 DOI: 10.3849/2336-2995.30.2021.04.093-108

Peer-reviewed

The New Wars: Terrorism and "Asymmetric" Warfare

Nové války: terorismus a „asymetrická" válka

Alexander Treiblmaier

Abstract: The term "new wars" is often used to describe how terrorist groups achieve objectives in addition to the "classic" means of intervention by states. Terrorist organizations use asymmetric methods of warfare to target the weaknesses of Western states. Consequently, conventional wars have also changed into hybrid wars. The legal status of terrorist organizations is a major problem for the rule of law. In responding to terrorist attacks, the distinction between crime and terrorism is difficult. The "war on terror" is governed by different rules and principles and is extremely difficult to wage. Conflicts last a long time and victory against terrorism is rarely possible due to the networked structure of terrorist organizations and the way they intermingle with the population. In addition to an alliance-wide approach, there is a national solution to answer these new threats in form of the comprehensive national defense in Austria.

Abstrakt: Termín „nové války" se často používá k popsání toho, jakým způsobem teroristické skupiny dosahují svých cílů vedle „klasických" prostředků v podobě intervence ze strany států. Teroristické organizace používají asymetrické metody války zaměřené na slabiny západních států. V důsledku toho se i konvenční války změnily v hybridní války. Právní postavení teroristických organizací je hlavním problémem právního státu. Při reakci na teroristické útoky je obtížné rozlišovat mezi zločinem a terorismem. „Válka proti teroru" se řídí odlišnými pravidly a principy a je nesmírně obtížné ji vést. Konflikty trvají dlouho a vítězství nad terorismem je zřídka možné kvůli síťové struktuře teroristických organizací a způsobu, jakým se prolínají s obyvatelstvem. Kromě celoaliančního přístupu existuje v Rakousku národní řešení, jak na tyto nové hrozby reagovat, a to v podobě komplexní národní obrany.

Key words: Terrorism; Hybrid; Conflict; Warfare; Trends.

Klíčová slova: terorismus; hybridní; konflikt; válka; trendy.

INTRODUCTION

Warfare has changed dramatically in recent decades. The war of position (World War I) became a war of maneuver (World War II) and then morphed into a more hybrid and irregular form of warfare. This development was due to changing actors, technological progress, and to demographic changes in Europe and the world. The aim of this article is to explain the changes in warfare and to present and compare nowadays frequently used terms like "new wars", "terrorism" or "asymmetric warfare" in a current context.

The derivations presented in the article are obtained through a hermeneutic analysis of current texts and studies. After defining the terms "old war" and "new war", the methods of asymmetric warfare and terrorism are discussed. This analysis focuses on Islamist terrorism, identified by the European Union as the "main threat." In addition, technological means and their potential hazards are examined. Subsequently, the "instrumentalization" of terrorism by states in the context of hybrid power projection is presented in more detail. Finally, concepts to counter these challenges are presented using the example of the EU, NATO and, as a national resilience model, the comprehensive national defense of Austria.

This paper concludes by bringing together the results of the analysis and evaluating the form in which terrorism in its current form can challenge the rule of law. The aim of this article is to provide a general overview of this subject area and to present relevant aspects.

1 TERRORISM IN THE 21ST CENTURY „THE NEW WAR"

War (old war / great war)

The term war is used in today's common parlance for many "conditions." Nearly every crisis-facing, conflict-ridden development in various dimensions and constellations can be referred to as "war."

A possible definition of the concept of war is provided by Carl von Clausewitz in his work *On War*: "*War, then, is an act of violence to force the enemy to do our will.*"[1] For Clausewitz, war as an act of violence "*… was the continuation of politics by military means.*"[2] Clausewitz goes on to say, that in the event of a war, all the means available to the state must be used to wage this "absolute war."[3] Clausewitz also calls this form of war a "Great War." This includes, above all, a symmetrical battle between the army of one state and the (equivalent) army of another state.[4]

1 Clausewitz, Howard (2007, p. 31.).

2 Ib. p. ix.

3 Cp. Clausewitz, Hahlweg (1990 Nachdr. 1991, p. 79ff.).

4 Cp. Jäger, Beckmann (2011, p. 211.).

One definition was made by Professor Mary Kaldor during a lecture. She mentioned: "'*Old War' refers to an idealized version of war that characterised [sic!] Europe between the late 18th and the middle of the 20th century. 'Old War' is war between states fought by armed forces in uniform, where the decisive encounter was battle."*[5]

Another possible legal definition is found in international law regarding warfare. Here, due to developments after the Second World War, the term "international armed conflicts" is used. According to Article 2 of the Geneva Convention of 1949, these include all cases of declared war or any other armed conflict arising between two or more states, even if the state of war is not recognized by one of those parties.[6]

For this paper, the term war is defined as the use of military, conventional force by a sovereign state. This use of military force can take place in a physical domain (land, air, sea, space) as well as in a non-physical domain (cyber and information space) and serves to achieve a political purpose.

War (new war / small war)

Clausewitz argued, that "small wars" could also be fought in the context of a "great war". For him, this meant, above all, deploying a small number of specialized soldiers against supply facilities or carrying out ambushes.[7]

Almost 170 years after Clausewitz, the political scientist Herfried Münkler extended the definition of war in his work *Die neuen Kriege*. In this work he observes that modern wars no longer only involve state actors, and that the objective-purpose context of war is often intangible. He moves away from Clausewitz's definition and expands the concept of war. Through an analysis of current developments, he concludes that Clausewitz's classic concept of war needs to be comprehensively rethought. New forms of warfare such as cyber warfare, economic wars and even terrorism must be included.[8] He refers to indirect or hybrid warfare in which hybrid power projection methods are carried out by state and non-state actors in all domains and with all instruments of power.[9] This is consistent in the broadest sense with Clausewitz's definition of "absolute war."[10] However, it extends it to include opponents of conflicts who are non-state actors.

The background for this development, according to Münkler, is the condition of "democratic" peace in Europe and the Western world. The result is that western democracies are no longer prepared to wage symmetric/conventional wars due to the expected number of casualties, the economic costs, and the accompanying phenomena. These "great" wars (symmetrical, conventional wars) are epitomized by the First and Second

5 Kaldor (2005, p. 2.).

6 Cp. Genfer Abkommen über die Behandlung der Kriegsgefangenen vom 12. August 1949 StF: BGBl. Nr. 155/1953 Artikel 2.

7 Cp. Jäger, Beckmann (2011, p. 211.).

8 Cp. Münkler (November 2018, p. 59ff.).

9 Ed. The instruments of power (PMESII) are political, military, economic, social, infrastructural, informational.

10 Ed. For Clausewitz, every great war was also an absolute war since it could only be fought if all the available resources of a state were devoted to it.

World Wars which caused millions of deaths and extensive destruction within a few years. Such a high level of sacrifice is no longer acceptable in today's western societies due to changes in demographics[11] and mentality.

This has led to the already described "further development" of warfare from conventional "big" wars of symmetrical states to conflicts described by Clausewitz in the broad sense as "small wars" [12] and by Münkler as "new wars."

These findings confirm the thesis that "old-style wars", as described here, can no longer be fought between states in our time.

Proxy war

Proxy wars are wars "*between the great powers fought in other countries, using third-party actors without those powers' direct involvement*".[13] The term proxy war has been used colloquially, especially since the Cold War, as a direct confrontation between global superpowers.[14] This development and the definition presented underlines Münkler's statement, that "old-style wars" as already described are no longer fought. Examples for this type of war are the Spanish civil war (1936-1939), the Vietnam war (1964-1975) and anymore. Nowadays the involved and instrumentalized third-party actors are also terrorist organizations and with their worldwide engagement capabilities this sort of conflict in the context of a hybrid conflict reaches a whole new dimension.

Terrorism

According to the U.S. Department of Justice and the Federal Bureau of Investigation, Terrorism is "*The unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives*."[15]

2 ASYMMETRIC WARFARE AND TERRORISM

Another important and often forgotten war theorist[16] is August Rühle von Lilienstern. In 1818 he wrote about avoiding the "great decision-making battle" and using the

11 Ed. This describes the population development by age group and shows, for example, a growing imbalance in Austria in the form of a decline in the number of people of working age and an increase in the number of older people.

12 Ed. For Clausewitz, the "small war" was not independent. It was part of a "Great War." It was characterized by the fact that only a small number of combatants were involved, mainly with light weapons and using irregular warfare methods. Cp. Teibus (2013, p. 2f.).

13 Bandeira (2019, p. 315).

14 Cp. Bandeira (2019, p. 21).

15 U.S. Department of Justice (2002. P. 6).

16 Ed. August Rühle of Liechtenstein (born Johann Jakob Otto Rühle of Liechtenstein) was a Prussian lieutenant general and completed numerous training courses and assignments together with Clausewitz. He was also a well-known geographer/cartographer and writer.

enemy's weak moments, e.g., the onset of winter or the arrival of supplies, as the goal of asymmetric warfare.[17]

This is still the case with "new wars." An essential characteristic of current conflicts is the strong asymmetry between conflicting parties. This imbalance is not a "new" development in the context of wars. Rather, conflict has always been aimed at either exploiting the strengths of one side or deliberately exploiting the weakness of the other.

Another possibility to define the term "asymmetric warfare" is according to Pfanner: "*Asymmetries in warfare include asymmetry of power, means, methods, organization, values, and time".*[18] An extension of this is mentioned by Schmitt as fallows: *"Asymmetry can be participatory, technological, normative, doctrinal, or moral".*[19] Fallowing these statements, it can be deducted, that wars always have contained at least some form of asymmetry. This definition confirms Lilienstein's statement that it is about avoiding decisive battles as well as depicting the possible dimensions of asymmetry in a military conflict. Following this definition, Dr. J. A. Khan argued, that asymmetric warfare can include three different types of warfare. These are strategic asymmetric wars, tactical asymmetric wars, and wars by proxy.[20]

Münkler describes these conditions as "asymmetries of strength" (using organizational and technical superiority, e.g., drone warfare) and "asymmetries of weakness" (trying to evade open combat and to carry the struggle into cities and the civilian population).[21]

This asymmetry of conflict is mostly expressed in the areas of manpower, equipment, and the level of technological expertise of the armed forces or combatants. A terrorist group is thus clearly inferior to a conventional armed force in terms of troop strength, armament, mobility, and protection. This forces such groups to avoid conventional confrontation[22] and to use "irregular" procedures. Therefore, from a historical point of view, asymmetry in warfare is the rule and symmetry is the exception.[23] In the context of the operation against the Islamic State, however, a change between a symmetrical and an asymmetrical operation occurred.

Organizations like the Islamic State use tactics such as ambushing, carrying out raids, deception, and subversion. This type of warfare (often referred to as irregular warfare) includes attacks by suicide bombers and other atrocities[24] which have been carried out by terrorists in recent decades.

---

17 Cp. Jäger, Beckmann (2011, p. 212f.).

18 Pfanner (2005, p. 151).

19 Schmitt (2007, p. 16).

20 Cp. Khan (2005, p. 100ff).

21 Cp. Richter (p. 176f.).

22 Ed. An example of conventional confrontation is an open battle in the form of tanks against tanks or infantry against infantry.

23 Cp. Münkler (2004, p. 89).

24 Ed. These include stabbing attacks, e.g., in Paris in April 2021 against a policewoman, and car attacks, e.g., in Nice 2016.

Actual threat scenario

In his diploma thesis, published in the magazine *Armis et Litteris*, Rentenberger maintains, that there are many different forms of terrorism. He also believes that organized crime and terrorism have become increasingly intertwined. In some parts of the world, terrorists have contributed to the massive destabilization of states and play an important role as a political force. He also mentions the effective use of modern media and technologies by terrorists. In his thesis he identifies Islamic terrorism as the main threat to the European Union.[25]

This has been confirmed by the EU's annual *EU Terrorism Situation and Trend Report by Europol*. In 2020, the report identified the following forms of terrorism as "main threats":

- Islamic terrorism
- Radicalisation of prisoners
- Right-wing terrorism
- Left-wing and anarchist terrorism
- Ethno-national and separatist terrorism
- Single issue terrorism[26]

Encouragingly, the report highlighted the decline in the total number of terrorist attacks carried out, failed, or thwarted in 2019. Furthermore, an increasing number of jihadist attacks were prevented. The report, however, identified the following as extant main threats: the situation in conflict areas outside Europe; the connection of hundreds of European citizens to ISIS; and the resurgence of Al-Qaeda.[27]

The analysis concluded that Islamist terrorism continues to pose the greatest threat to the EU. Using modern media and technology, it can expand its reach, finance itself, attract new members, and – through progressive radicalization – encourage potential individual perpetrators to implement their intentions.

Technological resources of terrorist organizations

The author believes that the changes in the operational management of terrorist organizations in recent years can also be attributed to, among others, technological developments. For this reason, some of these developments are discussed in the following section.

The effective use of mass media by a terrorist organization was demonstrated on October 7, 2001, in the video message of Osama Bin Laden, which was broadcast on Al Jazeera. The quality of this video and, above all, the timing of its dispatch and publication, ushered in a new era in the use of technology as a means of promoting terrorism.[28, 29]

---

25 Cp. Rentenberger (p. 54.).

26 Cp. Europäische Union Agency for Law Enforcement (2020, p. 5f.).

27 Cp. Ib.

28 Cp. Hoffman (2006, p. 305.).

29 Ed. The videos were recorded and sent in such a way that they could be broadcast on October 7, 2001. That day also saw the first American airstrikes in Afghanistan and thus the beginning of Operation Enduring Freedom as part of the "war on terror."

Communication within the terrorist group(s) has also changed. Whereas in the past secret radio stations, underground newspapers, posters, and publications were used, broadband networking now makes high-quality and, above all, faster communication available to almost the entire world.[30]

Internet

In the 21st century, the Internet has become the most important and widely used medium of communication and propaganda on the Islamist and jihadist scene, providing fast, secure, cross-border communication and interaction. It serves terrorist organizations, networks, groups and even individuals as a virtual platform for planning, executing and disseminating attacks.[31]

Above all, the quality of the websites, blogs and forums used by jihadist actors has greatly improved in recent years. The high availability of social networks and intelligence services has facilitated the intensive use of rallies, and demonstrations by terrorist groups and their sympathizers. According to a BBC article, the Islamic State (IS) coordinated, carried out and disseminated over 10,000 operations in Iraq and over 1,000 targeted killings between 2012 and 2013.[32]

The dissemination of brutality and the results of individual actions is a form of psychological warfare aimed at creating fear and horror among the population, opposing forces and their families. This media exploitation was illustrated by more than 40,000 ISIS tweets a day when Iraqi soldiers trained by the US-troops and equipped with state-of-the-art equipment fled out of Mosul in the summer of 2014 from ISIS.[33]

Training

The training of groups as well as individual perpetrators of terrorism is essential for the successful achievement of terrorist objectives. This training often takes place in "terror camps" which in recent years have been increasingly targeted by international forces.[27]Another form of training is the dissemination of content on the Internet. The following are examples of jihadist Internet magazines: *Inspire (Al Qaida), Dabiq (IS), Rumiyah (IS)*.[34]

These magazines give specific instructions on how to produce bombs and the execution of attacks. New information is constantly published on the website *Terror Trends*

30 Cp. ib. p. 308.

31 Cp. Görtz, Stefan (2016): Cyber-Jihad. Das Internet als vitales Instrument für Islamismus und islamistischen Terrorismus. https://www.kriminalpolizei.de/ausgaben/2016/dezember/detailansicht-dezember/artikel/cyber-jihad-das-internet-als-vitales-instrument-fuer-islamismus-und-slamistischen-terrorismus.html (18.06.2021).

32 Cp. BBC (2014): News. World/Middle-East. www.bbc.com/news/world-middle-east-27912569 (30.04.2021).

33 Cp. ib.

34 Cp. Görtz, Stefan (2016): Cyber-Jihad. Das Internet als vitales Instrument für Islamismus und islamistischen Terrorismus. https://www.kriminalpolizei.de/ausgaben/2016/dezember/detailansicht-dezember/artikel/cyber-jihad-das-internet-als-vitales-instrument-fuer-islamismus-und-slamistischen-terrorismus.html (18.06.2021).

Bulletin, which is disseminated through the channels of the various terrorist organizations. The following quote is taken from the Al Qaeda magazine *Inspire* on May 16, 2016: *"The magazine contains new detailed instructions on new types of Improvised Explosive Devices (IEDs) inside of books, attached to automobiles with magnets and attached to doors in homes."*[35]

AQAP[36] also used these magazines to directly incite violence calling on *"Knife Revolutionaries to conduct knife attacks specifically on Americans, such as been happening in Israel over the past year or so."*[37]

Similarly, the online magazine *Rumiyah*, in November 2012, gave clear guidelines for the planning and execution of attacks using vehicles. The contents ranged from the choice of ideal vehicles for attacks, possible targets to the planning and preparation of the attacks themselves.[38] The terrorist attack in Nice on July 14, 2016, in which the assassin Mohamed Lahouaiej Bouhlel drove a truck into a crowd, killing 86 people and injuring more than 400, some of them seriously, shows the topicality and intensity of this threat.

Unmanned aerial vehicles (UAVs) / drones

Drones are used in different ways by both terrorist groups as well as individual perpetrators of atrocities. Their field of application ranges from being used as documentation platforms for photo and film recordings as well as carriers for all kinds of weapons. The access to drones is simple and straightforward. Airworthy systems, including the necessary control elements, are freely available on the market. Construction manuals adapting them as weapons carriers, as well as explanations for possible operational tactics, are distributed on the platforms listed above.

Drones were first used for terrorist purposes in 1994 by the Aum-sect, which gained infamy in 1995 with a poison gas attack on the Tokyo subway. The drones were used to try to spread sarin gas.[39, 40] Further attacks followed using a combination of drones and weapons. In 2001 the G8 summit was bombed by a drone, in 2002 there was an

35 Holton, Christopher W. (2016): Al Qaeda Publishes Another "Inspire" Magazine; Here's What It Says. Terror Trends Bulletin. https://terrortrendsbulletin.com/2016/05/16/al-qaeda-publishes-another-inspire-magazine-heres-what-it-says/ (18.06.2021).

36 Ed. Al-Qaeda in the Arabian Peninsula (AQAP).

37 Ib.

38 Cp. Holton, Christopher W. (2016): Al Qaeda Publishes Another "Inspire" Magazine; Here's What It Says. Terror Trends Bulletin. https://terrortrendsbulletin.com/2016/05/16/al-qaeda-publishes-another-inspire-magazine-heres-what-it-says/ (18.06.2021).

39 Ed. Sarin is a chemical warfare agent that primarily attacks the nervous system. Due to the chemical properties (highly volatile), the distribution by drone was, fortunately, not successful.

40 Cp. Bunker (2015, p. 7ff.).

attempted anthrax[41] drone attack against the British House of Commons, and there have been many more such attacks, both successfully carried out and thwarted, to this day.[42] In 2014, ISIS successfully began using drones for reconnaissance and subsequently for the documentation of attacks. The high-quality videos of successful attacks were used directly in IS propaganda videos.[43]

A study published by the U.S. Army War College in August 2015 identified the following possible uses for drones:

- for enlightenment and monitoring
- for "messaging" in the form of carrying out protests (such as the violation of airspace by a Hezbollah drone in April 2005), propaganda (such as the dissemination of videos of successful attacks), and warning signs for allies
- as carrier systems for weapons and explosives
- as carrier systems for weapons of mass destruction (chemical, biological, nuclear)
- as transport systems for contraband
- as platforms for electronic warfare (for locating, transferring or disrupting mobile phone data).[44]

His study depicts three threat scenarios:

Threat Scenario	Time Period	Description	Significance
1: Single UAV—Human Controlled	Present Day	Tactical action utilized to create a terrorism incident. Scenario variants: Drone-up Shooting, IED Crowd Targeting, and Aircraft Takedown	Tactical (+Terrorism Disruptive Potentials)
2: Group of UAVs—Human Controlled or Semi-autonomous	Present Day Near Futures (Some Years)	Force-on-force engagement in insurgency environment. Scenario variants: Squad-sized Virtual Martyrs Unit and Semi-autonomous Drone Squadron	Operational
3: Swarm of UAVs—Autonomous	Futures (A Few Decades)	Robotic targeting of human personnel, materiel, vehicles, aircraft, and vessels in conflict and war. Scenario variants: Swarms and Micro-Swarms	Strategic

Figure 1: Terrorist and Insurgent UAV Use Threat Scenarios[45]

41 Ed. Anthrax toxin is produced by the bacterium Bacillus anthracis and was used in biological warfare in the Middle Ages. More recently, this toxin has become well known due to the anthrax accident in the former Soviet Union in 1979, its suspected production and storage in Iraq in the 1990s and the anthrax attacks in the United States on various government agencies in 2001.

42 Cp. ib.

43 Cp. Hall, John (2014): ISIS propaganda, Call of Duty-style: Latest footage shows drone's view of battle-ravaged streets of Kobane before swooping in to show gun battles on the ground. Mail Online News. https://www.dailymail.co.uk/news/article-2871389/ISIS-propaganda-Call-Duty-style-Latest-footage-shows-drone-s-view-battle-ravaged-streets-Kobane-swooping-gun-battles-ground.html (18.06.2021).

44 Cp. Bunker (2015, p. 16ff.).

45 Quelle: Bunker (2015, p. 25.).

The first threat –the single UAV threat scenario – is the most common at the time of writing this paper. This includes the already explained methods of filming or attacking using explosives or other weapons as well as attacks against other aircraft – which is a constant threat.[46]

Like scenario one, scenario two has become a reality. The GPS control[47] of drones without direct contact with a remote-control station and the automatic response of threats by obstacles is already standard. The collaboration of several independently controlled drones is already being observed on current battlefields.

The swarm technology depicted in scenario three also became a reality in 2021. In 2018, a swarm of thirteen drones attacked two Russian military bases in Syria.[48] The first manufacturers are already supplying mass produced systems. However, programming and controlling of at least the "lead drone" continues to be done by humans and not by artificial intelligence.

Technological advancement and the availability of powerful drones have provided a wide range of applications for terrorist groups and individual perpetrators of atrocities. The ability to detect, identify and defend drones by kinetic means or by using the electromagnetic spectrum is therefore essential.[49]

3 HYBRID POWER PROJECTION AND THE USE OF TERRORISM

Clausewitz's definition that war *"… was the continuation of politics by military means"*[50] is also relevant to the concept of hybrid warfare. Clausewitz was not simply referring to a sequential process of political measures and military action. Already in his time, the deterrent effect of armed force was an important means of "reinforcing" diplomatic measures.

There is currently no uniform definition of the term "hybrid warfare". In recent years, the terms asymmetric warfare, irregular warfare, unconventional warfare, conventional warfare, economic warfare, and many more have been used. Ever since the annexation of Crimea by Russia in 2014 and the many articles by the Chief of the General Staff of the Armed Forces of the Russian Federation known as the "Gerasimov doctrine", the term hybrid warfare has been on everyone's lips. However, in the following years, the term "hybrid power projection" has appeared in numerous publications.

46 Cp. Bunker (2015, p. 25.).

47 Global Positionen System (GPS).

48 Cp. Reid, David (2018): A swarm of armed drones attacked a Russian military base in Syria. Hg. v. CNBC. https://www.cnbc.com/2018/01/11/swarm-of-armed-diy-drones-attacks-russian-military-base-in-syria.html (14.06.2021).

49 Ed. For this reason, there is an element of electronic warfare for drone defense in the Austrian armed forces.

50 Clausewitz, Howard (2007, p. ix.).

A quite simple definition was published in 2008 as part of an article by Roland Dannreuther and Luke March. In this article hybrid warfare is defined as a combination of conventional forces, irregular tactics, as well as terrorist attacks and criminal influences:

"*Hybrid Wars incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder*."[51]

The Austrian sub-strategy defense policy[52] defines the concept of hybrid threats as the flexible use of conventional weapons, irregular warfare, information warfare, terrorism, and crime.[53] This agrees with Dannreuther's and March's definition but expands it to include the dimension of information warfare.

Brin Najžer expands this definition in "The Hybrid Age" (2020) by including political objectives (which is similar to Clausewitz's definition of war):

Hybrid warfare is a distinct form of low-level conflict spanning the spectrum of capabilities. It is a deliberately opaque merger of conventional and unconventional warfare and conducted under a single central authority and direction of a state and/or state-like actor. The aim of hybrid warfare is to achieve political objectives that would not be achievable, or would incur too high a cost, through the use of either form individually. The blend of conventional and unconventional enables the actor to exploit an opponent's strategic or doctrinal weakness while maintaining deniability and strategic surprise.[54]

The reference to hybrid wars as "low-level" conflicts supports the conclusion, that "old" wars are no longer tenable for European western states. However, the low level of intensity regarding the cost of personnel and conventional resources has been replaced by higher costs in terms of time, technology and other instruments of power.

In summary, hybrid warfare is a conflict between states and/or groups like states, which remains below the threshold of war and uses tactics and methods that take advantage of the respective weaknesses of the enemy. The entire hybrid "war" thus takes place in a "gray zone" as shown in figure 2.

51 Dannreuther, March (2008, p. 101.).

52 Ed. The sub-strategy Defense Policy is based on the Austrian Security Strategy and concretizes it in the areas of defense policy with a time horizon of ten years.

53 Cp. Republik Österreich, Bundesministerium für Landesverteidigung und Sport (2014, p. 28.).

54 Najžer (2020, p. 29.).

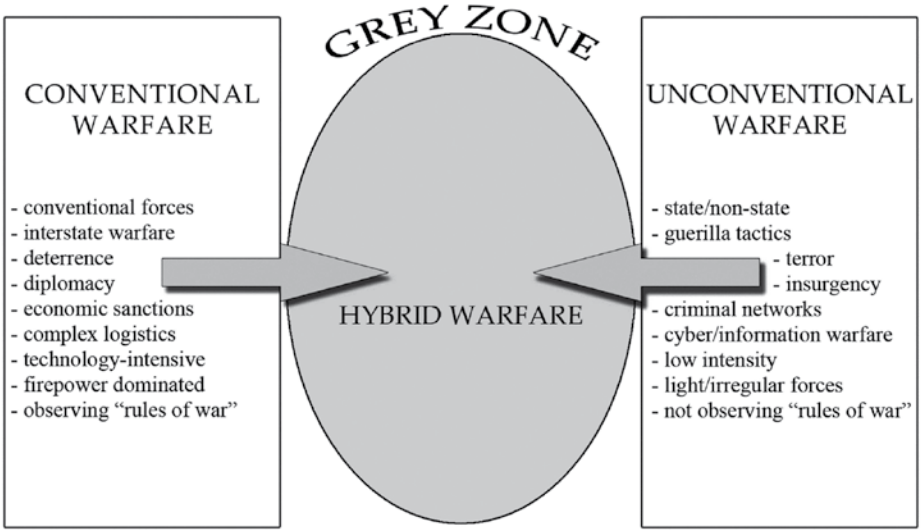

Figure 2: Hybrid warfare is a blend of conventional and unconventional warfare[55]

Terror, crime, and information warfare (fake news.) therefore play a role in hybrid warfare and are used depending on the situation and objective.

A legal reference relevant to the concept of hybrid warfare appears in an international treaty. If "violence" occurs in the context of hybrid warfare, it contradicts the prohibition of violence in Art. 2 para. 4 UN Charter: *"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."*[56] The possible manifestation of "violence" as military force is undisputed, but whether force can also be exercised in cyberspace is currently under discussion.[57, 58] The Tallinn Manual 2.0, Rule 70, states that "*a cyber operation, or threatened action, if carried out, would be an unlawful use of force*".[59] Thus, attacks on, for example, a pipeline such as that committed in May 2021 on the Colonial Pipeline[60] in the United States of America are also considered "violent" according to Art. 2 para. 4 UN Charter.

55 Source: Ib. P. 31.

56 United Nations Charter https://www.un.org/en/about-us/un-charter/full-text at 19.06.2021.

57 Ed. In the the Tallinn Manual 2.0, an attempt was made to approach the use of violence in cyberspace.

58 Cp. Hector (2016, p. 520ff.).

59 Schmitt, Vihul (2017, p. 338.).

60 Ed. Assigning attacks in cyberspace as cyberterrorism or cybercrime is complex and usually not possible without contradictions.

Consequently, the difficulty of attributing responsibility for aggression, as examples from recent years have shown is an issue that poses many challenges.[61] One of the great "strengths" of the hybrid (war) approach is that responsibility is difficult to prove. One area that is much debated today is the responsibility of states when actions emanating from their territory cause harm to other states. Above all, the obligations of the state to prevent such action need to be clarified.[62] This is particularly true regarding the support of hacker groups[63] (also known as "advanced persistent threats" (APT's)), which mostly operate from safe third countries. Due to the complexity and nature of these attacks, they can be assigned to a certain grouping. The company Fireeye is the market leader in the field of software for the identification and analysis of cyber-attacks and provides information about the most dangerous groups at the moment, their presumed bases of operations and their (state) supporters.

In a specialist article published in the *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* (ZaöRV) According to Hector, hybrid warfare increases factual uncertainty and makes it more difficult to apply the rules of international law. However, he concludes that it is not an entirely new category of warfare and as such there is no need to change international law when evaluating it.[64]

In the context of hybrid warfare or hybrid power projection[65], not only military, but also diplomatic, economic, and other means are used.[66] The use of terrorism for the purposes of a state is described by Ellinger as the provocation of a "domestic" war by using the help of terrorism. As such, he describes it as a "proxy war", where terrorist groups are supported by "protective powers."[67]

4 TERRORISM AND THE OVERLOADING OF THE STATE UNDER THE RULE OF LAW

Münkler often speaks in his publications about the disadvantages of a "post-heroic" society[68]. Because only "heroic" societies have the will to wage wars, "post-heroic" societies are particularly vulnerable to the phenomenon of terrorism. Democracies offer

61 Ed. This applies in particular to the assignment of hacker groups as well as to the soldiers in Crimea, often referred to as "green men" (their affiliation to Russia was subsequently confirmed).

62 Cp. Hector (2016, p. 522.).

63 Ed. Hacker groups have a base of operations from which they carry out attacks. These groups are often referred as APT groups.

64 Ib. Cp. P. 523.

65 Ed. The term has changed in its use in recent years from warfare to the projection of power, as the "threshold of war" is not crossed.

66 Cp. Hartmann (2015, p. 18f).

67 Cp. Ellinger (1990, p. 20.).

68 Ed. By this he means central European society from a time after the World Wars to the end of the Cold War and after. A society that has evolved and separated itself from its own past.

good and easy ways for terrorists to move around, with porous borders, mobility, and general freedom of movement. These possibilities and the often-incomplete surveillance measures of democratic states make it easy for terrorist groups to find "reward" targets for their attacks.

The West's dilemma is the debate over the enforcement of protective and anti-terrorist measures: whether to restrict freedoms and state supervision on the one hand or to decide on waging a "war on terror" on the other.[69] Many laws legislate, for example, against the financing of terrorism[70] or for the removal of terrorist content from the Internet.[71] The problem in the fight against terrorism and asymmetric methods is above all finding an "adequate" response to terrorist attacks. Maintaining public order and security is the focus but must be brought into line with democratic principles and fundamental rights. In particular, the first measures taken after a terrorist attack are often "hasty" and insufficiently evaluated in a cost-benefit calculation.[72]

The legal basis for ensuring adequate "protection" of the population and constitutional institutions, including cyberspace, is often difficult to reconcile with fundamental rights. Identifying and dealing with so-called "returnees" and "danger" poses a major challenge, as our legal understanding does not provide for preventive criminal prosecution. Essentially, for western democracies, it remains a tug-of-war between personal freedom and security, and the willingness to accept human losses and the high costs of "warfare" on terror.

5 THE AUSTRIAN COMPREHENSIVE APPROACH

The reactions and possible solutions are diverse. This section provides an insight into a nation-state approach using Austria as an example.

The Austrian "comprehensive national defense" is enshrined in the Federal Constitutional Act Art. 9a and includes the areas of military, intellectual, civil, and economic national defense.

The task of the intellectual national defense according to the Federal Ministry of Education, Science and Research "… consists in conveying democratic values and creating a comprehensive awareness of democratic freedoms and the civil and human rights enshrined in the federal constitution within the framework of political education."[73] This

69 Ed. This was declared by George W. Bush in the wake of the attacks of September 11, 2001, and by French President François Hollande in the wake of the attacks in Paris in 2015. It has far-reaching implications.

70 Ed. In Austria this was combined with the implementation of the directive 2015/84co9/EU, the 4th. Money laundering directive, the directive 2018/843/EU, the 5th. Money laundering directive in the form of the Finanzmarkt-Geldwäschegesetz (FM-GwG) and in the Strafgesetzbuch § 278d. Terrorismusfinanzierung.

71 Ed. The European Parliament Regulation on combating the dissemination of terrorist content online was adopted by the Council on 16 March 2021 and is expected to enter into force in 2022.

72 Cp. Kellner (Oktober 2017, p. 4f.).

73 Ed. This definition is released by the Federal Ministry Republic of Austria Education, Science and Research.

task is expressed, among other things, in the basic decree on political education and, based on this, in the curricula.

The military national defense as the second pillar of the "comprehensive national defense" is related to the Federal Ministry of Defense in Austria.

The third pillar of the "comprehensive national defense" is the civil national defense which includes the entire civil protection, as well as the functioning of the civil authorities in the event of a defense or the maintenance of internal security by the police.

The fourth pillar is the economic national defense which includes all measures that the economy can continue to operate in times of crisis and or war. This includes the storage of energy supplies, food, critical drugs, and other critical consumer goods.

The coordination and cooperation of these sub-areas to create a functioning, comprehensive national defense is one of the Austrian national goals and thus the top priority of politics.

CONCLUSION AND DISCUSSION

The appearance of wars has changed dramatically in the recent decades. Conventional wars between states are no longer waged due to the high use of resources by the entire state. Because of these changes, the term "new wars" is often used to describe how terrorist groups achieve objectives in addition to the "classic" means of intervention of states. Terrorist organizations are far inferior to Western armies in terms of weapon technology and manpower. For this reason, they use asymmetric methods of warfare to target the weaknesses of the Western states. These organizations use modern media for training, financing and recruitment, as well as technical networks (Internet) to achieve their objectives.

Consequently, conventional wars have changed into hybrid wars. In the context of this warfare, military-, diplomatic- and economic measures are used to achieve the objectives of the state. Supporting and using terrorist groups to achieve objectives is a simple and highly effective method to support own (hybrid) operations. This includes the provision of safe havens, weapons and equipment or the provision of information. This type of use of terrorist groups has meanwhile reached the cyberspace, where individual groups (state-affiliated APT groups) repeatedly succeed in carrying out successful actions.

The legal status of terrorist organizations is a major problem for the rule of law. Dealing with "returnees", responding to terrorist attacks, the distinction between crime and terrorism (especially in cyberspace) is difficult and not easy to solve.

The "war on terror" is governed by different rules and principles and is extremely difficult to wage (as past conflicts have shown). Conflicts last a long time and victory against terrorism is hardly possible due to the networked structure of terrorist organizations and the way they intermingle with the population.

Therefore, a statewide approach as conceived in Austria with the comprehensive national defence approach to increase the resistance of the state is a possible way to meet these challenges. Another approach must be a supranational cooperation in prevention and in strengthening the resilience of individual states.

Author: ***Major Mag.(FH) Dr. Alexander TREIBLMAIER, MA, MSc****, born 1981. He was promoted as officer in 2011 and completed the Master studies at the University of Sopron (Management and Leadership) and at the Austrian National Defence Academy in Vienna. He completed his doctoral studies at the University of Belgrade in the Department of International Management. He is the Head of the Institute Cyber and electronic warfare at the signal school of the Austrian Armed forces in Vienna. His military professional career and experience reaches from the work as platoon-leader, staff officer (G-6 branch) at the 3rd mechanized infantry brigade and teacher for tactics at the signal school. During his academic career, he specialized in military leadership in combination with management science and the impact of international trends and the technological developments on the training and education in the Austrian Armed forces.*

How to cite: TREIBLMAIER Alexander. The New Wars: Terrorism and "Asymmetric" Warfare. *Vojenské rozhledy*. 2021, 30 (4), 093-108. ISSN 1210-3292 (print), 2336-2995 (online). Available at: www.vojenskerozhledy.cz