinking about the Iraqi intervention or the air operations against Serbia (1999), the statement of Clausewitz is also valid for peace operations.

Wrong political decisions

The failure of peace operations is primarily and fundamentally consequence of wrong political decisions. In many cases, of course, politicians simply cannot make appropriate decisions; they have to make them in lack of time, and under embarrassment (like under the pressure of public opinion). However, in most of the cases, political decisions are also made near the optimum conditions, which already carry the likelihood of failure at the time of the adjudgement.

Through a specific example, the entire problem might be understandable easier. The difficulties caused by Somali pirates were not recent ones; the problem has reached the threshold level during the past years, when politics felt it is time to intervene. "*From 1991, following President and dictator Siad Barre's downfall, Somalia with its barely more than 9 million inhabitants was sunk into civil war, and it is still wearing its consequences. The central government was not working; the central management of the army and the police terminated, the country came under the leadership of clans and slowly sank into complete chaos. The fallen and disfunctional Somali Navy and Coast Guard was unable to defend the coastal marine waters, where foreign fishing flotillas were able to gain the rich tuna stocks unmolestedly off the Somali coast. From the unemployed, more and more*

[9] SZUN-CE: A hadviselés törvényei; Budapest, Zrínyi, 1963. http://mek.oszk.hu/01300/01345/01345.htm#alapelvek (downloaded 10 November 2013)
[10] Carl von CLAUSEWITZ: A háborúról; Budapest, Zrínyi, 1961, p. 56.

impoverished fishermen and from the former Navy and Coast Guard members ad hoc became organized marine units, the so-called militias. For the first time, they attacked these unpermitted foreign fishing boats. Militias began to attack merchant ships (sailing in international waters) after years only. Today, piracy has become an industry in Somalia, primarily in the parts of Somaliland and Puntland."[11] During the EU operational planning, intelligence information's clearly indicated that without the elimination of the pirates' coastal bases, only the problem's symptomatic treatment is expected. However, political reasons overwrote the justified operational steps, and a maritime operation started, where eight to ten ships are patrolling for years in an area, which is equivalent to the size of Europe. Only after years of the operation's beginning, the Commander of EUNAVFOR managed to perform limited strikes with land troops on the coastal bases of the pirates.

Of course, there are situations, such as relatively sudden bursts of ethnic conflicts, when there is no time to make grounded decisions from all aspects. The available forces must be sent to the location and endeavour to separate immediately the opposing parties. In such cases, sooner or later we need to find an answer to the question: how to go further? – but usually, this is the most difficult question to answer.

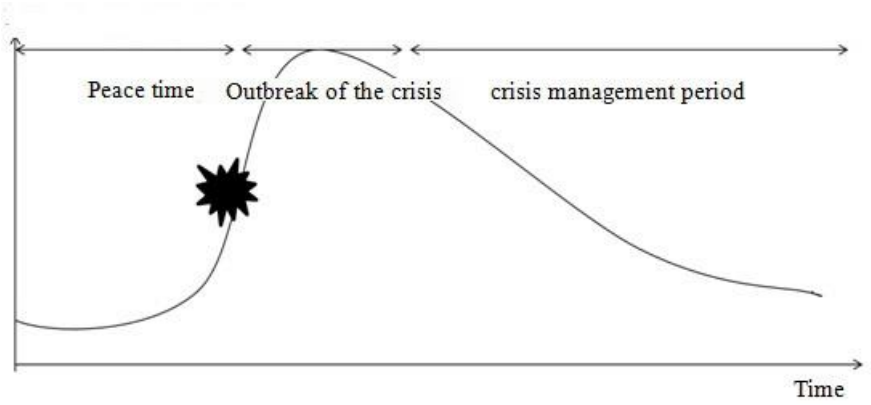

Figure 2: The intensity of the crisis

The Figure 2. (edited by Zsolt Lakatos) demonstrates the well-known crisis diagram. The star shows the moment of the crisis' outbreak. It can be seen that crisis management begins only after the outbreak, past the climax. The political aspects have decisive significance before the operations' preparation and planning, and the latter failure of the operation is already encoded in this section. Politicians and military planners need to determine the exact purpose and task of the involved forces within peace missions. What do we want to achieve? What is the strategic purpose of the operation? The soldiers only seek opportunities to act upon the received orders. If the strategic conceptions and planning are incorrect, than the final result can neither be long-lasting, nor favorable.

[11] Zsolt LAKATOS: Harcban a kalózokkal; Interpress Magazin, Dec 2012, p. 58. ISSN: 01331639

The responsibility of intelligence

The role of intelligence is crucial at the period of planning stage of a peace operation. The biggest and most difficult task is to give policymakers a realistic picture of the opposing forces' strength, ideas, terrain, and weather, political, economic and social conditions. Furthermore, the responsibility of intelligence is also to illustrate the difficulties, associated with the implementation of peace procession. This is the point where analysts have to reference very clearly, as they have to forecast the difficulties of the operation's launch and implementation; additionally, they have to give medium and long-term forecasts regarding the expected consequences. Throughout history, many examples can be found when politicians ignored the information and reports of the intelligence. Of course, they have the right for this, intelligence makes a "providing" activity, and it is not almighty. By investigating the peace operations, we can see that intelligence forecasts and reports are not taken seriously in more and more cases. The consequence is that politicians set bad strategic targets, which later, in the section of implementation, is going to lead to failure.

Summary

The "infinite" and "interfere and leave" type missions are results of policy failures. As the result of bad political decisions, the participant forces in peace operations are often responsible for enforcing a status quo, which cannot be maintained after the withdrawal of forces. Political leaders are not aware of the involved forces' capabilities and opportunities, thus they make claims which cannot be accomplished. To avoid this, it is necessary to theoretically prepare the political leaders on the possible military operations, including conflict management, and the application of different peace support forms.

During the strategic planning, objectives have to be determined for the final condition, in order to avoid the "infinite" and "interfere and leave" type missions. The responsibility of intelligence is to inform accurately and truthfully the top political and military leadership about the expected difficulties, and about the emergencies and risks regarding the peace operation.

Bibliography:

- A NATO-nak készen kell állnia a jövő válságaira, 24/11/2013. Honvédelem, http://www.honvedelem.hu/cikk/41131 (downloaded 24 November 2013)
- Crisis Management in NATO's Strategy, 16/15/03. pp. 1-8, 1-9
- Csak a daytoni szerződés miatt létezik Bosznia, 20/11/13. Magyar Nemzet**.** http://mno.hu/kulfold/csak-a-daytoni-szerzodes-miatt-lezetik-bosznia-1196372 (downloaded 24 November 2013)
- BALOGH Péter: Az Operation Unified Protector felderítő tapasztalatai, Hadtudomány, XXII. Vol 1. 2013. http://mhtt.eu/hadtudomany/2013/2013_elektronikus/2013_e_Balogh_Peter.pdf (downloaded 15 November 2019)
- CLAUSEWITZ, Carl von: A háborúról, Budapest, Zrínyi, 1961.
- CORDESMAN, Anthony H.: Transition in Afgahnistan: 2009-2013, Center for Strategic and International Studies, Aug 2013. http://csis.org/files/publication/130801_transition_afghanistan.pdf (downloaded 02 November 2013)
- LAKATOS Zsolt: Harcban a kalózokkal, Interpress Magazin, Dec 2012. ISSN: 01331639
- MAGYAR István: A koszovói válságkezelés katonai tapasztalatai, Hadtudomány, 2002, No. 2. http://mhtt.eu/hadtudomany/2000/2_8.html (downloaded 14 November 2019)
- PÜSPÖK Balázs: Az EU első haditengerészeti missziója, Fókuszban az Európai Unió, 2014.
- SELMECZI Attila: Harmincéves az MFO-misszió, 29/05/12. Honvédelem. http://www.honvedelem.hu/cikk/harminceves_az_mfo-misszio (downloaded 10 November 2013)
- SZUN-CE: A hadviselés törvényei, Budapest, Zrínyi, 1963. http://mek.oszk.hu/01300/01345/01345.htm#alapelvek (downloaded 10 November 2013)

TAMÁS TÓTH

GENERAL DESCRIPTION OF SOCIAL ENGINEERING AND ITS PLACE IN INFORMATION WARFARE

Abstract

Due to the ever expanding nature of Social Engineering (abbr.: SE), it is important to analyze its relationship to military and non-military operations in order to ensure more efficient prevention and counter-activities to it. This article strives to present both the illegal and illegitimate SE activities (e.g. organized crime, industrial espionage, etc.) as well as the legal and legitimate SE activities like criminal detection and national security SE counter-activities. When analyzing SE a special focus is put on the development of terrorism and its relation to SE.
The article aims to conclude the results of the same Author's previous these for university degree under the title of "Possibilities of the Employment of SE During Attacks in Cyber and Other Spheres" and to summarize the developments related to SE since the handing in of the above these.

***Keywords*:** social engineering, cyber terrorism, information warfare

Introduction

In some forms of information warfare, computer network operations, including attacks against information systems, have emerged with the advent of computer technology. These attacks can be carried out in cyberspace directly via IT systems using digital tools. In this case, they attack networks through the use of info-communication tools, exploiting vulnerabilities in software and hardware components. However, there is another way to carry out the attack, by attacking the cognitive dimension of cyberspace, that is, by exploiting the vulnerabilities of human users, to launch attacks against IT systems. This tool of cyber warfare, cyber operations, is referred to in the literature as social engineering (hereinafter SE). The Hungarian meaning of SE most closely corresponds to the concept of psychological manipulation, but it does not fully cover the functioning of SE either. SE is a complex process whose components form a system. the use of SE is described in this publication both from a legal and security-threat point of view, primarily in the focus of terrorism. Human intelligence (HUMINT), including the use of SE, plays an important role in the preparation of professionally executed terrorist acts, as it is possible to obtain sufficient relevant information about potential targets primarily through the internal staff of the infrastructure without the use of high-cost, hi-tech tools. Most of the information is currently managed in cyberspace using info-communication tools. Therefore, it is inevitable that terrorist organizations' destructive activities will be pursued in this dimension, as they will need to be present in cyberspace in order to meet their demand for information, in order to prepare for

effective attacks on information systems. The purpose of this article is to present the general characteristics of SE, its areas of application, and the relationship between SE and information warfare. This publication is intended to illustrate the results of a previous thesis[1] on the same subject.

1. The place of Social Engineering in the Information Warfare[2]

Globalization, the exponentially expanding information society and technological advances, place increasing emphasis on ensuring the robust operation of IT tools and user-generated cyberspace. Confidentiality, integrity and availability are essential for maintaining system security, as only in this case can full protection of the dimensions and levels[3] of security be guaranteed. In terms of the vertical architecture of security, individual, national, regional and global levels can be distinguished. In terms of dimensions, military and non-military areas should be split, taking into account their subsystems[4]

LEVEL (vertical)	**AREA (horizontal)**				
	Military	**Non-military**			
		Economic	**Political**	**Social**	**Ecological**
Global	*International Security*				
Regional	*National (external, internal) Security*				
National	*National (internal) Security*				
Individual	*Personal Security*				

Figure 1: The vertical and horizontal structure of the dimensions and levels of Security
(*Edited and translated by the author*[5])

---

1 TÓTH, Tamás: The Possibility of Applying Social Engineering in Attacks Perpetrated in Cyberspace and Escalating to Other Dimensions, National University of Public Service, Budapest, 2019

2 KOVÁCS, László: The Place and Role of Electronic Warfare in the Information Warfare of the Future, Military Science and Defense Matters, 2001. p. 1 http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/2195/hadtud_2001_2_kovacs.pdf?SEquence=1&isAllowed=y (downloaded 28 October 2018)

3 DR. VIDA, Csaba: Military Elements of Security and Security Policy, National Security Review 2013 /Issue 1, NKE, 2013. p. 90. http://archiv.uni-nke.hu/uploads/media_items/a-biztonsag-es-a- a-biztonsag politika-katonai elemei.original.pdf (downloaded 28 October 2018)

4 TÓTH, Tamás: New Challenges for Business Information Acquisition in Organized Crime Following Its Paradigm Shift in the 21st century, Professional Review 2018 / Issue No. 1, KNBSZ, Budapest, 2018. pp. 103-104. http://knbsz.gov.hu/hu/letoltes/szsz/2018_1_szam.pdf (downloaded 28 October 2018.)

5 HANGGI Heiner: Making Sense of Security Sector Governance, Table 1.1: The widening and deepening of the concept of security – Table 1.1: The scope and depth of the concept of security, 2003, p. 5. https://s4rsa.wikispaces.com/file/view/SEcurity+SEctor+Governance.pdf (downloaded 28 October 2018.)

Utilizing vulnerabilities in information, physical, and cognitive elements[6] of cyberspace, significant attacks can be carried out against facilities critical for the delivery of services for the population[7] and critical information infrastructures against social subsystems, including the civilian population. However, *"In addition to civilian applications, it is essential for military operations to gain IT support and information superiority."*[8] The individual, the organizational, the state, and the Alliance are distinguished in terms of the perpetrators of the attack and the injured parties. However, regional conflicts escalate to the international arena, thus threatening or jeopardizing the interests and security of an Alliance.

PERPETRATOR (Attacker)	**INJURED PARTY** (Target)			
	Individual	**Organization**	**State**	**Alliance**
Individual	CID unit	CID unit	National Security/ CID unit	Military unit
Organization	CID unit	CID unit	National Security unit	Military unit
State	-	-	National Security unit	Military unit
Alliance	-	-	National Security unit	Military unit

Figure 2: Players of IT attacks and distribution of defensive, responding forces from a legal theory point of view
(Edited by the Author)

The primary responsibility for eradicating illegal activities between individuals and organizations, that is, business entities that make up the business sector of the national economy, and criminal organizations, in order to maintain public security, lies primarily with the Criminal Investigation Division (CID) service branch of the police.

The primary responsibility for investigating cyber-attacks on the state lies with law enforcement agencies. It is not included in the table, but in the case of terrorist acts, it is not clear that the execution of countermeasures and the realization of the attackers is essentially a military operation, even though "*almost all experts state that it guerilla warfare and terrorism can be categorized as forms of asymmetric*

---

6 SIMON, László – DR. MAGYAR, Sándor: The Impact of Terrorism and its Indirect Effects on Cyberspace, National Security Review 2017/3. NKE, 2017. pp. 96-97. https://www.uni.nke.hu/document/uni-nke.hu/nemzetbiztonsagi-szemle-2017-3-1.original.pdf (downloaded 28 October 2018.

7 MOI Decree No 24/1997 (III. 26) on the range of facilities of special importance for the functioning of the state and the supply of the population.

8 GYÁNYI, Sándor: Methods of Attack and Defense against Information Terrorism, Doctoral (PhD) Dissertation, ZMNE HDI, Budapest, 2011. p. 9., http://portal.zmne.hu/download/KMDI/ERTEKEZES_TERVEZETEK/Gyanyi_Sandor_PhD_ert_tervezet.pdf (downloaded 28 October 2018)

warfare"[9], since the handling of attacks on the civilian population also raises law enforcement tasks due to the criminal category of terrorism.'

Attacks on alliances, even those of an IT nature, carry the potential for a global escalation of security threats[10], as alliances are affected, meaning more Member States and their civilian populations can be affected. It is therefore appropriate to carry out military-defense information operations[11] in both defensive and offensive ways. The Member States of the North Atlantic Treaty (hereinafter referred to as "NATO"), in *Article 5 of the North Atlantic Treaty*, have adopted the following procedures in the event of an attack that are already in effect in during attacks perpetrated in cyberspace: "*The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.*"[12] According to NATO's 2010 Strategic Concept on Defense and Security: "*Cyber-attacks are becoming more frequent, more organized and increasingly damaging to governments, businesses, economies and potentially critical transportation and supply networks and other critical infrastructures. They can reach a threshold that is already threatening national and Euro-Atlantic prosperity, security and stability. Foreign forces and intelligence and secret services, organized criminals, terrorists and / or extremist groups may equally be the perpetrators of such an attack"*[13]

Based on the foregoing, it can be stated that SE is applicable to military operations in cyberspace and thus forms part of the information warfare. This is also the case with social engineering when it is introduced during terrorist acts, since terrorism is classified as an asymmetric form of warfare. In the following, this publication focuses on information warfare operations, mainly in the areas of

---

9 János TOMOLYA – József PADÁNYI: Terrorism and Guerrilla Warfare - Similarities and Differences, MHTT, Military Science 2014 / Issue No. 1. Budapest, 2014. pp. 133. http://www.mhtt.eu/had science / 2014 / 2014_electronic / 11_TOMOLYA_PADANYI.pdf (downloaded 28 October 2018)

10 GAZDAG Ferenc: The Nature of Security Policy Challenges, Chapter III: Security threat classification, Grotius, Corvinus University NTI, 2012. pp. 6-14., http://www.grotius.com/doc/pub/DQFPQW/2012_35_rich_a_security_policy_termeszetol.pdf (downloaded October 2018)

11 INFOOPS - Information Operations (See AJP 3-10. Allied Joint Doctrine for Information Operations) http://info.publicintelligence.net/NATO-IO.pdf (downloaded October 28, 2018)

12 The North Atlantic Treaty, Article 5, NATO, Washington DC, April 4, 1949 https://sites.google.com/ site / honvedelem / nato contracts (downloaded 13 February 2018)

13 NATO, Lisbon, 2010, Strategic Concept of Member States' Defense and Security of the North Atlantic Treaty Organization

electronic warfare[14] and SE operations in computer network operations[15], focusing on illegal actions.

2. Definition of SE

According to Kevin D. Mitnick and Wiliam Simon: "Social engineering, by the means of influence and persuasion, deceives, manipulates, or persuades people that the social engineer is really what they say they are. As a result, the social engineer, with or without the use of technology, is able to exploit people in order to obtain information."[16] Employing SE is basically implemented using IT and human-based methods. Possible means of influencing the IT system are, for example, text messages (sms, email) or certain advertisements. The criterion of the human intelligence gathering method is direct contact with the target person, such as asking for help, offering help, and referring to power.[17] Direct contact can take place through personally meeting the target person or even through contacting them by telephone. Social engineering is thus none other than "manipulating the interested human resources, with or without the use of technical means, in for the purpose of obtaining information order to satisfy the information needs of the interested party."[18]

The formulation of SE demonstrates its widespread applicability as it is not only cyber-crime or terrorist organizations that use manipulation. It plays an important role both in general public intelligence or intelligence gathering HUMINT operations[19] and in the activities of defensive intelligence gathering organizations in the private sector.

The use of SE elements may also be tied to the assertion of the interests of national security, economic security, public security and private security. A good example of psychological manipulation in the exercise of state authority is the deployment of covert investigators using a cover or a legend for purposes of crime detection. The purpose of the operation is to vindicate the criminal prosecution needs of the state, which introduces a new identity and life-legend for the undercover investigator upon infiltrating the criminal organization.[20] It is perceptible that members of a criminal organization are being deceived in a legal and legitimate manner in the interest of the whole of society. Criminal organizations can use information obtained by psychological manipulation to prepare for physical attacks.

---

14 EW – Electronic Warfare

15 CNO – Computer Network Operations

16 MITNICK, Kevin D. – SIMON, William L.: The Legendary Hacker - The Art of Deception, Perfact-Pro Ltd. Budapest, 2003, cover

17 Veronika DEÁK: Human-Based Attack Techniques in Social Engineering, p.4 technical (downloaded 14 February 2018)

18 Tamás TÓTH: The Possibility of Applying Social Engineering in Attacks Perpetrated in Cyberspace and Escalating to Other Dimensions, National University of Public Service, Budapest, 2019. p. 9

19 KIS-BENEDEK, József: Information Gathering with the Use of Human Resources, In.: Basics of National Security, Subchapter 7.3 Editor: KOBOLKA, István, National Public Service and Schoolbook Publishing Inc, Budapest, 2013, pp.145-151.

20 MÉSZÁROS, Bence: Covert Investigation in Criminal Prosecution, Doctoral thesis, PTE ÁJK DI, Pécs, 2011, pp. 16-21. http://ajk.pte.hu/files/file/doktori-iskola/meszaros-bence/meszaros-bence-vedes-ertekezes.pdf (downloaded 02 September 2019)

Contacting employees of bank security companies and establishing a relationship of trust can lead to the acquisition of enough information on security inspections, cash transportation, and physical security. During attacks in cyberspace, SE seeks to cover the data and information acquisition phase. SE, whether legitimate or illegitimate, unlawful or illegal, is always designed to detect and exploit vulnerabilities in the organization one is trying to attack.

3. Areas of SE application

Based on the foregoing, it can be stated that an SE may not only be an activity threatening and violating security, but also an offensive or defensive information gathering process applied by public or private security agencies to ensure national, economic and corporate security. In addition to describing the SE operations used in illegal activities, it is important to look at the entire segment of the SE application, including its legal and legitimate uses.

State covert intelligence, counterintelligence and overt information gathering activities:

The application of the SE is part of the activity of safeguarding national, economic and public security in the exercise of state authority. The meaning of the need for intelligence is to inform the state leadership and the defense agencies, in the course of decision support activities, in order to assert the interest of the whole society. Enforcement bodies are law enforcement agencies and defense forces that operate in a regulated legal environment using intelligence and criminal investigative techniques.[21] The activity is basically legitimate and legal, as long as it does not violate the sovereignty or economic interests of another state, for example in the conduct of economic intelligence.[22]

Business information gathering activities:

In the course of defensive and offensive business (intelligence) information gathering[23], SE can only be conducted under ethical principles[24] in a regulated legal environment, in a legal and legitimate manner. The purpose of the need for intelligence is to establish and maintain company security, monitor rival companies, examine the economic environment, and support decision-making activities of the

---

21 Chapters XXV and XXVI of Schedule 1. of Government Decree No. 160/2011 (VIII.18.) On the Approval of the Export, Import, Transfer and Transit of Military Equipment and on the Certification of Companies

22 PORTEOUS, Samuel D.: Economic Espionage II. Commentary, CSIS Publication, Canada 1994, p. 46

23 Business (intelligence) information gathering at the strategic and operational level of the company, is a legitimate activity with legal principles to establish and maintain active and passive economic security, designed to maximize profit (TÓTH, Tamás: New Challenges of Business Information Gathering As a Result of the Paradigm Shift in Organized Crime in the 21st Century, Professional Review 2018/Issue No. 1., KNBSZ, Budapest, 2018. p. 106. http://knbsz.gov.hu/hu/letoltes/szsz/2018_1_szam.pdf (downloaded 28 October 2018)

24 MIKULÁS, Gábor: A Test of Vigilance: Business Counterintelligence, Figyelő, (Observer), 2003/Issue No. 20. Budapest, p. 46.

management to maximize profit, at sector, strategic, and tactical levels[25]. Its users include elements of the private security sector, decentralized business intelligence agencies, or centralized departments within the company.

Organized crime activities:

The purpose of SE for organized crime is to obtain unauthorized profit, with the direct consequence of inflicting social harm. With globalization and the rise of capitalist market economies, the corporate sector has the greatest influence in the field of economic regulation, with the result that transnational corporations make the greatest profits in the national and international economies. As a result of the information society gaining ground, these companies have become the main targets of organized crime groups that are trying to make significant illegal profits by attacking their information and communication systems. Attacks can come from criminal organizations, as well as industrial espionage activities of rival companies[26] from within the corporate sector. This conduct posing a threat to society is a punishable (criminal) conduct, i.e. it is neither legitimate nor legal. The purpose of the need for intelligence is to obtain the maximum amount of illegal profits and an opportunity to legalize them.

Terrorism:

Terrorist organizations fought armed struggles on land, air and water before entering cyberspace.[27] What distinguishes these militant and separatist organizations from the organized crime groups is that for them the financial gain was conceived only as an instrument and not as a goal. These organizations have always pursued their activities to assert political interests, and referring to religious and ethnic reasons, they have made destabilization their goal, mainly through the attack on the civilian population. Guerrilla warfare can be considered a first-generation, structured terrorism, since "*traditional terrorism, whether separatist or ideologically based, has always had a political and social objective, such as gaining independence, expelling foreigners, or creating a new social order.*"[28] The use of manipulation was realized in the course of physical attacks, with an intellectual intent. That is, the demand for intelligence is realized in the preparation for physical attacks, for example, regarding the degree of protection of the target facility, vehicle, person, security deficiencies. The purpose of the attack is to effectively execute the political interest-assertion activities of the separatist forces in order to achieve their sovereignty. Such

---

[25] ORMOSY, Gábor – HARMADOS, György – JASENSZKY, Nándor – FORRÓ, György: Business Intelligence and Counterintelligence (Textbook), Police Staff College, Budapest, 2010, pp. 175-185.

[26] PORTEOUS, Samuel D.: Economic Espionage II. Commentary, CSIS Publication, Canada 1994, p. 46.

[27] RESPERGER, István – KISS, Álmos Péter – SOMKUTI, Bálint: Asymmetric warfare in the modern age – Small-scale wars with great impact. Zrínyi Publishing House, Budapest, 2014. pp. 13-44.

[28] HOFFMAN, Bruce: Inside Terrorism, New York, Columbia University Press, 2006, pp. 60-62.

organizations include the Kurdish Workers' Party (PKK), the Irish Republican Army (IRA)[29] and the Palestine Liberation Organization (PLO).

In modern-day terrorism, one cannot speak of an intellectual inducer generated by general political and social interest. According to the thoughts of Dr. János Tomolya and Dr. József Padányi: "*New terrorism has a different character: its political objective is not clearly defined, the focus is on social destruction and the extermination of a large part of the population*."[30] The ultimate purpose of the need for intelligence is the overthrow of the social order, the physical attack on the civilian population, using either religious or political views. The use of SE has a dual purpose, one of which is to select potential perpetrators and then radicalize them, while the other objective is realized in the preparation for the operation, i.e. gathering information on the degree of protection and vulnerability of the target facility or vehicle. Such organizations include al-Qaeda in Iraq, Jema Islamiya[31] in Indonesia, and the Islamic State (ISIS).

Lone assailants become perpetrators of postmodern terrorist acts. The training of terrorists and the preparation for their operations can be structured, organized on an organizational basis, on a network basis and in an individual context.[32] In this case, "*a state of reduced consciousness, or a simple but prolonged experience of helplessness may trigger a terrorist act.*"[33] This may be the case for second and third generation immigrants due to discrimination, religious and cultural differences, i.e. the lack of the ability to integrate and adapt. Summarizing the results of Dr. Ágnes Hankiss's research, the vast majority of cases have links between offenders and terrorist organizations in the form of networks.[34] The purpose of SE, as well as the demand for intelligence, is the same as that of modern-day terrorism, which escalates into an attack on society as a result of hatred of the individual in operations in various theater settings. As a result of the globalization of the information environment, cyberspace has emerged as a new dimension beyond the four dimensions of the theater of operations.[35] In addition to the traditional warfare methods used so far, there is a

---

29 VERES Gábor – DR. BÁCS, Zoltán György: Terrorism in Northern Ireland, Terror & Counterterrorism 2017/Issue No. 3, TEK TT, Budapest, pp. 113-168.

30 TOMOLYA, János – PADÁNYI, József: Terrorism and Guerrilla Warfare - Similarities and Differences, Military Science 2014/Issue No. 1. MHTT, Budapest, 2014, p. 134. http://www.mhtt.eu/hadtudomany/2014/2014_elektronikus/11_TOMOLYA_PADANYI.pdf (downloaded 02 September 2019.)

31 AL-AGHA Cintia Asoum: Radical Islam in South-East Asia, Terror & Counterterrorism 2017/Issues No 1-2, TEK TT, Budapest, pp. 68-69.

32 DR. BÁCS, Zoltán György: The Relationship between Radicalization and Terrorism, Some Forms thereof, Thoughts on the Possible Perspectives of Prevention, National Security Review 2017/Issue No. 1, NKE NBI, pp. 14-15. http://archiv.uni-nke.hu/uploads/media_items/dr_-jur_-bacs-zoltan-gyorgy-a-radikalizacio-es-a-terrorizmus-kapcsolata_-egyes-formai_-gondolatok-a-megelozes-lehetsegesperspektivairol.original.pdf (downloaded 02 September 2019)

33 SZŰCS, László: The Psychology of Terrorism, https://honvedelem.hu/cikk/61828_a_terrorizmus_pszichologiaja (downloaded 02 September 2019)

34 HANKISS, Ágnes: The Legend of the „Lone Wolf", Face & Mask 2017/Issue No. 2-3, Béla Hamvas Research Institute, Budapest, 2017. pp. 204-213. http://www.hamvasintezet.hu/arc-es-alarc-3/ (downloaded 02 September 2019)

35 Warsaw Summit Communiqué – Articles 70-71, NATO Summit in Warsaw, July 2016

need to focus much more on cyberwarfare operations, cyber operations and the threats of information operations in the global information environment, as cyberspace is currently one of the most appropriate venues for terrorism to achieve political and military goals.[36]

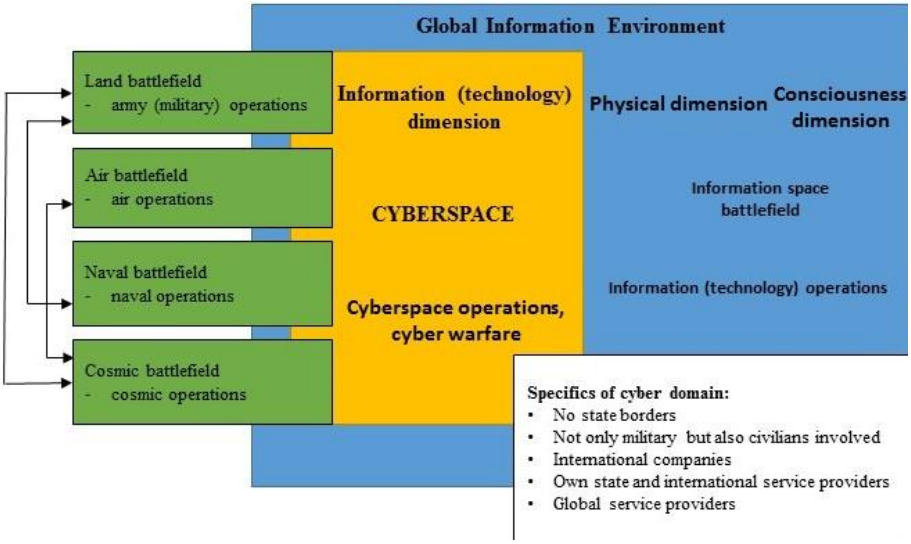

Figure 3: Interpreting cyberspace[37]
(Edited by László Kovács)

In conducting terrorist attacks in cyberspace, terrorists basically need intelligence or data on the degree of security, security conditions, and vulnerabilities of the information system they want to attack. As a result of the organic evolution of security technology, technological vulnerabilities have been reduced, so one of the most effective ways to obtain information is to exploit the users' inadequate security awareness. Utilizing the vulnerabilities of the human factor can provide the most sophisticated influence in cyberspace dimensions by enabling users to attack hardware and software components, as well as accessing cognitive information and data repositories.

In such operations, the identity of the perpetrator may be hidden, as the deceived person will be used to obtain the necessary information and to carry out the attack. The following diagram illustrates the relationship between the human factor, data, information, software and hardware, IT infrastructures.

---

36 HAIG, Zsolt: Information, Society, Security. NKE Service Providing Plc, Budapest, 2015. pp. 93-122.

37 KOVÁCS, László: Cyber Warfare in Hungary, Ludovika Free University, Budapest, 2015. https://www.uni-nke.hu/document/uni-nke-hu/7-kovacs-laszlo.original.pdf (downloaded 03 September 2019.)

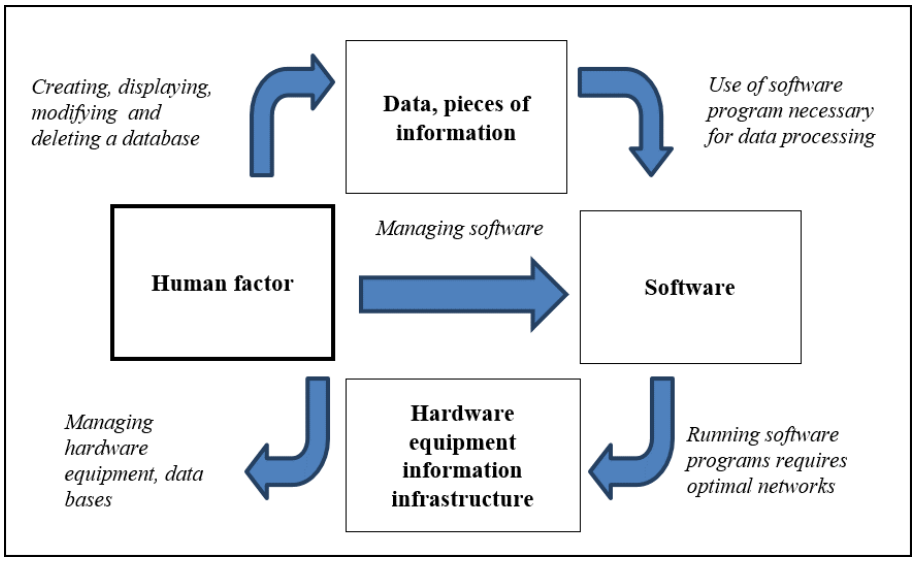

Figure 4: The connection between the human factor and elements of the electronic information system[38]
(Edited by the Author)

Obtaining relevant information can range from a one-off contact approach to long-term operations. The temporal dynamism of the SE operation directly influences the negative social impact of the attack's outcome. This is what makes SE tenable. Based on the above, it can be stated that individual, organizational and governmental efforts to increase security awareness in order to prevent and counteract SE can add significant value to security, because: – according to Dr. Lajos Muha and Dr. Csaba Krasznay – "*The human factor is the weakest link in defense, and it will be exploited by the adversaries and enemies of the organization."*[39] However, based on this statement, the corporate sector's approach to the issue is that, according to Márton Németh and Gergely Takács, „*Generally speaking, a significant portion of businesses devote the most attention and resources to building and operating various physical and IT security systems when it comes to improving security.*"[40]

[38] OROSZI Eszter: Social Engineering –Human Resources as the Critical Factor in Information Security BCE GTK SZTT, 2008, p. 12. http://krasznay.hu/presentation/diploma_oroszi.pdf (downloaded 03 September 2019)

[39] MUHA, Lajos – KRASZNAY, Csaba: Managing the Security of Electronic Information Systems, NKE VTI, Budapest, 2014, p. 54. http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/9975/Teljes%20sz%C3%B6veg%21?sequence=1&isAllowed=y (downloaded 03 September 2019)

[40] NÉMET, Márton – TAKÁCS, Gergely: The Human Factor as the Weakest Link in Security - The Corporate and National Security Aspects of Social Engineering, Face and Mask 2018/ Fall-Winter Issue, Béla Hamvas Cultural Research Institute, Budapest, 2018. ISSN 1578-7949

Conclusions

Based on the ideas expressed in the article, it has been confirmed that, in terms of information warfare, social engineering can be classified as information-gathering operations that can be used illegally and legally. The presence of SE can be detected in information warfare elements in both electronic and computer network operations as well as cyber operations. Its primary function is to obtain information, which can be regarded as a supporting activity during the planning and execution of attacks, however, the purpose of deceiving a manipulated victim may also be to carry out a physical attack – on a person, a system or a facility. The presence of terrorist organizations in cyberspace enhances the presence of illegal SE operations, the prevention and countering of which is a high priority task for defense forces and law enforcement agencies. However, the corporate sector, for example, is still not paying adequate attention to reducing the human risks that can be exploited in the implementation of SE, in order to prevent and counter it. The main focus for them is to strengthen physical and electronic security, which should also increase the level of security awareness among employees and users.

In addition to illegally obtaining information, SE can also be used to assert national, public and private security interests, both legally and legitimately. It is then used against individuals and organizations that have a negative impact on society. In this case, the manipulated offender may provide information about his or her organization and activities to the undercover law enforcement officer, who can eliminate a criminal organization and prevent a terrorist attack or other crimes. Undercover activities are not possible for the purpose of offensive and defensive business intelligence, as only law enforcement agencies are authorized to conduct undercover operations.

Bibliography:

- Schedule NO. 1 to Government Decree 160/2011 (VIII. 8.) on the Approval of the Export, Import, Transfer and Transit of Military Equipment and Services and on the Certification of Companies. (VIII. 18.)
- AJP 3-10. Allied Joint Doctrine for Information Operations http://info.publicintelligence.net/NATO-IO.pdf (downloaded 28 October 2018.)
- AL-AGHA Cintia Asoum: Radical Islam in South-East Asia, Terror & Counterterrorism 2017/Issues 1-2, TEK TT, Budapest, 2017., HU ISNN 2067-0374
- MOI Decree No. 24/1997 (III. 26) on the range of facilities of special importance to the functioning of the state and the supply of the population
- Strategic Concept of the North Atlantic Treaty Organization on the Protection and Security of Member States 12 NATO, Lisbon, 2010.
- Article 5, North Atlantic Treaty, NATO, Washington, 4 April 1949. https://sites.google.com/ site/honvedelem/nato-szerzodes (downloaded 13 February 2018.)

- DEÁK, Veronika: Human-based attack techniques of social engineering, http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-szamitogep-alapu-social-engineering-tamadasi-technikai (downloaded 14 February 2018.)
- Dr. BÁCS, Zoltán György: The relationship between radicalization and terrorism, some of its forms and ideas on possible perspectives of prevention National Security Review 2017/Issue No. 1, NKE NBI, Budapest, 2017. http://archiv.uni-nke.hu/uploads/media_items/dr_-jur_-bacs-zoltan-gyorgy-a-radikalizacio-es-a-terrorizmus-kapcsolata_-egyes-formai_-gondolatok-a-megelozes-lehetSEgesperspektivairol.original.pdf (downloaded 02 September 2019) ISBN: HU ISSN 2064-3756
- Dr. VIDA, Csaba: Military components of security and security policy, National Security Review 2013/Issue No 1, NKE, 2013. http://archiv.uni-nke.hu/uploads/media_items/a-biztonsag-es-a-biztonsag-politika-katonai elemei.original.pdf (downloaded 28 October 2018) ISBN: HU ISSN 2064-3756
- GAZDAG, Ferenc: On the nature of security policy challenges, Chapter III: Categorization of factors threatening security, Grotius, Corvinus University NTI, Budapest, 2012. http://www.grotius.hu/doc/pub/DQFPQW/2012_35_gazdag_a_biztonsagpolitikai_kihivasok_termeszeteol.pdf (downloaded 28 October 2018)
- GYÁNYI, Sándor: Methods of attack and protection against information terrorism, Doctoral thesis (PhD), ZMNE HDI, Budapest, 2011. http://portal.zmne.hu/download/KMDI/ERTEKEZES_TERVEZETEK/Gyanyi_Sandor_PhD_ert_tervezet.pdf (downloaded 28 October 2018.)
- HAIG, Zsolt: Information, Society, Security. NKE Service Providing Plc, Budapest, 2015.
- HANGGI, Heiner: Making Sense of Security Sector Governance, Table 1.1: The widening and deepening of the concept of security – 2003. https://s4rsa.wikispaces.com/file/view/SEcurity+SEctor+Governance.pdf (downloaded 28 October 2018)
- HANKISS, Ágnes: The Legend of the "Lone Wolf", Face and Mask 2017/Issues 2-3, Béla Hamvas Research Institute, Budapest, 2017. http://www.hamvasintezet.hu/arc-es-alarc-3/ (downloaded 02 September 2019.)
- HOFFMAN, Bruce: Inside Terrorism, Columbia University Press, New York, 2006. ISBN 0231510462
- KIS-BENEDEK, József: Information gathering through the human intelligence (HUMINT) method, In.: Basics of National Security, Edited by KOBOLKA, István, National Public Service and Schoolbook Publishing House, Inc, Budapest, 2013. ISBN 978-615-5344-32-9
- KOVÁCS, László: The place and role of electronic warfare in future information warfare, Military Science – Military Affairs, 2001. http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/2195/hadtud_2001_2_kovacs.pdf ?SEquence=1&isAllowed=y (downloaded 28 October 2018.)

- KOVÁCS, László: Cyber warfare in Hungary; Ludovika Free University, Budapest, 2015., https://www.uni-nke.hu/document/uni-nke-hu/7-kovacs-laszlo.original.pdf (downloaded 03 September 2019.)
- NÉMET, Márton – TAKÁCS, Gergely: The Human Factor as the Weakest Link in Security - The Corporate and National Security Aspects of Social Engineering, Face and Mask 2018/ Fall-Winter Issue, Béla Hamvas Cultural Research Institute, Budapest, 2018., ISSN 1578-7949
- MÉSZÁROS, Bence: Covert investigation in criminal prosecution, Doctoral (PhD) thesis, PTE ÁJK DI, Pécs, 2011., http://ajk.pte.hu/files/file/doktori-iskola/meszaros-bence/meszaros-bence-vedes-ertekezes.pdf (downloaded 02 September 2019)
- MIKULÁS, Gábor: A Test of Vigilance: Business Counterintelligence, Figyelő, (Observer) 2003/Issue No. 20, Budapest, 2003.
- MITNICK, Kevin D. – SIMON, William L.: The Legendary Hacker – the Art of Deception, Perfact-Pro Plc. Budapest, 2003. ISBN 978 963 206 55 57
- MUHA, Lajos – KRASZNAY, Csaba: Managing the Security of Electronic Information Systems, NKE VTI, Budapest, 2014., http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/9975/Teljes%20sz%C3%B6veg%21?SEquence=1&isAllowed=y (downloaded 03 September 2019) ISBN 978-615-5491-65-8
- ORMOSY, Gábor – HARMADOS, György – JASENSZKY, Nándor – FORRÓ, György: Business Intelligence and Counterintelligence, (Textbook) Police Staff College, Budapest, 2010.
- OROSZI, Eszter: Social Engineering – Human Resources as the Critical Factor of Information Security, BCE GTK SZTT, 2008, http://krasznay.hu/preSEntation/diploma_oroszi.pdf (downloaded 03 September 2019)
- PORTEOUS, Samuel D.: Economic Espionage II. Commentary, CSIS Publication, Canada 1994.
- RESPERGER, István – KISS, Álmos Péter – SOMKUTI, Bálint: Asymmetric Warfare in the Modern Age – Small-scale Wars with Great Impact, Zrínyi Publishing House, Budapest, 2014. ISBN: 9789633275924
- SIMON, László – DR. MAGYAR, Sándor: Terrorism and its Indirect Effect in Cyberspace, National Security Review 2017/Issue No. 3, NKE, Budapest, 2017. https://www.uni-nke.hu/document/uni-nke.hu/nemzetbiztonsagi-szemle-2017-3-1.original.pdf (downloaded 28 October 2018)
- SZŰCS, László: The Psychology of Terrorism, https://honvedelem.hu/cikk/61828_a_terrorizmus_pszichologiaja (downloaded 02 September 2019)

- TOMOLYA, János – PADÁNYI, József: Terrorism and Guerrilla Warfare – Similarities and Differences, MHTT, Military Science 2014/Issue No. 1, Budapest, 2014. http://www.mhtt.eu/had/tudomany/2014/2014_elektronikus/11_TOMOLYA_PADANYI.pdf (downloaded 28 October 2018)
- TÓTH, Tamás: The Possibility of Using Social Engineering in Attacks perpetrated in Cyberspace and Escalating into Other Dimensions, National University of Public Service, Budapest, 2019.
- TÓTH, Tamás: New Challenges for Business Information Gathering as a Result of a Paradigm Shift in Organized Crime in the 21st Century, Professional Review 2018/Issue No 1, KNBSZ, Budapest, 2018. http://knbsz.gov.hu/hu/letoltes/szsz/2018_1_szam.pdf (downloaded 28 October 2018) HU ISSN 1785-1181
- VERES, Gábor – DR. BÁCS, Zoltán György: Terrorism in Northern Ireland, Terror & Counterterrorism 2017/Issue No. 3, TEK TT, Budapest, 2017. HU ISSN 2064-0374
- Warsaw Summit Communiqué – NATO Summit Communiqué, NATO, Warsaw, 2016.

TAMÁS KUN

CRITICAL INFRASTRUCTURES: THE BOTTLENECK OF SOCIETAL SECURITY

Abstract

With the appearance of cryptocurrencies, the idea of "making money" has been implemented again and just like in the 19th century, the famous 'Gold Rush' in California, this phenomenon is so much similar in many ways. Connecting critical infrastructures to the internet is one of the most dangerous impact on societal security, because that gives a big opportunity for remote access to a high-power source. Cybercriminals can exploit these weak points, which has been made by co-workers and serious problems can arise. On the other hand, there are also organizational activities against these assets, which can be targeted by political motive. The main concept of this paper is to spotlight the purposes of financial gain, the reasons behind the actions and the great risks which can evolve from these interests.

Keywords**:** critical infrastructure, cyber activities, vulnerability, financial gain, cryptocurrency

INTRODUCTION

Critical infrastructures are key elements for guarantee many things in everyday life. Power supply, financial transactions, commerce, telecommunication etc. Attacks against these are often violates homeland security, because they are destabilizing routine activities. A simple vulnerability caused by human failure can bring forth imponderable circumstances. For instance, the power plant on Paks contributes approximately 40% of Hungary's electricity production, which means its cancelling denies more than one third of electrical power. A financial institution denial can occur negative client behavior, halting trades on market, tax problems, delays in purchasing and billing procedures and so on. In order to maintain continuity, we must concern with these matters with high-level compliance. From another point of view, let's take a clear example of the topic. A bridge. On first thought, generally we are thinking about a bridge as a tool for crossing a river and traffic. But what if that bridge is blocked, destroyed or closed for maintenance? Struggles the base activity, the primary function. This is the reason why monitoring and protection of these infrastructures are relevant. Another one is the Internet, where millions communicate, do business, get information etc. day by day worldwide. Dealing with distance through technology is a fair minimum today, a fault in these nearly equal with a blackout.

Literature review

Johnson writes the following: *"Protection is something that is done to components and composites, which we will call more often systems."* In order to be

called a system, there must be an organized network of rules (that is how it can work). Furthermore, he describes it with an example of highway system, which is not only includes the network of roads, but its supporting subsystems as well (electrical lights, fresh and waste water, communication etc.). It is like a great puzzle, where every piece must fit in its place. On a higher level, these systems are mostly automated and controlled by remote access. The automated system controls called SCADA (Supervisory Control and Data Acquisition) systems. An oil pipeline, where the oil flows under pressure, too much pressure breaks the line, too little stops the flow. For proper function, the pressure must be on a measured level, which has been optimized in the control center. When the demand changes, the operators in the command center can change values fitting for that, but normally these systems are communicating with each other without human interference.[1]

Newlove-Eriksson et. al. referring on what systems a government should own (a few examples as telecommunication, non-road transport and energy) and the idea of the 'invisible hand' that is so well used in economic matters, in case of lowering costs and increasing efficiency. There was a trend around the millennium, where governments 'outsourced' (privatized) these in hope for getting better results in public administration, but did not calculate with the side effects, that would be an impact on national security.[2]

Losing direct control from its own power sources in any way is one of the highest threats for a country. There were several cases in the recent years, where confidential or sensitive information has been leaked out to private companies and individuals, which are carrying more risks and danger for the future, than enduring the cost of keeping these under governmental operation.

Critical Infrastructures in the crosshair of political motives

A. Oil facility attack in Saudi-Arabia

The world's largest oil processing facility (which is crucial to global energy supplies) has been attacked with drones supposedly by Houthi rebels. The attacks landed on a major oilfield, which is operated by Aramco and sparked a huge fire with smoke. The kingdom's output and export has been sabotaged with one source claiming 5 million barrels per day of crude oil production, which is nearly the half of the overall output said by Reuters. On behalf of that, Saudi Arabia is cancelling its output reports The Wall Street Journal. It is unknown that production or export have been affected by the attack.[3]

---

1 JOHNSON, Thomas A.: Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. Boca Raton, FL, Taylor and Francis Group, 2015. pp. 70-72. ISBN-13: 978-0367240387.

2 The Invisible Hand? Critical Information Infrastructures, Commercialisation and National Security. Lindy, Newlove-Eriksson; Giampiero, Giacomello; Johan, Eriksson. 2., Informa UK Limited, Taylor & Francis Group, 05 29, 2018, The International Spectator, Vol. 53., pp. 124-140. ISSN 1751-9721.

3 The Guardian: Major Saudi Arabia oil facilities hit by Houthi drone strikes; The Guardian. 09 14, 2019.

Figure 1: The regional map around the target[4]

On Fig. 1. we cannot see, but the attack came from a neighboring state from the south, Yemen. This facility is crucial, it is part of the world's oil production's bigger distribute known as the 'Strategic Ellipse'. This region includes the six Gulf states: Iraq, Iran, Qatar, the United Arab Emirates, Saudi Arabia and Kuwait (namely the Gulf OPEC) completed with Western Siberia where are more than two-thirds of the world's deposits are located at summary.

B. Targeting the U.S. power grid

The 'first disruptive cyber event' on March 5, where Russian hackers would have interrupt electricity for a few hours at least warned by U.S. Director of National Intelligence Dan Coats. The effect would be similar with the Ukrainian outages in 2015 and 2016, that caused problems with power to a quarter-million people in the region. This attack hit web portals for firewalls. *"The hacker or hackers may not have even realized that the online interface was linked to parts of the power grid in California, Utah and Wyoming."*[5]

---

4 Ibid.

5 SOBCZAK, Blake: Report reveals play-by-play of first U.S. grid cyberattack; https://www.eenews.net/stories/1061111289. (downloaded 09 November 2019.)

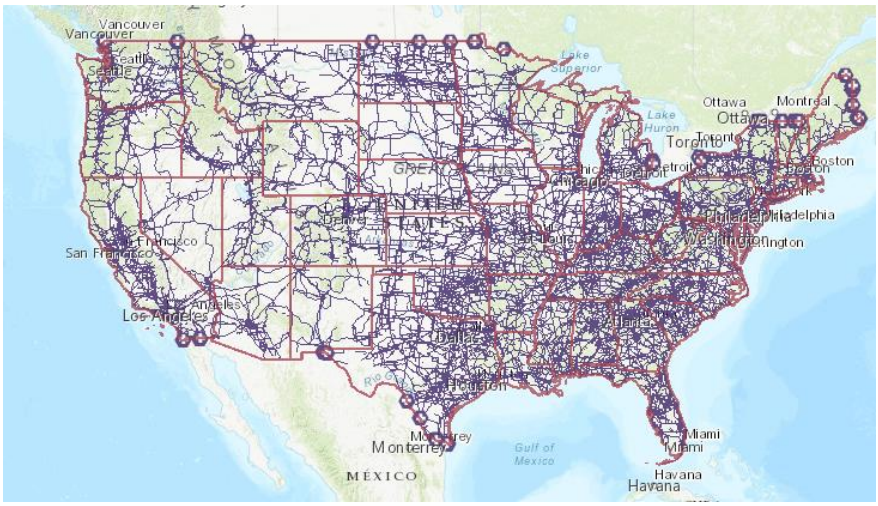

Figure 2: U.S. Electric transmission lines[6]

A report describes, that there was an exploit on the vendor's firewall, which enabled hackers to do reboot on devices. That resulted in a denial of service (DoS) attack, so denied communication between field devices and the control center. The monitoring tools notifications showed, that the firewall reboots occurred over 10 hours, where the offline status was less than five minutes per firewall.[7]
Fig. 2. shows, that the electrical lines are asymmetric in U.S., so that attack would be a fair warning. The first lesson from this, that the control center and field equipment shouldn't be connected to the internet or more layers should be added. Secondly, I would highlight that might be the denial of a service had been last less than five minutes, but hackers were able to cripple these systems over 10 hours simultaneously, what is nearly half a day.

C. Threat on nuclear facilities

Companies whom operating with nuclear power plants or other energy facilities has been targeted by cyber activities reported by FBI and Department of Homeland Security. Among the targets there were the Wolf Creek Nuclear Operating Corporation, who has a nuclear power plant near Burlington, Kansas. Hackers sent well-prepared emails linked with fake résumés with control engineering job offers to senior level employees, whom had access to critical industrial control systems. These documents implemented with malware, which after executing would send credential data to the attackers. During the attacks on May 11, 2017, U.S. President Donald Trump singed an executive order to strengthen the defense of both federal and critical infrastructure. The order has been addressed for public companies, instructed them to work together with governmental agencies to reduce the risks of cybercriminal

6 North American Electric Reliability Corporation (NERC); https://www.eenews.net/assets/2019/09/06/document_ew_02.pdf. (downloaded 12 November 2019.)
7 Ibid.

activities like energy disruption and outages. Critical infrastructures are getting commonly controlled by SCADA systems, which has been used by manufacturers and operators to monitor variables of field equipment. These systems can be also used to pinpoint unexpected problems as well, for example wrong pressure level, flowing rate, electrical charge etc. On the other hand, these can be compromised in opposing operators (cybercriminals) hands.[8]

In this case, we can detect a common spear-phishing attack method. The procedure is the following

1. detecting vulnerabilities and key actors,
2. deep investigation on victims,
3. making the bait (the job offers, which can be offer well-paid positions = financial gain),
4. launching the attack.

In common, these attacks can build a pattern with time, the difference will be only its context, the subject of the bait. Cybercriminals crafting their attacks on common motives, for instance 'easy' earnings or 'last' chance (fake time-out), so the victim may not realize the real reason in the background.

The new gold: cryptocurrencies

A. Ukrainian power plant and mining

On July 10, a power plant near Yuzhnoukrainsk in South-Ukraine has been raided by the Ukrainian Security Service (SBU). On the investigation they have been examining that the attackers could have used the mining rigs as an end point to breach the nuclear plant's network and gather information about the systems, such as physical defense and protection. There was another equipment which has been seized by the SBU, guarded by a military unit, who has been tasked with the protection of the power plant.[9]

[8] PERLROTH, Nicole: Hackers Are Targeting Nuclear. The New York Times. 07 06, 2017, p. 5.

[9] CIMPANU, Catalin: Employees connect nuclear plant to the internet so they can mine cryptocurrency. Zero Day. 08 22, 2019

Figure 3: Nuclear Plants of Ukraine[10]

On Fig. 3. we can see, that Ukraine has 15 nuclear reactors and the country's power grid depends on them heavily. There are geopolitical matters with the southern region, and there are massive Russian interests what are becoming reality with the blackouts that happened in 2015 and 2016. Creating chaos and destabilizing the electricity services may have resulted disappointment in the society, what could be adopted in the eastern side of the country or even expanding from the Crimea beneath vision. Cyber activities against these facilities are weakening the credibility of the ruling government, which can be result in further territorial losses.

B. Is that crypto would be the "new dollar?"

Kaspersky says, that both ransomware and miners have their own monetization (money making) model. In the case of miners, we can talk about money laundering, after infecting victim's PC, they are making coins, which is likely to be exchanged throughout legal sources (cryptocurrency exchanges) and the end they are coming out as real money from banks. In ransomware, the procedure quite simple: infect PC, decrypt data (and locking computer) and get the money from the ransom. Difference comes from detecting the attack, at ransomware attack detection is obvious, opposing with mining, where the hijack can be invisible. Miners can remain hidden, because if they operate their mining process with care, they can optimize resource allocation and the infected user won't realize that their PC is being used. An average person using

[10] World Nuclear Association. Nuclear Power in Ukraine. https://www.world-nuclear.org/information-library/country-profiles/countries-t-z/ukraine.aspx. (downloaded 15 November 2019.)

the PC for browsing the Internet (news, TV series, mailing etc.) which is using a low demand of CPU and GPU power, that the mining process requires.[11]

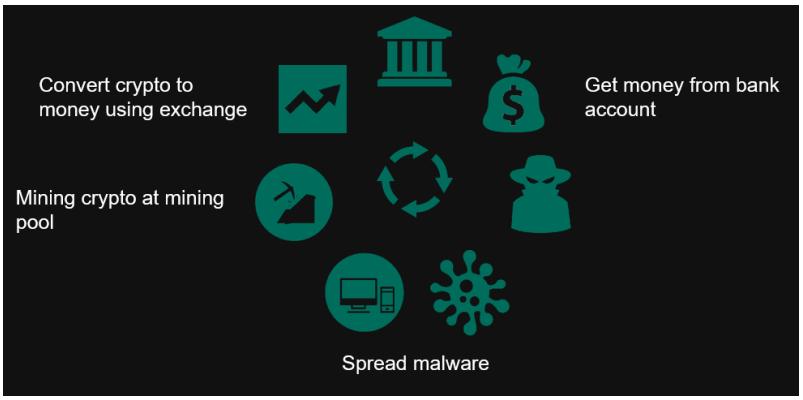

Figure 4: Miners' monetization scheme
(Source: Kaspersky Labs)

What we can see in Fig. 4. is a clear schematic for money laundering. First, we build up resources for mining (creating the Botnet, that is crime in the first place), selling the 'product' on legal markets and getting the money from a bank. In short term, just like a bank robbery without arms, but we are not stealing directly from the financial institute. But the real question is that all for just money? My answer is no, that is not that simple. Building up so much resource, building enormous networks just for financial gain would be a big joke. This logic used to be like secret services a couple decades ago. These networks just like military personnel, which can be used for planned operations: cyber-attacks.

C. The energy consumption of the Bitcoin

In mining the cost is not reasonable for individuals, but the overall is highly mentionable. The 'product of mining' the calculations need to verify the cryptocurrency requires more than 70 terawatt-hours per year, which is enough electrical power to supply 6.5 U.S. households with electricity according to Digiconomist. Costs could be distributed with the use of cryptomining malware and cryptojacking, so the owners of the host systems will pay the price for the upkeep. Most of cryptocurrencies have highly complex computational need to produce coins. Crescent Energy Supply calculated with average electricity prices and resulted in, that a single Bitcoin cost between 3224 and 9483 U.S. dollar in power, which means that business can be profitable only, if other people pay the bill. One more thing comes

[11] IVANOV, Anton – LOPATIN, Evgeny: Mining is the new black; Kaspersky Labs, 03 05, 2018. https://securelist.com/mining-is-the-new-black/84232. (downloaded 04 November 2019)

from this, that in order to make more calculations more computer needed, and these systems must be linked.[12]

We arrived at a few keywords: naivety, greed, botnets, cyber warfare supplies and so on. Since the appearance of the new payment method or tool, the motive is the same. Convince as many people as we can that governments and regulations, neither financial institutions are not needed in financial matters (e.g. purchasing transactions), at least two or more actor of a deal can agree without consultants. When authorities disappear from these transactions, criminal activities potential arises. A green light for hackers to use these resources as they want, first hand to launch DDoS attacks, gather information about the linked victims following connections (these can be friends, colleagues, family members etc.) which can be used for later espionage, industrial spying and other routine.

The main point about this story is the idea. The Bitcoin appears around the financial crisis in 2009. Offers a new currency which has no physical appearance, governmental or corporate background, the inventor's personality is unknown, only a nickname what we know with hundred percent. Another fact, that with many stock market product, speculations and bidding against each other remains as 'value'. Tech companies like graphic card manufacturers profited well from this, after that has become established fact GPUs have higher potential making the calculations, and this extra charge has been implemented in their products price.

Conclusion

Cyber activities against critical infrastructures should be treated such as war crimes. There is a long discussion between the experts of this field. In my opinion, these events that occurred recently must be organized strategically. Small groups of hackers won't target nuclear facilities just for money. They are attacking with purpose, attacking with territorial demands, backed with nation states. The so often called cyberwarfare is not the future, it is the present. Energy and information are key concepts of our everyday life, I think nearly rivals with food supplies and water. Without energy, the computers are not working, we are getting cut off from communication, media, health services, databases, traffic control and the end of the line is far away. The world is highly connected and digitalized, with many things that has physical appearance back in the day.

Analyzing the connection between critical infrastructures and societal security has been showed, that in several cases when governments are losing control, they are losing twice. One problem is coming from the other, because these structures are similar with castles. In the medieval times, when a nation lost a castle, it resulted territorial loss, the encountered army moved on the field towards the capital. The concept would be the same, when a government loses control over a power source (that can mean information as well, not just energy), the enemy is one step closer, but in parallel their own citizens dissatisfaction will be the next. These actions are against

[12] LEMOS, Robert: Tallying Up the Hidden Costs of Cryptomining Malware. Symantec.com, 06 20, 2018. https://www.symantec.com/blogs/feature-stories/tallying-hidden-costs-cryptomining-malware. (downloaded 04 November 2019.)

the order, in methods they are similar with terrorism, just there are no bombs. Data protection and financial regulation are big problems today (many data breaches and the question of cryptocurrencies), ascending money laundering and financing terrorism beneath legal sources (through dark web) will be worse in the recent future. NATO has Cyber Defense HQ since 2008 in their lines and politicians are aware of the challenge either, because the topic appears more and more in their communication. Standards, protocols are working in the best of cases, but resilient workforce with critical-thinking should be best practice to counter these.

On technological side of the topic, CI-s should be hidden, or sealed away from internet connection points, but if we are clinging for remote access anyway, few layers of security are not enough for guarding such as objects against cyber-attacks. More level security is a guarantee for extra time to act but does not mean superior protection. In this field, we must have a backup plan for any scenario, never put everything on one card. The human interference cannot vanish completely from the process, we must establish option for emergency interaction as an opportunity, but the main point is: in physical construction.

Bibliography:

- CIMPANU, Catalin: 2019. Employees connect nuclear plant to the internet so they can mine cryptocurrency; Zero Day. 08 22, 2019.
- IVANOV, Anton – LOPATIN, Evgeny: Mining is the new black; Kaspersky Labs, 03 05, 2018. https://securelist.com/mining-is-the-new-black/84232/.(downloaded 04 November 2019.)
- JOHNSON, Thomas A.: Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. Boca Raton, FL: Taylor and Francis Group, 2015. pp. 70-72. ISBN-13: 978-0367240387.
- LEMOS, Robert: Tallying Up the Hidden Costs of Cryptomining Malware. Symantec.com, 06 20, 2018. https://www.symantec.com/blogs/feature-stories/tallying-hidden-costs-cryptomining-malware (downloaded 04 November 2019.)
- North American Electric Reliability Corporation (NERC). 2019. 09 04, https://www.eenews.net/assets/2019/09/06/document_ew_02.pdf. (downloaded 12 November 2019.)
- PERLROTH, Nicole: Hackers Are Targeting Nuclear. The New York Times. 07 06, 2017, p. 5.
- SOBCZAK, Blake: Report reveals play-by-play of first U.S. grid cyberattack; 09 06, 2019. https://www.eenews.net/stories/1061111289. (downloaded 09 November 2019.)
- The Guardian: Major Saudi Arabia oil facilities hit by Houthi drone strikes; The Guardian. 09 14, 2019.

- The Invisible Hand? Critical Information Infrastructures, Commercialisation and National Security. Lindy, Newlove-Eriksson; Giampiero, Giacomello; Johan, Eriksson. 2018. 2., Informa UK Limited: Taylor & Francis Group, 05 29, 2018, The International Spectator, Vol. 53., pp. 124-140. ISSN 1751-9721.
- World Nuclear Association. Nuclear Power in Ukraine; [https://www.world-nuclear.org/information-library/country-profiles/countries-t-z/ukraine.aspx. (downoladed 15 November 2019.)

JÓZSEF STEIGLER PhD

THE REBIRTH OF AIRCRAFT PRODUCTION IN HUNGARY, THE INTRODUCTION AND APPLICATION FIELDS OF AIRCRAFT MANUFACTURED BY MAGNUS AIRCRAFT LTD.

Abstract

In Hungary, by the end of 2011, 30 companies have acquired the AS 9100B certification for the aerospace industry. Among those 30 companies there are five major aerospace companies as follows: GEES Veresegyház; Lufthansa Technologies Budapest; Flame Spray Gödöllő; Magnus Aircraft Zrt. Pécs-Pogány; Diehl Aircabin Debrecen. Three types of aircraft are manufactured in Hungary: 2-seater gyrocopter, 1-seater racing aircraft, and 2-seater plastic sport aircraft.

***Keywords*:** Hungary, aircraft production, Magnus Aircraft Ltd.

Introduction

In accordance with the intentions of the Hungarian Government, particular attention should be paid to the development of the defense industry in Hungary, the use of the tools developed and manufactured in Hungary in the high-level performance of the State's tasks. These intentions are formulated and performed during the implementation of the Zrínyi Plan[1] started off in the Hadik Plan.

In order to achieve the Government's goal, the Government could, by means of significant and efficient support, start the resurrection of the bases of aircraft manufacturing in Hungary, and the establishment of the necessary manufacturing base in Pécs-Pogány region.

The emerging high-tech manufacturing base is of special importance for the national economy and national security aspects, as far as both the manufactured raw material and the aircraft that would be produced as a result of developments.

In our article, we would like to give an insight into the fields and possibilities of application, and the advantages of the application of the aircraft manufactured by Magnus Aircraft Ltd., a Hungarian company representing the Hungarian development and manufacturing capacities, being exclusively in Hungarian ownership.

[1] "Zrínyi 2026 National Defence and National Defence Development Program." (In Hungarian) https://honvedelem.hu/files/files/108409/zrinyi2026_190_190_7.pdf (downloaded 02 March 2019)

About us

101 years after János Adorján's flight with his plane called "Szitakötő" (Dragonfly) and powered by a two-cylinder engine, and designed by himself and bearing his name, the Magnus Aircraft Ltd. was established.

Our company has been dealing with

- design,
- manufacturing,
- and sale of composite, two-seater aircraft since 2011 in the ultra-light (UL) and light-sport aircraft (LSA) category under the brand name "Fusion 212".

In 2014, our company together with the Siemens Group started developing a common electric powered aircraft called eFusion. The maiden flight of the prototype was successfully performed in April, 2016.

Starting in the second half of 2018, we may say that our aircraft is 100% made in Hungary, because we manufacture the airframe in Hungary with domestic experts.

Our company is committed to the revival of the Hungarian aircraft industry in accordance with the economic policy and economic development efforts of the Government, which has been pursued so many times in recent decades.

Our goal is that the aircraft developed and manufactured in Hungary should be part of the Hungarian Air Force, which would be established as a result of the force development, would become part of the pilot training implemented in the framework of defence education, and the aerospace industry in Hungary should be successfully represented on the world market.

It is not a secret plan for us to reorganize air transport within Hungary, with the involvement of the Government, one hundred years after the Austro-Hungarian Ministry of War issued a bill for the uniform regulation of air traffic on 24 November 1917. At the time of the change of the political system (1990), there were 30 registered airports and airfields in our country, by which Hungary was at the forefront on a European level.

Magnus Fusion aircraft designed in Hungary

Figure 1: Magnus Fusion 212 in flight[2]

The company designs, manufactures and continues the international sale of two-seater aircraft in UL and LSA categories. In addition to a strong fuselage, it has a wide range of equipment, both in the drive chain and in the interior, ensuring market price competitiveness.

Our target groups:

- private individuals,
- companies,
- training bases,
- industrial and control bodies,
- medical courier service,
- disaster management,
- armed forces and law enforcement agencies,
- border guard and facility protection, protection against terrorism,
- agriculture, forestry and wildlife management,
- environmental protection.

Market leeway factors

The Magnus Fusion 212 is the most economical sport and training aircraft in the world.

1. Aircraft equipped with internal combustion engine do not require any special fuel; they are operated with 95-octane unleaded gasoline (usually referred as MOGAS).

[2] https://www.magnusaircraft.com/media (downloaded 02 March 2019)

2. Due to the design of the airframe, it is also able to perform aerobatic training at low operating costs.
3. Due to the materials used for manufacturing, the aircraft operating at low height has a significantly small effective radar cross section (RCS) value, so it can be used for sensitive border guard and military reconnaissance purposes.
4. The seats located next to each other are very suitable for training purposes and pilot training.
5. As a result of continuous development, we are able to participate in joint ventures with Hungarian and foreign universities, as well as scientific entities in cooperation with Hungarian and foreign sales partners. The chance to do so may further expand the sales opportunities in Hungary and in partner countries, as well as may provide a longer-term cooperation and the establishment of joint manufacturing facilities.

Engine	Rotax 912 ULS/iS // ULPower 260iSA // ROTAX 915 iS
Propeller	MT Propeller / DUC / Woodcomp
Power	80-100-130 HP
Length	6,700 mm
Wingspan (with winglet)	8,330 mm
Wing area	10.834 m^2
Load factor limit	+6/-3 g
Empty weight / with rescue parachute	cca. 297 kg (base version)
MTOM / with parachute	472.5 kg UL / 600 kg LSA
Fuel capacity	90 litres
Baggage capacity	20 kg
Seating capacity	2
Cockpit width	1,170 mm
V_A - maneuvering speed	194 km/h - 104 kts
V_H - maximum horizontal speed	240 km/h - 130 kts
V_{NE} - never exceed speed	280 km/h - 151 kts
V_{cr} - cruising speed at 75% power	185-240 km/h / 100-130 kts
Service ceiling	12,000 feet
Stall speed (with flap)	45 kts
Takeoff roll	120-130 m
Landing roll	150-200 m
Cross wind landing	20 kts
Fuel consumption	16-21 litre/hour
Range	800-1,100 km

Figure 2: Technical specifications of the Magnus Fusion aircraft

Fusion 212 comparison

Normal version

Advantages	Disadvantages
Low price	Relatively sensitive flight controls
Low operating costs	
Easy operation	
Side-by-side seating arrangement	
Ergonomic cab	
Built-in rescue system	
Benevolent and does not tend to fall into corkscrew	
Can be flown for aerobatics between +6 and -3 g	
Short takeoff and landing distance	
220 km/h cruising speed	
1,100 km range	

Agricultural application (under development)

Advantages	Disadvantages
Low price	Can take small amount of chemicals (150 litre)
Low operating costs	Can spray in a relatively narrow zone
Easy operation	
Short take off and landing distance	
Good manoeuvrability	
Narrow turn radius	
Can be quickly prepared again	
Can be used over a smaller area	

The agricultural version of the Fusion 212 is a low-cost solution even for small farms to control pesticides with chemicals. It can also be used effectively to cover smaller areas that larger aircraft cannot. It can also be operated from short, poorly prepared runways. It operates with traditional car petrol (RON95), compared to its larger counterparts that use more expensive and less accessible aviation gasoline. Once the chemical tank is empty, it can be quickly prepared for the next take-off.

Surveillance (Sentinel system)

Advantages	Disadvantages
Easy operation	Higher operating costs compared with drones
Due to the material of the fuselage, it can fly covertly in the lower region of the radar height	
Long flight time	
Long range	
Narrow turn radius	
Onboard operator	
Short takeoff and landing distance	

The surveillance version of the Fusion 212 can operate with a variety of cameras (daytime, night vision, infrared, and a combination of these). It is possible to transfer real-time data to a ground station that can be quickly installed and transported in a rolling container. Its range can be increased with the help of terrestrial repeaters. If there is no need for a real-time relay, the data can be stored on board and downloaded later on the ground. The operator on board can make immediate decisions based on their onsite observations. The aircraft may also operate from short, poorly prepared temporary runways.

Specification of the Sentinel camera system

Electro-optical sensor
Name: Hitachi DISC 120R
Vertical FOV: 37.9°-1.3°
Resolution: HD 720p 1270×720 optical zoom 30×

IR sensor
Name: XBn
Type: 3-5μ staring array, cooled
IR lens: 15×zoom lens 18-275 mm
Vertical FOV: 24.5°-1.5°
Resolution: SD 640×480
Frame rate: 30 fps

Laser rangefinder
Type: diode laser
Range: up to 5,000 m
Accuracy: better than 1 m

Laser illuminator
Wavelength: 830 nm
Power output: 50 mW

IR sensor DRI
Target: human/NATO
Detection: 8.6 km/12.4 km
Recognition: 2.9 km/7 km
Identification: 1.4 km/3.5 km

Sentinel surveillance aircraft versus drones

Drones

a) Extremely expensive production;
b) Expensive maintenance;
c) The fact that they are procured from abroad is a national security risk by itself, as the intentions and defence capability of the State may become known;
d) The possibility of a human error from the remote control is very high. As a result, the device may be damaged or become uncontrollable, or its capabilities may become limited;
e) There is a high risk of further damage caused by a device that has been destroyed or with limited control;
f) There is a serious risk of using drones in case there is a computer malfunction or loss of control over the device, so it can fall into unauthorized hands;
g) There is a high risk of significant collateral damage or casualties when using drones;
h) A serious consideration should be given to using drones in a so-called "Cold Heart" way, it is a coward process that denigrates the conflict to be managed because it may seem like a video game and would not encourage ethical decision-making;
i) Drone control link is vulnerable, can be cracked and exposed to virus infection;
j) The use of drones is complicated by the fact that their certification and usage circumstances are not sufficiently legally regulated and their social acceptance is very low;
k) Many problems have not yet been solved in the technical field. Loss of visual perception is a common problem. There is no resolution of air traffic control anomalies.

Advantages for using Magnus Sentinel aircraft

a) Pilot and operator perform their duties side-by-side, better crew interactions.
b) It is cheaper than satellite-based drone control
c) Detecting drones from an aircraft significantly easier, free visual perception is more effective
d) Detection, perception and response are also effective even in difficult flight conditions
e) Larger range, longer protection time
f) Radio-electronic jamming can be better performed

g) Cost-effectiveness
h) Longer life
i) Larger load capacity, higher take-off weight
j) Combined with a camera system, it is a more efficient surveillance and protection device

Public relations and objectives

In developing social relationships, it is of paramount importance that using our capacities we fully participate in our country's patriotic commitment and sacrifice by increasing it for the protection/defence of Hungary, taking into account volunteering, in the implementation of defence/protection education and pilot (pre-) training (known as Initial Flight Screening, IFS in the U.S.)

During this phase, candidate pilots are screened, motivated and prepared for entry in the undergraduate pilot training program. Since this is the absolute beginning of flight training, skills learned in Initial Flight Training (IFT) are very similar to the skills required for obtaining a private pilot license (PPL).[3] The program is therefore performed at civilian flight schools as well, and is typically executed in light aircraft (LSA or VLA).[4] This training consists of three blocks:[5]

1. *Orientation*: In this part of the program, basic aircraft control is practised together with some basic manoeuvres. Examples are cockpit organisation, departure and arrival, trim use and clearing.
2. *Fundamental manoeuvres*: The next step builds further on basic aircraft control and includes some additional manoeuvres like traffic patterns, steep turns and ground reference manoeuvres.
3. *Navigation fundamentals*: In addition to the previously learned skills, situational awareness is built and students learn the basics of navigation.

The most important objective of social activity is to be able to ensure the broadest possible knowledge and commitment to the protection/defence of Hungary in order to maintain and develop our country's defence/protection capabilities. By making good use of the aircraft's flight and operating benefits, the advantages of manufacturing it in Hungary, it is important even for the high school age youngsters to get acquainted with flying through pilot training and pre-training. With this, not only the expressed aspirations of a multitude of young people will be satisfied, but also a complex defence/protection education program will be elaborated, which will enable to lay the foundations of a career, with regard both to its civilian or military usage.

---

3 BAZZOCCHI, E.: Military Pilots Training and its Equipment; Aeronautica Macchi, 1978. Lecture held at the Federal Institute of Technology in Zürich.

4 Definitions see in: European Aviation Safety Agency, ED Decision no. 2010/014/R: Definitions and abbreviations used in Certification Specifications for products, Parts and Appliances; European Aviation Safety Agency, Cologne, 2010.

5 Air Education and Training Command, Combat Systems Officer (CSO) Initial Flight Screening (IFS) for Civilian Part 61/141 Flight Schools, Randolph AFB: Air Education and Training Command, 2009.

With all this intent, the participation in the Cadet Program can provide an opportunity for young people committed to defence/protection.[6] Appropriately building on the training system of the schools involved in the program, the training system integrated in the education period ensures its harmonization with the curriculum subjects and to acquire the necessary theoretical knowledge as follows:

- aerodynamics: 10 hours – physics,
- airframes and structures: 10 hours – physics,
- engine knowledge: 8 hours – physics,
- instrumentation: 15 hours,
- meteorology: 20 hours – geography,
- navigation: 20 hours – geography,
- air law: 14 hours,
- human performance and limitations: 10 hours – biology,
- communication: 18 hours.

When providing the teaching staff with the necessary skills and experience for training, the involvement of retired pilot and technical support personnel in training should be considered.

In addition to the schools participating in the Cadet Program, the involvement of schools dedicated to defence/protection education in the training system requires great attention.

It is necessary to provide responsibility and opportunity for the implementation of pilot training, national defence training in Hungary in accordance with the mission of the Defence Sports Association, and of the establishment of Defence Sports Centres.

The appearance in higher education can further strengthen the implementation of an independent pilot training in Hungary. The most important base for this is the National University of Public Service, into whose high-level training the multi-purpose aircraft developed and manufactured in Hungary can be easily integrated.

Parallel to the accomplishment of educational tasks, it is very important to economically optimize the number of flying hours of professional flight crews, to increase flight safety and to provide continuous training. The Hungarian aircraft type meets the requirements of professional flight crew training in every respect, with the huge advantage (in addition to economy and its production in Hungary) that it significantly reduces the exposure to external impacts of training.

---

[6] BALI, Tamás: Conceptual Approach to Pilot Recruitment; Aviation Science Periodica (Repüléstudományi Közlemények, in Hungarian) XXVIII. 2016. orcid.org/0000-0001-6098-8602 (downloaded 02 March 2019)

International relations

The Fusion 212 aircraft offers significant international cooperation opportunities due to its multipurpose features, based on international licenses and certifications obtained.

The leaders and specialists of the Ministry of Foreign Affairs and Trade and of the Ministry of Innovation and Technology play a key role in the development of international relations, thus enabling its involvement in international trade using diplomatic channels and tools in order to become integrated in the international innovation process.

In addition to traditional trade and military diplomacy, we have achieved considerable support in establishing international relations by addressing the Honorary Consular Network, conducting production and flight demonstrations organized for them.

The implementation of national independent pilot training is a primary national security task for all sovereign states, thus the technology export provides an opportunity to cooperate in its implementation considering national economy and national security aspects. China has the greatest potential for this, where the manufacturing and pilot training cooperation is highly advanced based on high-level consultation and preparatory work.

In line with the Government's foreign trade objectives, South Africa is a major focus area. In some countries in this area (Kenya, Namibia), the implementation of activities in connection with assembly, training and special applications (e.g. wild game management, wildlife protection) is very advanced.

We should not ignore the international tradition of hobby flying, whereby the US and Australia, the states of the Arabian Gulf present the greatest demand alongside the leading European economic powers.

In many cases, international relations also raise the need for improvements such as the issues of availability for airborne medical services, or the emergence of "air taxi" service in Hungary.

Summary

After a many decades long break in Hungary’s aircraft manufacturing, nowadays its government-sponsored development and manufacturing activities is of particular importance in revitalizing this branch of the industry.[7]

The available technological development and the multi-purpose usage of aircraft in Hungary provide outstanding opportunities for the aerospace industry and the

[7] József ROHÁCS: Impact of Air Transport and Aeronautical Industry of the Economy; Aviation Science Periodica (Repüléstudományi Közlemények, in Hungarian) XXX, 2018. orcid.org/0000-0002-4607-9063

interdisciplinary areas in our country and in the international environment, as well. The implementation of this activity is linked to several Government programs, which ensure the protection/defence of Hungary, national defence/protection education, high-tech operation and the implementation of the employment policy goals.

The development of the aircraft industry in Hungary has a global market outlook in terms of market opportunities that could enable Hungary to play a leading role in civil and military aviation in some regions.

Bibliography:

- Air Education and Training Command, Combat Systems Officer (CSO) Initial Flight Screening (IFS) for Civilian Part 61/141 Flight Schools, Randolph AFB: Air Education and Training Command, 2009.
- BALI, Tamás: Conceptual Approach to Pilot Recruitment; Aviation Science Periodica (Repüléstudományi Közlemények, in Hungarian) XXVIII. 2016. orcid.org/0000-0001-6098-8602 (downloaded 02 March 2019)
- BAZZOCCHI. E: Military Pilots Training and its Equipment; Aeronautica Macchi, 1978. Lecture held at the Federal Institute of Technology in Zürich.
- European Aviation Safety Agency, ED Decision no. 2010/014/R "Definitions and abbreviations used in Certification Specifications for products, Parts and Appliances". European Aviation Safety Agency, Cologne, 2010.
- Lafortune, T. J. Preparing Specialized Undergraduate Pilot Training Graduates for F-35A Training, Master thesis, United States Air Force Academy, 2010.
- Magnus Aircraft Zrt. https://www.magnusaircraft.com/media (downloaded 02 March 2019)
- ROHÁCS, József: Impact of Air Transport and Aeronautical Industry of the Economy; Aviation Science Periodica (Repüléstudományi Közlemények, in Hungarian) XXX, 2018. orcid.org/0000-0002-4607-9063
- "Zrínyi 2026 National Defense and National Defense Development Program." (In Hungarian) https://honvedelem.hu/files/files/108409/zrinyi2026_190_190_7.pdf (downloaded 02 March 2019)

AUTHORS OF THIS ISSUE

- **MRS. JÚLIA FELEGYI** is a PhD student at the Public Service University;
- **MR. KRISZTIÁN JÓJÁRT** is a PhD student at the Public Service University;
- **MR. TAMÁS KUN** is a PhD student at Óbuda University Doctoral School of Safety and Security Sciences;
- the late Lieut. **COL. ZSOLT LAKATOS** (†) was a military and security policy as well as terrorism expert;
- **LT. BALÁZS PÜSPÖK** is a security and military policy expert,
- **COL (OUT OF SERVICE) JÓZSEF STEIGLER PHD** is the Director for Security of MAGNUS;
- **Mr. TAMÁS TÓTH** is a cyber security expert.

EDITORS OF THIS ISSUE

- **LT.COL. ANITA DEÁK PHD**;
- **LT.COL. (RET.) CSABA GÁL** is a security policy and military technology expert;
- **COL. JÓZSEF KIS-BENEDEK PHD** is an independent terrorism and security policy expert;
- **COL. SÁNDOR MAGYAR PHD** is an IT and cyber security expert.
- **LT.COL. BÉLA PUSKÁS** is a cyber security expert;

CONDITIONS FOR PUBLISHING IN THE NATIONAL SECURITY REVIEW

Requirements to be met by the writings

Ethical requirements:

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

Content requisites:

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

Formal requisites:

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

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

Formal requirements of academic communications

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

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

Bibliographical reference

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

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

Citations

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

First citations

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

Examples:

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

List of biographical references (biography):

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

Examples:

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

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

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

Requirements for abbreviations and foreign terms:

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

Points of Contact of the MNSS Scientific Board:

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

E-mail: natsecreview@gmail.com

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