Daniel Brezina[1]

Hybrid Warfare: Case Studies

The primary motivation for choosing the topic under the name *Hybrid Warfare: Case Studies* was that many ambiguities and problematic areas in this area had not been addressed in the past. Suppose individual countries are to be sufficiently prepared and leading government officials can respond adequately to the impact of hybrid threats. In that case, it is necessary to streamline decision-making processes. This publication's primary goal is to analyse selected topics of international political and social events and their subsequent application to the concept of hybrid threats. The case studies examine different forms of hybrid threats and, simultaneously, allow gathering information from which to build a "database" for crisis management, national or international. Case studies present valuable lessons that can be used to streamline decision-making processes and create new strategies. The importance of case studies increases if we want to learn from mistakes that have occurred in the past. The problem can be their misunderstanding and eventual rejection by the competent authorities or the public. The basis for the preparation of the publication was the scientific research activity of the author, as well as the opinions and attitudes of many professionals and experts from various domestic and foreign institutions dealing with the issue of hybrid threats.

Theoretical background

The number and severity of hybrid threats have been increasing in recent years. This phenomenon began to come to the fore especially after the annexation of Crimea by the Russian Federation. Individual countries are confronted with many requirements, the aim of which is to ensure the required level of crisis prevention with an emphasis on hybrid threats and the ability to effectively and efficiently respond to real threats. This is connected with the need to make optimal decisions and effectively use the available resources needed to deal

[1] Armed Forces Academy of General Milan Rastislav Štefánik.

DOI: https://doi.org/10.36250/01237_11

with hybrid threats. With the development of more complex techniques and technologies, the possibility of the emergence of hybrid threats that hurt the natural evolution of human society increases quite often. Questions about preventing their occurrence and solutions are becoming an increasingly topical subject. They can affect a large number of inhabitants and hurt a large area. Their consequences primarily negatively affect the human community and the material, social and cultural values in the territory affected by the influence of hybrid threats. In some cases, the functionality and stability of the overall operation of the state's economy may be threatened and disrupted. In the introduction of the paper, it is necessary to define the basic terms and concepts related to the solved problem. These will be part of the theoretical basis for analysing selected case studies and will allow us to assess the conditions in which different forms of hybrid threats operate. Several factors influenced the choice of individual terms and their concepts. The issue of fighting in a mixed way is quite complicated. It is necessary to have specific knowledge about systems' behaviour, functions and connections to manage the negative consequences of hybrid threats. Hybrid threats are defined as threats using a specific combination of political, military, economic, social and information means and conventional, irregular, catastrophic, terrorist and criminal activity methods with various state and non-state actors.[2] Hybrid threats are interconnected and operate in the disruption of state functions. As part of conducting a mixed operation in the grey zone, the space is not limited by physical barriers. In this context, actors can use cyberspace, media, operational space, diverse spaces of operations, etc.[3] A tool of hybrid threats can be massive disinformation campaigns and the use of social media for propaganda or radicalisation, recruitment and direct control of supporters. A hybrid attack represents the synchronised use of several power tools adapted to specific weaknesses in the entire spectrum of social functions to achieve a synergistic effect. The advantage of a hybrid attack is that it is complicated to assess whether the application of hybrid tools is taking place in the initial stages. These can be applied for a more extended time, with the damage starting to show itself only after a delay when the target's ability to defend themselves effectively

[2] Glenn 2009.
[3] Jurčák–Turac 2018.

due to these attacks is already significantly impaired.[4] Hybrid threats can also be directly or indirectly related to Chaos Theory. The butterfly effect points out that the movement of a butterfly's wings on one side of the planet can, over time, cause a hurricane on the other side of the earth. These are relatively minor events that can trigger crises. A prerequisite for proper and effective prevention, as well as an effective solution to hybrid threats, is an understanding of their essence, the function and tasks of the bodies responsible for their preparation and resolution, their purpose, culture and processes taking place within them.[5] In case of hybrid threats, it is difficult to predict their emergence and comprehensive course. In addition, the negative impact of hybrid threats can cause several secondary crises, whether in the public or private sector. For this reason, the existence of a specific type of management that deals with this issue and is known as crisis management is essential. For the first time, the term crisis management was used and practically applied in 1962 during the Cuban crisis. American President John Fitzgerald Kennedy assembled a group of experts from various fields whose task was to prevent the outbreak of World War III and to find a peaceful solution to the international crisis during the Cold War.[6] Over time, crisis management has established itself in various areas not only of military but especially of a non-military nature, such as politics, the economy and the field of public administration. The subject of crisis management can be a state, or a group of conditions for joint activity, for example, in the military or the economy. Crisis management, as one of the primary tasks in the field of security, includes various military and non-military procedures that must be carried out, whether in the phase of prevention or response to emerging crises. The North Atlantic Alliance (NATO) has various political–military tools at its disposal to deal with problems with an emphasis on hybrid threats that may threaten the security of the territory and the population of all members of the Alliance.[7] The fundamental theoretical model of crisis management (Figure 1) consists of four crisis management processes – prevention, crisis planning, response and recovery.

4 Cullen – Reichborn-Kjennerud 2017.
5 Ishikawa–Tsujimoto 2006.
6 Šimák 2016.
7 NATO 2022.

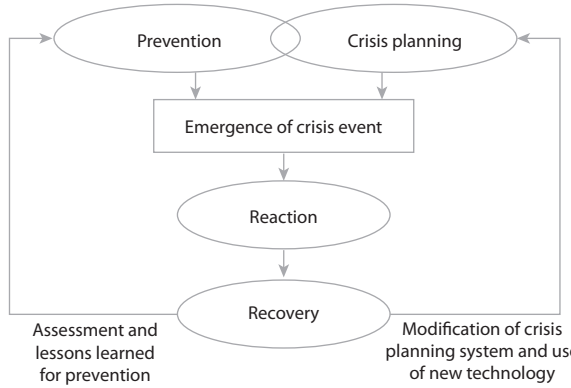

Figure 1: The basic theoretical model of crisis management
Source: Horemuž 2010

In the prevention phase, the essential step is identifying and assessing all current risks and threats, followed by processing crisis forecasts and scenarios. The primary goal of prevention is the prevention of adverse consequences of crises through various measures and activities. A separate and no less critical phase of crisis management in the preparatory phase is crisis planning, within which different types of crisis plans are processed.[8] The protection of society created the prerequisites for connecting the prevention phase and the planning documents. The period of preparation for solving crises and their emergence is followed by the period of solving problems. An immediate response to a situation requires the rapid deployment and coordination of the forces and resources necessary to solve it. This phase follows from the direct acquisition of information about the emergence of a crisis and its correct assessment and evaluation. The immediate response is carried out through various activities, the primary objective of which is to save human lives and material values, the environment and cultural monuments. The recovery phase is predominantly developmental, allowing the system to return to its original stabilised (pre-crisis) state. Feedback is of great importance in the basic model of crisis management. It represents a means for improving the quality of crisis management at its various levels.[9] Crisis manage-

[8] Šimák 2016.
[9] Sanseverino-Godfrin 2016.

ment is one of the primary tasks of NATO. As part of implementing an adequate response to emerging crisis phenomena of a natural or military nature, Marinov developed a strategic concept of crisis management within NATO. The model assesses the current situation and creates a comprehensive response through a six-phase crisis management process:

- identification of risk factors with subsequent warning of the population and notification of specific bodies and institutions involved in crisis management
- comprehensive assessment of the crisis phenomenon
- planning phase
- phase of the adequate reaction
- implementation of other necessary measures to minimise the negative consequences of crisis phenomena of a natural or military nature
- transition to a phase that no longer poses a threat to countries that are members of NATO[10]

Marinov's model allows crisis staff and committees within the NATO institution to coordinate their work and provide information to the North Atlantic Council. The individual phases are not precisely given from a time and organisational point of view. They can overlap, and their length depends on the specific situation. One of the basic approaches that will allow us to assess the conditions in which different forms of hybrid threats operate is the analysis of selected case studies. There are five stages to creating a good case study. In the first phase, deciding whether a case study is a suitable method for investigating the selected problem is necessary. The second phase consists of defining the case, the third of data collection and the fourth of their analysis. In the fifth, i.e. the final step, the interpretation occurs, where the researcher's task is to state what he found out about the case during the research.[11] Similarly to the definitions of "hybrid threats" and "crisis management", it is also possible to note considerable terminological inconsistency and ambiguity in the purpose of the term case study. A case study is an ideographic investigation of one individual, family, group, organisation, village or society; its primary purpose is a description. Attempts at explanations are also acceptable.[12] The basis of a case study is

[10] Marinov 2011.
[11] Creswell–Poth 2013.
[12] Rubin–Babbie 2001.

capturing the complexity of cases, describing relationships and their integrity.[13] The premise of the case study is that we can understand many similar cases based on the analysis of one point.[14] A high-quality case study should contain five essential characteristics: the significance of the case, the completeness of treatment, consideration of alternative perspectives, a sufficient amount of data, creativity and attractiveness in therapy.[15] A case in a case study can be explained as a spatially bounded phenomenon observed at one point in time or one period of time. A case in a case study can also represent a fixed phenomenon that is an example of a class of similar phenomena forming a population.[16] The objective of the quantitative research strategy is to standardise specific work procedures. Within the framework of a qualitative research strategy, it is essential how the process of working with the researched object and the specifics of the researched case proceeds, as well as understanding ongoing changes and interactions. As it follows from the individual characteristics of the case study as a research method, many data sources are essential, especially for methodological triangulation. Data analysis is a demanding activity due to its complexity and quantity.

Case study: Czechoslovak Sudetenland

When examining the definition of the term hybrid war in detail, it can be concluded that the manifestations of this specific type of war are not only characteristic of the period of the 21st century but can be dated much earlier. One of the first ways of conducting a hybrid war was, for example, the annexation of the Czechoslovak Sudetenland to Nazi Germany. The creation of the Czechoslovak Republic in 1918 was preceded by a long academic debate between prominent Czechoslovak politicians and philosophers, which, since the time of Jungmann and Bolzano, concerned the issue of the organisation of the Czech state (territorial principle versus national principle). Tomáš Garrigue Masaryk, the first Czechoslovak President, with his idea of Czechoslovakism, eventually became the most influential thinker and figure in the creation of the

[13] Hendl 2005.
[14] Hendl 2016.
[15] Yin 2009.
[16] Rohlfing 2010.

Czechoslovak Republic.[17] The problem lay in the designation "Czechoslovak" being somewhat imprecise. About 50% of Czechs (approximately 6.8 million), 24% of Germans (approximately 3.2 million), 15% of Slovaks (approximately 1.9 million) and other national minorities such as Hungarians lived in the territory of the then Czechoslovak Republic, in addition to Ukrainians (Rusyns), Jews, Poles and others.[18] President Masaryk offered the Germans to eliminate their anti-Czech attitude and try to build a Czechoslovak state with other citizens. He promised them minority rights and a democratic way of dealing but assured them that the border territory would remain with Czechoslovakia.[19] Soon after the declaration of the Czechoslovak Republic, the military occupation of predominantly German-inhabited territories followed, which, since the end of the 19th century (especially in the Chebsko region), formed one of the pillars of extreme pan-Germanism.[20] The process of assimilation of the Sudeten Germans took place mainly in the form of migrations of the Czech population to create ethnically diverse areas.[21] The year 1938 became a fundamental turning point in the Czechs' view of the Sudeten Germans, especially after the events connected with the signing of the Munich Agreement. The then President Edvard Beneš, in his statement in 1942, stated, among other things, that "the word 'Sudeten', 'Sudetenland', 'Sudeťák' will forever be associated in the Czech lands with the Nazi brutality against us Czechs and democratic Germans carried out in the fatal crisis before and after 1938". Even shortly after the end of the Second World War, various measures were issued that prohibited the use of the designation Sudetenland and similar derived terms.[22] Hitler planned to take responsibility for the Germans in Czechoslovakia. He decided to proceed differently than in the case of Austria. He counted on the use of the Sudeten Germans, who were supposed to facilitate his seizure of Czechoslovakia.[23] If Germany wanted to implement its plans with Czechoslovakia, there had to be a closer German–Italian alliance. This would eliminate the possibility of intervention by France and Britain in favour of Czechoslovakia.[24] The instruction from Berlin was to submit

17 Kural 1993.
18 Peschka 2013.
19 Pavlíček 2002.
20 Sládek 2002.
21 Krystlík 2010.
22 Hruška 2008.
23 Beneš–Kural 2002.
24 Čelovský 1999.

proposals that Czechoslovakia could not fulfil, so there could not be an agreement between Czechoslovakia and Germany.[25] A typical example of conducting a hybrid war was the demand of the Sudeten German party, whose goal was the establishment of autonomous municipalities, districts and territorial administration. They should have been under the leadership of district governors, councils and committees and the administration was conducted in the language of the population.[26] Hitler's fascism was greatly strengthened by the withdrawal of the Czechoslovak borderland, especially by the economic and human potential and the weakening of the Czechoslovak army, which Hitler's generals feared.[27] A hybrid war can have different aspects, for example, economic, energy or logistical. Most coal mining, energy bases, and metallurgical and chemical industries were located in separate territories. In the region that remained in Czechoslovakia, agriculture prevailed over the industry. Germany wanted to turn the rest of Czechoslovakia into an agrarian "pendant" of the German industrial wheel. They cleverly determined the new Czechoslovak borders to cut through all the main transport links, which made economic consolidation and eventual defence against attack impossible. The state, territorially crippled in this way, was also crippled by a change in its internal structure. Fascist Germany directly interfered in internal affairs, regardless of the central government. In Munich, the Czech bourgeoisie sacrificed their nation and important positions of power. She left Slovakia to the will of the people's clero-fascists and believed that the economically weak Slovak bourgeoisie would need the cooperation of the Czech capitalists.[28] In the occupied sectors, so-called card files were lists of defendants, where it was written what status belonged to them. It was distinguished, e.g. arrest, resolve, confiscate, police surveillance, etc. The commandos were supposed to provide all the tasks performed by the state police authorities in Germany.[29] The national aspect was one of the most critical aspects of conducting a hybrid war. Most of the German population renounced Czechoslovak citizenship after the occupation of the border and the declaration of the protectorate of Bohemia and Moravia. On the one hand, this change increased their enthusiasm that the territory they lived in was annexed to Germany after many

[25] Kubů–Klimek 1995.
[26] Kural 2002.
[27] Hubenák 1998.
[28] Čapka 1998.
[29] Osterloh 2006.

years. On the other hand, accepting the citizenship of the German Empire also meant military duty. After the outbreak of war in the fall of 1939, most Sudeten men were conscripted into the German army. The border areas suddenly began to face a labour shortage, and, in addition to political issues, they also had to deal with economic and social problems.[30] Czech historians often view the displacement of the Czech population as an expulsion by the Germans and Hitler. Still, most of the Czech population fled "voluntarily" due to the loss of employment and livelihood. Moreover, the Czech population was not expelled by the German authorities but by the Sudeten German Freikorps and the Voluntary Protection Services, which Karl Hermann Frank[31] later stopped. Of course, the biggest concern was the part of the population who moved to the Sudetenland in the interwar period as part of the development of the Sudetenland. The number of old settlers who had always lived there mostly stayed in the Sudetenland. Those residents who owned property acquired through the land reform, Czech nationalists, members of the defence units, officials of the physical education association Sokol and former legionnaires also voluntarily left the Sudetenland. They were all associated with the oppression of the Sudeten Germans for the past twenty years, and they were all worried about how Hitler would react to them.[32] In addition to the controlled eviction, there was also the evacuation of the Czech intelligentsia, especially doctors, judges, officials, teachers, etc., who were heading to the interior or the villages located on the demarcation line.[33] Czechs lived in the city without any cultural and social activities. Only German films were shown in the cinemas, the same in the theatre or concerts. The success was the rescue of four thousand books from the Czech city and district library destined for liquidation. German members of the Hitler Youth group attacked Slovak pupils to prevent them from saving the books.[34] There were arrests of German anti-fascists, communists and social democrats, e.g. in Odary, Opava, Bielovci or Příbor. In the first years of the occupation, the resistance movement was mainly concentrated around the industrial centres of Novojičín and Ostrava. Deputations, petitions and even demonstrations were

[30] Gubič 1997.

[31] Karl Hermann Frank (1898–1946) was one of the highest ranking Nazis within the Protectorate of Bohemia and Moravia during the occupation of the Czech lands from March 1939 to May 1945.

[32] Zimmermann 1999.

[33] Myška 1965.

[34] Andrýsek 1963.

organised against the work in Czech areas, such as Příbor, Kopřivnice, Štramberk or Straník. In the autumn of 1938, illegal groups of Czech and German anti-fascists were formed in Kopřivnica, Štrambersko and Příborsko.[35] An exciting example of German propaganda was the change of the printed newspaper Neutitscheiner Zeitung to Deutsche Volkszeitung. The motif of liberation was visible on all sides. Everything was coloured red, and everything was decorated with portraits of Hitler and swastikas. Hands with broken shackles became an important symbol of liberation from twenty years of suffering alongside the Czechoslovakians. We would also find Germans who did not care about joining the Reich. The Head of the district court and the district judge in Bystrica pod Hostýnom wanted to stay in the rest of Czechoslovakia because they had Czech families and lived in a Czech environment, and did not know the German language. The relocated District Office in Hranice was even involved in staying in the republic. Czech cities and towns sent petitions against the German occupation, and demonstrations were held, due to which martial law was declared. While martial law was not declared in Novojičín in September, October and November 1938, this measure was taken due to Czech protests.[36] Germany built the occupation administration gradually, and its ultimate goal was to pursue a "final solution" to the Czech question. The Nazi occupation was supposed to culminate in the "Germanisation of space and people". It means the ethnic and, thus, for the most part, the physical liquidation of the Czech nation. Efforts for the intellectual liquidation of the country were already manifested after the university riots on 28 October 1939. The shooting of student Jan Opletal and the demonstration at his funeral gave the occupiers an excuse to close all universities, and Czech students lost the right to education. The tactic of dividing Czechoslovakia worked out for Hitler precisely as he planned. Since the Munich Agreement, nothing has prevented him from doing so. Questions of what would have happened if the Western powers had not accepted Hitler's game are difficult to solve today. Richard Chamberlain's policy of "saving peace at all costs" led to the demise of Czechoslovakia and the strengthening of the power of Nazi Germany.[37]

[35] Bartoš 2000.
[36] Trnčáková 2019.
[37] Kováč 1997.

Case study: The first and second wars in Chechnya

The first and second wars in Chechnya between 1994 and 1996, respectively from 1999 to 2009, can be considered another example of conducting war in a hybrid way. The conflicting groups in the first Chechen war were Russia on one side and Chechen separatists on the other, supported by a smaller number of Islamic fighters from various Islamic countries.[38] At the time of the war, Russia and the Russian army were headed by Boris Yeltsin. On the side of Chechnya, it was mainly the then-president Dzhokhar Dudayev. But military commander Shamil Basayev also played an important role.[39] Within the framework of the first and second wars in Chechnya, specific instruments of warfare were used in a hybrid way. One of the ways can be referring to the nation's collective historical memory. Individual arguments, whether in the form of historical facts or myths, were used as a tool to approve participation in the war conflict and the mobilisation of society. On both sides of the conflict, the nation's historical memory was activated in Chechnya. For example, part of the Chechen ideology was mainly a traumatic history, full of suffering, oppression and fights with Russia for freedom, their land, and the image of Russia as a constant danger and threat.[40] The wars in Chechnya were, among other things, labelled as an information war. The victory of Chechnya in the first war was helped by its victory in the information campaign, namely that Movladi Udugov, a Chechen politician, ideologist and propagandist, created a favourable image of Chechnya. However, in the second Chechen war, Russia learned from its mistakes and used the situation in the information environment to its advantage. Chechen ideology worked with the fact that Chechens are historically, culturally, ethnically and religiously different from Russians and Russia. For centuries, they were variously oppressed, persecuted, or even liquidated by the Russians. Chechnya always had a special status during the Soviet era. This region claimed the right to self-determination and independence after the collapse of the Soviet Union. On the other hand, the Russian side considered Chechnya an integral part of its territory and did not want to give it up.[41] During the war, Chechen separatists combined the conventional way of conducting an armed struggle with the

38 Karim 2013.
39 Souleimanov 2012.
40 Campana 2009.
41 Cornell 2001.

guerrilla way of fighting. Psychological operations were carried out to sway the local population to their side and, at the same time to carry out criminal activities and terrorist attacks not only on the Chechen Autonomous Republic but especially on the rest of the territory of the Russian Federation. Many of the Chechen separatists' activities have been labelled war crimes. They have resulted in the deaths of many innocent civilians, including children, such as in the Beslan massacre in 2004.[42] In case of the first Chechen war, it is possible to observe hostile groups, the presence of leaders, a clear conflict ideology, demonstrable organisation and communication in groups, and sufficient financing of both sides of the conflict. The conflicting groups in the second Chechen war were the same as in the first, the only difference being the higher rate of involvement of groups of Islamic fighters.[43] A typical manifestation of the leadership conflict in a hybrid way is various terrorist and sabotage actions. The causes and consequences of terrorism in the post-Soviet space as the most severe non-military threat would require a unique analysis. It is a severe problem that the Russian Federation will probably have to face in the future to an increasing extent or to work closely with other states to eliminate it.[44] Terrorist acts of armed men (bandits) related to the so-called first Chechen war (terrorist acts in Budjonnovsk, Kizľar, in 1995 and 1996) had the task of transferring violence and instability beyond the borders of Chechnya. Terrorist acts in the second Chechen war (the controversial explosions of residential buildings in Moscow in 1999, which preceded the invasion of Chechnya by federal troops, the last terrorist attack on the theatre in Dubrovka in 2002, or on the school in Beslan in 2004) were in some way connected with the so-called "Chechen trail" – by persons of "Caucasian nationality" (explosion of trains on the Moscow – St. Petersburg line in 2007 or 2009). However, it is essential that in the fight against terrorism, the Russian political leadership took an uncompromising position and tried to solve the situation violently. The political solution to the Chechen conflict was also influenced by the fact that the majority of the population of Chechnya did not identify with violent (terrorist) ways of fighting nor with Islam, to which Dudayev's regime initially began to lean.[45] Within the first Chechen war framework, it is also possible to discuss the conflict due to the dispute over raw materials. In the Chechen territory, there

[42] Renfrew 2011.
[43] Wilhelmsen 2005.
[44] Souleimanov 2006.
[45] Horemuž 2010.

are relatively large reserves of oil and plants for processing this raw material, and an oil pipeline passes through there, which was already in the Chechen territory during the Soviet era. Therefore, it is possible to assume that, among other things, Russia did not want to lose the stocks of this strategically important raw material and control over the oil pipeline. Economic enrichment was present during the first Chechen war in various criminal activities, but the funds obtained from it were used to finance the conflict.[46] During the second Chechen war, the situation in the case of economic enrichment was different. Before the outbreak of the second Chechen war, individual leaders of military groups in Chechnya also competed for power. For this competition, they used financing from Islamic states and criminal activities of various natures. This financing was used in the interwar period to gain influence and power in Chechnya. Most of them were carried out in exchange for accepting Islamist ideas. This indicates that individual Chechen leaders were not only interested in the future of Chechnya (although it still played a primary role) but also for personal benefit, which is connected with economic enrichment.[47]

Case study: The second Lebanon War

In 2006, the second war occurred in Lebanon, where Israel and Hezbollah fought against each other. This conflict was not successful on the part of Israel. The row erupted on 12 July 2006, after Hezbollah began shelling Israeli military positions and border villages in northern Israel with rocket launchers and mortars. One of the reasons the Israeli army failed to fulfil its goals was the false hope for the success of the new operational concepts and strategies associated with the revolution in military affairs. The main problem of the Israel Defense Forces, which became apparent in the war with Hezbollah, was that the Israeli army did not function as a whole.[48] In practice, it looked like the structure and equipment of the Israeli army had already been adapted to the new standards related to the revolution in military affairs. However, operationally the army still functioned based on the concepts of low-intensity conflict and limited conflict. Among other things, the fact that Hezbollah knew how to use the experience of the wars against Israel

[46] Dunlop 1998.
[47] Wilhelmsen 2005.
[48] Marcus 2015.

to counter many aspects of the new strategy, inspired by the revolution in military affairs, played an important role. Hezbollah demonstrated this approach, for example, by hiding its soldiers among the local population so that the Israeli army would not be able to identify key Hezbollah positions and neutralise them with precision-guided weapons. In addition, Hezbollah also focused on counterattacks. These consisted, for example, of guerrilla forms of attacks, asymmetric tactics, or persistent rocket attacks aimed at Israeli population zones.[49] No operational and tactical doctrine with elements of a revolution in military affairs can effectively act against an ideologically motivated and determined enemy, who uses simple but effective technologies and relies on decentralised forms of management and command. On the other hand, attributing the failure and low effectiveness of the Israeli forces in the war in Lebanon in 2006 is an oversimplified perception of reality. The Lebanon war cannot serve as empirical evidence for the new operational strategy of the Israel Defense Forces because it was not actually implemented in this conflict.[50] A typical manifestation of the hybrid war in the conflict between the Lebanese Hezbollah and Israel can be considered to be the use of, for example, the partisan way of conducting information warfare, psychological warfare, and criminal and terrorist activities. In the fight against the Israeli armed forces, the leadership of Hezbollah was able to concentrate, use and coordinate the attacks and movements of paramilitary units, criminal groups and terrorist cells, set traps and use Iranian military, financial, material and technical support. Attacks on Israeli troops were preceded by a massive information campaign aimed at Arab and Muslim communities and the world public as part of the hybrid way of conducting the battle. Photos of dead civilians, destroyed buildings, and videos showing the suffering of older men, women and children, bombed civilian homes, schools and hospitals after Israeli attacks were intended to gain sympathy for themselves and condemn Israel. Photos and videos were immediately sent to all the world's media and published on the Internet. As a result, there were reactions from many countries, which demanded an end to Israeli attacks on Lebanese territory, accused of committing war crimes, and psychological pressure was put on the leading political and military leaders of the Jewish state.

[49] Kober 2008.
[50] Adamsky 2010.

Case study: Russian Federation cyberattack on Estonia

The large-scale and sophisticated cyber operation began on 1 May 2007, and lasted 22 days. The reason for the attack was supposed to be the relocation of a Red Army monument from the centre of Tallinn. First, the opening pages of the official websites were removed and replaced with images that defamed the Prime Minister. Several hacked websites were replaced with Russian propaganda or fake apology sites, but most attacks were aimed at shutting them down. An Estonian Ministry of Defence spokesman compared these attacks to those against the United States of America on 11 September 2001.[51] Internet communication immediately collapsed, and servers were overwhelmed. Russian-speaking residents took to the streets of the capital Tallinn. The domestic population of Estonia began to feel fear and insecurity. The attack was directed not only at press institutions but also at large commercial banks. Information systems were blocked, and Estonians of Russian origin invaded the capital's centre. Subsequently, the sale of fuel and typical food commodities was interrupted. Estonia expected the Russian Federation to send military convoys to their country. However, no alarm was declared, the border guard did not announce any interventions, and Estonian airspace was not violated. It was about operations in cyberspace. The situation was also complicated because attackers constantly improved their malicious attacks to avoid filters. It means that whoever was behind it was sophisticated, fast and intelligent.[52] At the time of the attack, about 98% of the territory of Estonia was covered by the Internet, two-thirds of the population used the Internet daily, and more than 95% of banking operations were conducted electronically.[53] The only possible defence was to cut the Internet connection between Estonia and the rest of the world. The main goal of the attack was to destabilise society in Estonia. A Botnet network was used in the attack. This technique, working on the principle of the Trojan horse, makes it possible to carry out attackers' commands directed at tens of thousands of computers, control them remotely and conduct massive attacks. It was necessary to ensure the protection of the media. Without access to information, people are unable to understand individual contexts. The cyberattacks on the Estonian Government are considered the first-ever case of

[51] The Economist 2007.
[52] Raboin 2007.
[53] Centre of Excellence – Defence Against Terrorism Ankara 2008.

cyber warfare. As it was a politically motivated and highly coordinated attack on the government of a sovereign state by another state, the definition of cyber terrorism, in this case, is no longer sufficient.[54]

Case study: The war in Georgia

The war in Georgia began on 1 August 2008, when Georgian troops started shelling Tskhinvali – the capital of the separatist region South Ossetia, including residential areas – with mortars, grenade launchers and small arms. The first people died, the first material damage occurred, and as Georgia continued to concentrate and deploy its forces on the borders of South Ossetia, the evacuation of civilians to North Ossetia began.[55] On 7 August, units of the Georgian armed forces shelled Tskhinvali and other Ossetian cities again. The war finally broke out in full on 8 August 2008, the opening day of the 29th Summer Olympics in Beijing. Georgia surprisingly attacked South Ossetia after signing a ceasefire, surrounded its capital and launched a massive offensive. They also attacked the Russian barracks and killed ten Russian soldiers during the attack. Russia requested an extraordinary session of the UN Security Council. After Georgian troops continued to attack Tskhinvali and other Ossetian cities by land and air, the South Ossetian Parliament asked Russia for help. This launched a counter-offensive a few hours later by units of the 58th Army, which radically changed the balance of forces on the battlefield. After the expulsion of Georgian troops from South Ossetia, Russian military units continued to attack Georgian armed forces, military facilities, warehouses, bases and command posts and advance through Georgian territory. They stopped 55 km from Tbilisi when Russian President Dmitry Medvedev ordered them to end military operations in Georgia.[56] Both sides of the armed conflict waged an intense information war, which made it difficult to separate the facts from the deliberately spread misinformation. In addition to Moscow and Tbilisi accusing each other of killing civilians and creating a humanitarian disaster, Moscow blamed Georgia for unleashing the bloodshed and likened its actions in South Ossetia to genocide. In contrast, Georgian President Mikheil Saakashvili accused Russia of trying to subjugate

54 Tisdall 2010.
55 Kyselová 2008.
56 Ivančík 2016.

his country. Later, a report (commissioned by the European Union) was drawn up by a team led by Swiss diplomat Heidi Tagliavini directly stating that there was a massive Georgian sniper and artillery attack on the city of Tskhinvali on the night of 7–8 August 2008. This was considered the beginning of the state of war.[57] Three years later, the Prime Minister of Georgia, Bidzina Ivanishvili, also accused President Saakashvili and his supporters of being responsible for starting the war with Russia in 2008. The independent Georgian commission of inquiry reached the same conclusion, which dealt with the causes and consequences of escalating the situation in the Caucasus in 2008.[58] On the other hand, Russia was criticised by several parties and by several prominent politicians for the entry of Russian troops into the territory of Georgia. In the report above, the European Union accused Moscow of provocations and his disproportionate reaction to the attack on Russian soldiers. Three main themes dominated the information war:

- Georgia and especially its President Saakashvili were the aggressors
- Russia was forced to intervene to defend its citizens and prevent a humanitarian catastrophe
- The West has no legitimate reason to criticise Russia because Russia only did what the West did in 1999 in Serbia and Kosovo

In parallel with the information war against Georgia, cyber warfare also occurred. Several prominent Georgian websites were hacked and altered, including those of the Georgian President, the Ministry of Foreign Affairs, the National Bank, the Parliament and the Supreme Court. These cyberattacks were centrally directed and coordinated. In addition, Russian airborne troops and special purpose forces played an important role.

Case study: Cyberattacks on Iran's nuclear facilities

Cyberattacks also often affect such areas as the energy industry and the supply of network services and utilities in general (heat, water, etc.). An attacker or their group tries to gain access to crucial information or infrastructure elements (power plants, distribution systems, control centres) to control them or upload malicious code into them that will execute specific commands. This is helped by

[57] Euractiv 2009.
[58] Hlavné Správy 2012.

the fact that, at present, there is almost no complex energy or network system that would be managed without the use of information technology.[59] One example of a cyberattack on an energy facility is the attack on a uranium enrichment plant in 2010. This attack aimed to delay or completely stop the start-up of a nuclear power plant in Iran. From the point of view of cyber warfare, the most significant is the Stuxnet worm, also called the "father of cyber weapons".[60] This specific form of hybrid warfare aimed to disable and destroy several hundred uranium enrichment centrifuges by altering their rotational frequency. First, they spun above the permitted limit and then slowed down to an extended speed. This caused their collapse, financial losses and delays in commissioning the power plant itself. Given the architectural complexity of Stuxnet, it is very likely that its authors were experts with substantial financial potential. For this reason, the USA and Israel were suspected of the attack.[61] The capabilities of this worm were such that it is considered the most expensive and challenging project in the history of malware to date. Stuxnet reportedly contained security certificates stolen from legitimate software companies, used several zero-day vulnerabilities, and was able to spread both over a computer network and via a USB device. The initial infection is believed to have originated from an employee or supplier's USB drive. The attack itself had three phases. In the first phase, the infected worm targeted the MS Windows OS. In the second phase, it infiltrated the Windows-based Siemens Step7 software, which he further compromised and gained access to the PLC (programmable logic automaton) controlling the uranium enrichment centrifuges, which also became infected. In the final phase, Stuxnet used two techniques to self-destruct the centrifuges. First, there was an adjustment of the frequency of change of spins of centrifuges above and below safe operating values. Subsequently, it caused over pressurisation of the centrifuge and thus an increased load on the rotor. Stuxnet was also able to hide its presence both because it had control over communication with the PLC and also through the use of rootkit functions. In one year, Stuxnet is believed to have damaged a fifth of the centrifuges at Natanz and contributed to the slowdown of Iran's nuclear program.[62]

[59] Beránek–Dvořák 2016.
[60] Langner 2013.
[61] Zetter 2011.
[62] Ivezic 2018.

Case study: The war in Libya

The causes of conflict are identical to the objects of mutual incompatibility, that is, the publicly declared incompatible interests of the primary actors involved. We can register the split of opinion and attraction between the parties involved on several levels, namely political, ideological, religious and economic. In the political dimension, understanding the incompatibility of interests is relatively simple. The decentralisation of political power and the absence of a central, generally acceptable government represented an opportunity for several militarily significant and influential actors to try to legislate their political agenda and thus become a dominant actor in post-revolutionary Libya.[63] The revolutionary public sentiment that began to spread across the Middle East also hit Libya on 15 February 2011, when security forces in Benghazi arrested prominent lawyer Fathi Terbil, representing the families of more than 1,000 prisoners killed by security forces during the Abu Salim prison riot in 1996. After being released on the same day, Terbil set up a web camera in Benghazi's main square to film families protesting his arrest. Security forces intervened and suppressed the protests. The video quickly spread across the Internet. This demonstration occurred two days before the so-called "day of anger" planned by youth groups via Facebook and Twitter for 17 February 2011. The protests, concentrated in the eastern part of Libya, centred on Benghazi, soon spread to other cities. By 21 February 2011, almost all of Libya, fuelled by the regime's brutal response, which also brought casualties and was marked by panic, was in revolt. By the end of the month, the insurgents (although organisationally incompetent) imposed control over the eastern half of the country. But Muammar Gaddafi made it clear that he was ready to fight. In early March, forces loyal to the leader began successfully attacking cities and oil facilities in the east of the country to regain lost territory.[64] The insurgents suffered thousands of casualties but were able to seize and control several cities, including Benghazi. The rebels and volunteers could continue to the port of Cyrenaica. These troops were undisciplined, poorly trained and confused; they controlled less than one-third of the territory and even less of the natural resources. An incredible number of rivalries emerged between the self-proclaimed members of the transitional council.[65] The specific reason

[63] Gartenstein-Ross – Barr 2015.
[64] Bix 2011.
[65] Cordesman et al. 2011.

for conducting a hybrid war in Libya was, of course, also an economic interest. Libya currently has an oil wealth of more than 48 billion barrels of oil. Control of oil fields and elements of the oil infrastructure is therefore desirable for all the essential actors of the civil war. This was also reflected in the dynamics of the conflict since locations rich in oil or necessary in the context of its transportation or processing are the places of the most frequent and intense armed clashes.[66]

Case study: Russia's annexation of Crimea

Having learned from the conflict with Georgia, Russia used a wide range of military (symmetric and asymmetric), political, economic, information, propaganda, diplomatic and cyber means of warfare during the successful annexation of Crimea in the spring of 2014. By Gerasimov's concept of a hybrid war, it turned out that Moscow was not about eliminating the enemy but dominating him. The use of conventional military force has become almost useless. Controlling the minds of the Crimean population, soldiers, sailors and members of other armed forces resulted in them betraying their state and supporting the aggressor under the informational and psychological influence (pressure). By doing so, they enabled Russia to achieve the set goal.[67] The operation took place according to the prepared scenario. After the transfer of well-armed, equipped and trained personnel, critical administrative buildings, offices, airports and military bases were quickly occupied. A supply of destabilising civilian groups was ensured to provoke discontent among the local population. Special forces, intelligence services and members of private security agencies with experience in Transnistria, Chechnya and Bosnia and Herzegovina were deployed. At the same time, informational and psychological warfare continued, focusing on the elimination of places of resistance.[68] Ukraine was not at all prepared for such a situation. Its new political leadership was incapable of taking decisions adequate to the problem and issuing meaningful orders to the state's armed forces. Due to the absence of orders from the highest representatives of the country, their command was unable to manage, organise and certainly not coordinate the activities of individual armed and security forces and take effective and efficient

[66] *OPEC Share of the World Crude Oil Reserves* 2017.
[67] Bērziņš 2014.
[68] Beskid 2014.

countermeasures to prevent the annexation of the peninsula. The problem also consisted of the Ukrainian army and the security troops being underfunded, insufficiently armed, equipped and supplied for a long time. Low levels of preparedness and training, with little or no experience in combat operations, resulted in low levels of loyalty to the government.[69] In case of the annexation of Crimea and the conflict in Southeastern Ukraine, unlike the Russian–Georgian war in 2008, all methods of conducting a hybrid war, both military and non-military, have already been fully demonstrated. Russia and its supported separatists can deploy many troops and military equipment into the conflict within the military dimension. According to the U.S. Department of Defense, in November 2014, Russia had 7,000 soldiers in Ukraine (not including Crimea). More than 40,000 of them have been deployed in Ukraine, which Russia denies. On the contrary, it accuses the United States and NATO countries of helping the Ukrainian armed forces, both regular and irregular, through advisers from the armed forces, special forces and intelligence services and private military and security companies financed by them. Russia and Russian organisations, on the other hand, actively support (logistically, materially and personally) the separatists, who represent a combination of the local population, citizens of Russia and other countries of the former Soviet Union, including several volunteers from Slovakia, the Czech Republic and other European countries. Within the non-military dimension, it is necessary to point out the use of diplomatic, economic, informational, cyber and humanitarian tools. For example, Russian diplomacy strives on the ground of world organisations to defend its activities and weaken Kyiv's position, mainly by promoting the federalisation of Ukraine. Among the economic instruments, it especially concerns the manipulation of the price of imported Russian natural gas and restrictive non-tariff measures on Ukrainian food products. Sanctions in the form of a ban on importing various types of food and goods to Russia or using Russian airspace by Ukrainian airlines are also unpleasant for the Ukrainian economy. Russia also uses the so-called new propaganda, which does not aim to convince the recipient of the information, but mainly to make him uncertain about what is true and what is not and what can be believed. To maintain the support of the domestic population, Russia uses a wide range of media, especially state television, which, with its coverage of Ukraine, can significantly influence not only trained but also Ukrainian public opinion. An essential role in this area is also played by paid internet bloggers, who contribute to discussions on domestic

[69] Jones 2014.

and foreign websites expressing support for Russian activities and questioning anti-Russian views and actions. As part of the use of cyber tools, several cyberattacks on websites and systems of Ukrainian state institutions, transport networks, websites of volunteer battalions, and cyberattacks using malware or spyware can be mentioned. Within the framework of non-military instruments, we cannot forget the supply of food, medicines, material and equipment through humanitarian convoys from Russia and the fulfilment of other tasks under the guise of humanitarian activities.[70] The conflict in Ukraine has shown that some key battles may take place in cyberspace or the communications sphere rather than on land, sea or air. This conflict is an example of an operation in which the use of conventional forces was minimised. Throughout the conflict, Russia used the possibilities offered by modern technology and media. This led to the mobilisation of his supporters, the demonisation of his enemies and the enemy government's demoralisation.[71] In this context, we can talk about the so-called information war, which represents a set of activities, often mutually coordinated in terms of goal, place and time. They extract, disable, change, damage or destroy the information or its resources. This makes achieving advantages in combat or victory over a specific opponent. Thus, through informational and psychological influence, Russia managed to influence the minds of the Crimean population, military and other armed forces, who subsequently switched to Russia's side and thus helped the annexation of Crimea.[72]

Results and discussion

The paper's primary goal is to analyse selected cases of international political and social events and their subsequent application to the concept of hybrid threats. The content of the methodology is the analysis and comparison of selected forms of hybrid threats through case studies. An evaluation table of these case studies was created to analyse selected forms of hybrid threats through case studies, followed by their comparison (Table 1). The columns contain chosen case studies, and the rows represent the criteria – selected characteristics of individual

[70] Ivančík 2016.
[71] Lange-Ionathamischvili – Svetoka 2015.
[72] Unwala–Ghori 2016.

case studies. The desired characteristics are the different types and forms of means used for the conduct of hybrid warfare.

Table 1: Evaluation table of selected case studies

Criteria – Case Studies	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Military means	Yes	Yes	Yes	No	Yes	No	Yes	Yes
Political means	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Economic means	Yes	Yes	Yes	No	No	No	No	Yes
Information resources	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Cyber means	No	No	No	Yes	Yes	Yes	Yes	Yes
Propaganda means	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Diplomatic means	No	No	No	No	No	No	No	Yes
Psychological means	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Terrorist means	No	Yes	Yes	No	No	No	No	No
Media resources	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Controlling the minds of the population	No	No	Yes	Yes	No	No	Yes	Yes
Destabilising units	No	No	Yes	No	Yes	No	No	Yes
Protest potential of the population	Yes	Yes	Yes	Yes	No	No	Yes	Yes

Source: Compiled by the author

The evaluation table of selected case studies was processed through comparison. The assessment of the case studies was carried out primarily based on selected professional literature from various authors dealing with the issue of hybrid threats, including consultations with specialists and experts from institutions dealing with the issue of hybrid threats, such as the Armed Forces Academy of General Milan Rastislav Štefánik in Liptovský Mikuláš, the Academy of the Police Force in Bratislava, the General Tadeusz Kościuszko Military University of Land Forces in Wroclaw and the Occupational Safety Research Institute in Prague. The selection and formulation of evaluation criteria, or characteristics of individual case studies, were influenced by several facts. The evaluation criteria were designed to consider the structure and nature of hybrid threats in the past with practical application to the current global security environment. All the mentioned case studies have a different nature of the action of various forms of hybrid threats. Each selected case study has its specific position, principles and environment in which the participants used the mixed threat factors. Hybrid warfare is not a new type of warfare but a form that has been present since the beginning of written history. The combination of regular and irregular military

forces and other measures aimed at destabilising the adversary is not new. However, about hybrid warfare in the past, the critical dimension today is to achieve dominance in the information domain. The importance of acquiring information dominance is visible in the analysed hybrid war examples (Lebanon, Crimea). The use of propaganda-psychological warfare in combination with intelligence operations and other types of coercion is aimed at destabilising society and facilitating external intervention to gain control over it. An essential means and characteristic feature of conducting a hybrid war is the use of the population's protest potential (dominant in the conflicts of the Arab Spring, Estonia and Ukraine). When discussing defence against hybrid threats, the role of external factors (NATO, EU) is often emphasised. However, suppose the attacked society, nation, or state cannot face the first attack. In that case, the external assistance could be delayed or fail if the attacking party achieves the desired goals with quick actions. This means that the first line of defence is the preservation of the social cohesion of the attacked community (example of Chechnya). The state's resistance to hybrid combat will be maintained and built. In hybrid warfare, the aggressor seeks to quickly achieve victory in situations where he is unprepared or unable to launch a conventional military attack. Suppose the attacked state can successfully counter the first attack. In that case, the aggressor is faced with withdrawing or further escalating the crisis by conducting direct military intervention (a situation sought to be avoided by using hybrid warfare). Even if the aggressor succeeds, maintaining long-term social cohesion in the attacked state creates an opportunity to negate the aggressor's success. National identity is crucial for maintaining social cohesion.

Conclusion

States have power structures that manage available resources in peace. These structures aggregate various military headquarters, facilities and organisations created for filling, training and arming military units. The tactical level mainly uses standardised forms, but they are different from the structures built in times of war and other crises. The military system includes regular and active units, reserves and militias. Some elements even cooperate with irregular forces. Analysing new threats and preparing to act against them is essential to ensure security. However, in case of hybrid threats, this process is complex. The hybrid adversary is fast-changing, flexible and adaptable. This contribution had the

ambition to clarify its structure to understand its possible action better. However, it is necessary to realise that its structure is extensive and diverse. The activities of the individual components can be managed from one coordination centre to achieve the maximum synergistic effect, or the individual elements are independent, and each pursues its interest. When creating enemy forces of a hybrid nature for the needs of military exercises, it is, therefore, necessary to simulate the complexity of individual actors in the operational environment, determine their mutual relationships and create combat formations in which they will operate on unique battlefields. Hybrid threats are a new type of threat in the global security environment. For the effective elimination of hybrid threats, it is necessary to prepare the security forces of the state focused on these threats. Preparation should include the implementation of interdepartmental and military exercises aimed at the decision-making process, command and control systems, and tactical activities. For the practices to be as similar as possible to reality, it is necessary to focus primarily on creating the structure and combat formations of hybrid threats. Training units before deployment into an operational environment requires a different approach than in the past. Teams must be prepared to carry out a full range of operations in the face of a wide range of possible threats and, simultaneously, be ready to face third parties whose interests may differ. None of the hybrid threats is purely military. The above analysis of the content of the training aid can be an inspiration for the future training of units of the Slovak Armed Forces. Even though the concept of hybrid wars has undergone a complex development since its beginnings, numerous conferences, workshops, round tables and publications, we cannot say that it has reached clear limits. We cannot precisely characterise this type of war, what else belongs to it and what does not. It is documented by several definitions, which are empirical, and almost every conflict, whether state or non-state, can be included in this type of war. Instead, the concept is associated with the complex action of various actors, with the problematic use of military and non-military tools, which are aimed not only at the state's military power, or the North Atlantic Alliance but at the whole society. The presented structure of hybrid threats serves primarily as a training aid. The threat must be an uncooperative adversary, able to screen all the capabilities and critical tasks necessary for success. However, it must be tailored to the specific requirements of particular training. In most cases, however, in addition to creating the structure itself, it is also necessary to develop the battle's organisation and the units' assignment to tasks and activities. Various tools and means for modelling and simulating hybrid threats or their secondary

consequences also serve this purpose. Their primary goal is to facilitate the work of commanders in making decisions from the point of view of the offered options, even if the commander himself must make the final decision. It is advantageous to use this possibility either during the preparation and planning of operations or only during exercises for real situations at different levels and types of command.

Questions

1. What significance did the personality of Tomáš Garrigue Masaryk have in connection with the independence of Czechoslovakia?
2. What terrorist and sabotage actions took place during the first and second Chechen war?
3. Describe the main problem of the Israel Defense Forces during the second Lebanon war.
4. Describe the three main themes that dominated the information war in Georgia in 2008.
5. In which case studies has protest potential of the population not been used as part of the tools of hybrid warfare?

References

Adamsky, Dmitry (2010): *The Culture of Military Innovation. The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel.* Stanford: Stanford University Press.

Andrýsek, Rudolf (1963): Nový Jičín za německé okupace (10. 10. 1938 – 6. 5. 1945). In Otto, Karel et al. (eds.): *Čtení o Novém Jičíně. Soubor statí a vzpomínek k oslavám 650 let Nového Jičína.* Nový Jičín.

Bartoš, Jozef (2000): Odpor a odboj ve vládním obvodu Opava 1938–1945. In Radvanovský, Zdeněk (ed.): *Historie okupovaného pohraničí 1938–1945.* Ústí nad Labem: Univerzita J. E. Purkyně, 157–175.

Beneš, Zdeněk – Kural, Václav (2002): *Rozumět dějinám: vývoj česko-německých vztahů na našem území v letech 1848–1948.* Praha: Gallery.

Beránek, Michal – Dvořák, David (2016): Kybernetické útoky v energetice. *IT Systems,* (9). Online: https://www.systemonline.cz/it-security/kyberneticke-utoky-v-energetice.htm?mobilelayout=false

Bērziņš, Jānis (2014): *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy.* Online: https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf

Beskid, Jan (2014): Vojna novej generácie realizovaná na Kryme. In *Národná a medzinárodná bezpečnosť 2014 – zborník vedeckých a odborných prác.* Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika.

Bix, Herbert P. (2011): The North African – Middle East Uprisings from Tunisia to Libya. *The Massachusetts Review,* 52(2), 329–347.

Campana, Aurélie (2009): Collective Memory and Violence: The Use of Myths in the Chechen Separatist Ideology, 1991–1994. *Journal of Muslim Minority Affairs,* 29(1), 43–56. Online: https://doi.org/10.1080/13602000902726756

Čapka, František (1998): *Dokumenty a materiály k národním dejinám 1918–1945.* Brno: Masarykova Univerzita.

Čelovský, Boris (1999): *Mnichovská dohoda, 1938.* Praha: Tilia.

Centre of Excellence – Defence Against Terrorism Ankara (2008): *Responses to Cyber Terrorism.* Amsterdam: IOS Press. Online: http://public.eblib.com/choice/publicfullrecord.aspx?p=334204

Cordesman, Anthony H. et al. (2011): Symposium: The Arab Uprisings and U.S. Policy. *Middle East Policy,* 18(2), 1–28.

Cornell, Svante E. (2001): *Small Nations and Great Powers. A Study of Ethnopolitical Conflict in the Caucasus.* London: Routledge.

Creswell, John W. – Poth, Cheryl N. (2013): *Qualitative Inquiry and Research Design. Choosing Among Five Approaches.* Los Angeles: SAGE.

Cullen, Patrik J. – Reichborn-Kjennerud, Erik (2017): *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare.* Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

Dunlop, John B. (1998): *Russia Confronts Chechnya. Roots of a Separatist Conflict.* Cambridge: Cambridge University Press.

Euractiv (2009): Správa EÚ: Rusko je víťaz, Gruzínsko agresor. *Euractiv,* 1 October 2009. Online: http://www.euractiv.sk/obrana-a-bezpecnost/clanok/sprava-eu-rusko-je-vitazgruzinsko-agresor-013720

Gartenstein-Ross, Daveed – Barr, Nathaniel (2015): *Dignity and Dawn. Libya's Escalating Civil War.* The Hague: ICCT.

Glenn, Russell W. (2009): Thoughts on "Hybrid" Conflict. *Small Wars Journal,* 2 March 2009. Online: http://smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf?q=mag/docs-temp/188-glenn.pdf

Gubič, Otto (1997): *Jasné slovo o minulosti: česko-německé vztahy – fašismus a antifašismus na Karlovarsku 1933–1945.* Karlovy Vary: Okresní Výbor Českého Svazu Bojovníků za Svobodu.

Hendl, Jan (2005): *Kvalitativní výzkum. Základní metody a aplikace.* Praha: Portál.

Hendl, Jan (2016): *Kvalitativní výzkum. Základní metody a aplikace. 4., prepracované a rozšírené vydanie.* Praha: Portál.

Hlavné Správy (2012): Budúci premiér Gruzínska: Za vojnu s Ruskom je vinný prezident. *Hlavné Správy,* 25 October 2012. Online: http://www.hlavnespravy.sk/ivanisvili-saakasvili-a-jeho-ludia-suzodpovedni-za-patdnovu-vojnu-s-ruskom/40917

Horemuž, Martin (2010): Bezpečnostná politika Ruskej federácie z pohľadu geopolitiky. *Medzinárodné vzťahy (Journal of International Relations),* 8(2), 115–130.

Hruška, Emil (2008): *Sudetoněmecké kapitoly.* Praha: BMSS-Start.

Hubenák, Ladislav (1998): *Slovenské a československé dejiny štátu a práva v rokoch 1918–1945.* Banská Bystrica: Univerzita Mateja Bela.

Ishikawa, Akira – Tsujimoto, Atsushi (2006): *Risk and Crisis Management.* Singapore: Shumpusha Publishing.

Ivančík, Radoslav (2016): Hybridná vojna – vojna 21. storočia. *Kultura Bezpieczeństwa. Nauka–Praktyka–Refleksje,* (22), 205–239. Online: https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ceon.element-2157653d-6c10-39e2-9e75-5c3fa98fe5c3/c/pdf-01.3001.0012.2654.pdf

Ivezic, Marin (2018): *Stuxnet: The Father of Cyber-Kinetic Weapons: While Stuxnet Is Gone, the World Now Knows What Can Be Accomplished Through Cyber-Kinetic Attacks.* Online: https://www.csoonline.com/article/3250248/stuxnet-the-fatherof-cyber-kinetic-weapons.html

Jones, Sam (2014): Ukraine: Russia's New Art of War. *Financial Times,* 28 August 2014. Online: https://www.ft.com/content/ea5e82fa-2e0c-11e4-b760-00144feabdc0

Jurčák, V. – Turac, Jan (2018.): *Hybridné vojny – výzva pre NATO. Bezpečnostné fórum 2018.* Banská Bystrica: Interpolis.

Karim, Moch Faisal (2013): How Ethnic Civil War Transforms into Religious Civil War: Evidence from Chechnya. *CEU Political Science Journal,* 8(1), 54–78.

Kober, Avi (2008): The Israel Defense Forces in the Second Lebanon War: Why the Poor Performance? *Journal of Strategic Studies,* 31(1), 3–40. Online: https://doi.org/10.1080/01402390701785211

Kováč, Dušan (1997): *Dejiny Československa.* Bratislava: Academic Electronic Press.

Krystlík, Tomáš (2010): *Zamlčené dějiny 2.* Praha: Alfa Nakladatelství.

Kubů, Eduard – Klimek, Antonín (1995): *Československá zahraniční politika 1918–1938: kapitoly z dějin mezinárodních vztahů.* Praha: ISE.

Kural, Václav (1993): *Konflikt místo společenství? Češi a Němci v Československém státě (1918–1938).* Praha: Nakladatelství.

Kural, Václav (2002): *Češi, Němci a mnichovská křižovatka.* Praha: Karolinum.

Kyselová, Marianna (2008): *Ruská invaze do Gruzie.* Online: http://www.epolis.cz/clanek/ruska-invaze-do-gruzie.html

Lange-Ionathamischvili, Elina – Svetoka, Sanda (2015): Strategic Communications and Social Media in the Russia Ukraine Conflict. In Geers, Kenneth (ed.): *Cyber War in Perspective. Russian Aggression against Ukraine.* Tallinn: NATO CCD COE Publications. Online: https://www.caleaeuropeana.ro/wp-content/uploads/2015/12/cyberwarinperspective_lange_svetoka_121.pdf

Langner, Ralph (2013): Stuxnet's Secret Twin. *Foreign Policy,* 19 November 2013. Online: http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack

Marcus, Raphael D. (2015): The Israeli Revolution in Military Affairs and the Road to the 2006 Lebanon War. In Collins, Jeffrey – Futter, Andrew (eds.): *Reassessing the Revolution in Military Affairs. Transformation, Evolution and Lessons Learnt.* London: Palgrave Macmillan, 92–111. Online: https://doi.org/10.1057/9781137513762_6

Marinov, Ivo (2011): *NATO Crisis Management.* National Defence Academy, Operational Art Department. Online: https://docplayer.net/24781706-Nato-crisis-management.html

Myška, Milan (1965): Novojičínsko od Mnichova k 15. březnu. In Král, Jaroslav et al. (eds.): *Mnichov není jen historie. Sborník materiálů z ideologické konference OV KSČ v Novém Jičíně k 25. výročí Mnichova dne 9. října 1963.* Nový Jičín.

NATO (2022): *Crisis Management.* Online: http://www.nato.int/cps/en/natolive/topics_49192.htm

OPEC Share of the World Crude Oil Reserves (2017). Online: https://www.opec.org/opec_web/en/data_graphs/330.htm?fbclid=IwAR2zQsMTteWDrJknXVsIPpJ_bjBijYF5OMW_ZA_jwypLYsl1yf-JbWMSTiM

Osterloh, Jörg (2006): *Nationalsozialistische Judenverfolgung im Reichsgau Sudetenland 1938–1945.* Mnichov: Collegium Carolinum.

Pavlíček, Václav (2002): *O české státnosti: úvahy a polemiky.* Praha: Karolinum.

Peschka Otto (2013): *Jak to bylo doopravdy mezi Čechy a Němci: o Češích, Němcích a jiných tématech na pozadí memoárů člena smíšené rodiny, který pochází ze Sudet.* Ústí nad Labem: Paprsky.

Raboin, Bradley (2011): Corresponding Evolution: International Law and the Emergence of Cyber Warfare. *Journal of the National Association of Administrative Law Judiciary,* 31(2), 602–668.

Renfrew, Barry (2011): *Chechnya.* Online: http://www.crimesofwar.org/a-z-guide/chechnya/

Rohlfing, Ingo (2010): *Methodologies of Case Studies.* ECPR Summer School on Methods and Techniques. Online: https://www.uni-bamberg.de/fileadmin/bagsb/externe_Seminare/rohlfing-case-study-research-2014-ecpr-ssmt.pdf

Rubin, Allen – Babbie, Earl (2001): *Researchmethods for Social Work.* Belmont: Brooks/Cole.

Sanseverino-Godfrin, Valérie (2016): The Problems of the Late Implementation of the Legal Prevention Measures for Flood Risk. *Flood Risk 2016 – 3rd European Conference on Flood Risk Management,* 7, 1–11. Online: https://doi.org/10.1051/e3sconf/20160713010

Šimák, Ladislav (2016): *Krízový manažment vo verejnej správe. Druhé prepracované vydanie.* Žilina: EDIS.

Sládek, Milan (2002): *Němci v Čechách.* Praha: Pragma.

Souleimanov, Emil (2006): *Terorismus ve světle geneze ideologie a technologie asymetrických konflikt.* In Souleimanov, Emil (ed.): *Terorismus. Válka proti státu.* Praha: Eurolex Bohemia, 13–63.

Souleimanov, Emil (2012): *Konflikt v Čečensku: Minulost, současnost, perspektivy.* Praha: SLON.

The Economist (2007): A Cyber-riot. *The Economist,* 10 May 2007. Online: http://www.economist.com/node/9163598

Tisdall, Simon (2010): Cyber-warfare 'Is Growing Threat'. *The Guardian,* 3 February 2010. Online: https://www.theguardian.com/technology/2010/feb/03/cyber-warfare-growing-threat

Trnčáková, Adriana (2019): *Novojičínsko v době zářijové krize roku 1938.* Brno: Masarykova univerzita, bakalářská diplomová práce.

Unwala, Azhar – Ghori, Shaheen (2016): Brandishing the Cybered Bear: Information War and the Russia–Ukraine Conflict. *Military Cyber Affairs,* 1(1), 1–11. Online: https://doi.org/10.5038/2378-0789.1.1.1001

Wilhelmsen, Julie (2005): Between a Rock and a Hard Place: The Islamisation of the Chechen Separatist Movement. *Europe–Asia Studies,* 57(1), 35–59. Online: https://doi.org/10.1080/0966813052000314101

Yin, Robert K. (2009): *Case Study Research. Design and Methods.* London: SAGE.

Zetter, Kim (2011): How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. *Wired,* 11 July 2011. Online: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/

Zimmermann, Volker (1999): *Die Sudetendeutschen im NS-Staat: Politik und Stimmung der Bevölkerung im Reichsgau Sudetenland (1938–1945).* Essen: Klartext.