SPECIAL EDITION

ISSN. 1307 - 9190
Vol/14-2022

Defence Against Terrorism Review

DATR

Terrorism Threat During Peer-to Peer Conventional War - A Backround Study -

Tamás Csiki Varga - Krisztán Jójárt
András Rácz - Péter Tálas

COE-DAT
Centre of Excellence Defence Against Terrorism

Tamás Csiki Varga[1] – Krisztán Jójárt[2] - András Rácz[3] – Péter Tálas[4]:

Terrorism Threat During Peer-to-Peer Conventional War

A Background Study

[1] Research fellow: Institute for Strategic and Defense Studies, Eötvös József Research Center, National University of Public Service, Budapest, Hungary
[2] Assistant research fellow: Institute for Strategic and Defense Studies, Eötvös József Research Center, National University of Public Service, Budapest, Hungary
[3] Senior Research Fellow: German Council on Foreign Relations (DGAP), Berlin, Germany. Senior Associate Fellow: Institute for Strategic and Defense Studies, Eötvös József Research Center, National University of Public Service, Budapest, Hungary. His research was supported by the research grant No.129243., titled "Tradition and Flexibility in Russia's Security and Defense Policy" provided by the National Research, Development and Innovation Office of Hungary.
[4] Director of the Institute for Strategic and Defense Studies, Eötvös József Research Center, National University of Public Service, Budapest, Hungary. This research was supported by the research grant No. TKP2021-NVA-16, titled "Research in applied military engineering, military and social sciences in the field of national defense and national security at the Faculty of Military Science and Officer Training" provided by the National Research, Development and Innovation Office of Hungary.

Preface

(Terrorism Threat During Peer-to-Peer Conventional War: A Background Study)

War and strategy developed reciprocally as instruments by which nations may impose their will on other nations. The unrestrained use of all the possible instruments of war were used with few legal restraints until the late 19th Century. The advent of industrialized warfare introduced devastation on a far larger scale than previous wars. As a result of the ramifications of such destruction, international regulations were constructed to push nations to negotiations instead of war to settle international disputes and to lay out what is acceptable or unacceptable in war.

As Clausewitz stated in his book "On War", there are always Purpose, Goal, and Means in war. The Purpose of war is for one's will to be enforced, which is determined by politics. The Goal of the conflict is to defeat the opponent in order to exact the Purpose. The Goal is pursued with the help of a strategy that might be brought about by various military or non-military Means to resolve the conflict (such as propaganda, economic sanctions, and political isolation). Thus, any resource of the human body and mind and all the moral and physical powers of a state might serve as Means to achieve the set goal. In the 21st Century, the evolving nature of communication and war uncovered terrorism as a Means to achieve one's Purpose.

The dissolution of the Soviet Union ended the rivalry between the USSR and NATO, and, for a period of time, established a unipolar world order. The world is yet again changing, this time from a unipolar to a multi-polar world. In this process, NATO, and partner nations, must consider the prevalent view of war as comprising conventional kinetic actions to include unconventional and hybrid activities that fall below the threshold of conventional kinetic warfare. The rise of Russia as a resurgent great power that is significantly weaker than NATO, requires Russia to use all Means possible to confront NATO to include terrorism as a means of hybrid warfare.

The aim of this study is to explore how terrorism was and could be used by Russia to integrate with potential conventional warfighting efforts during a peer-to-peer conflict. Keeping in mind what the NATO Heads of States articulated in the most recent Brussels Summit communique: "Russia's aggressive actions constitute a threat to Euro-Atlantic security; terrorism in all its forms and manifestations remains a persistent threat to us all." COE-DAT suggests that the cases, which are tackled in this paper, and approaches can be best practices to consider when planning a defense against terrorism.

This study is a collaboration between COE-DAT and the Institute for Strategic and Defence Studies, Eötvös József Research Center, National University of Public Service, Hungary. I would like to thank them for their partnership and collaboration. I also sincerely appreciate the tireless efforts of the authors and my staff. A very special thanks goes to Colonel Attila CSURGO, because without him it would have been impossible to finish this project. COE-DAT is also grateful to everyone who contributed to this project.

A little about COE-DAT

COE-DAT provides key decision-makers with a comprehensive understanding to terrorism and CT challenges, in order to transform NATO and Nations of interest to meet future security challenges. This transformation is embedded into NATO's three declared core tasks of Collective Defence, Crisis Management, and Cooperative security.

As a strategic level think tank for the development of NATO DAT activities sitting outside the NATO Command Structure, COE-DAT supports NATO's Long-Term Military Transformation by anticipating and preparing for the ambiguous, complex, and rapidly changing future security environment. COE-DAT is able to interact with universities, think tanks, researchers, international organizations, and global partners to provide critical thought on the inherently sensitive topic of CT. COE-DAT strives to increase information sharing within NATO and with NATO's partners to ensure the retention and application of acquired experience and knowledge.

Oğuzhan PEHLİVAN (PhD)
Colonel (TUR A)
Director COE-DAT

DISCLAIMER

The research paper is a product of the Centre of Excellence-Defence Against Terrorism (COE-DAT). It is produced for NATO, NATO member countries, NATO partners, related private and public institutions and related individuals. It does not represent the opinions or policies of NATO, COE-DAT or the framework and sponsoring nations of COE DAT. The views and terminology presented in this research paper are those of the authors.

Table of contents

I. Introduction

Though its original core task was and still is to ensure the military security of its member states, the North Atlantic Treaty Organization (NATO) has for long been extending its competences, also adopting the goal of effectively countering the various forms of terrorism. This has particularly been so since the end of the Cold War, when the end of bipolarity has resulted in the emergence of a highly unstable, unpredictable security environment and the growing action potential and broadening capacities of non-state actors. The tragic attacks on New York and Washington D.C. on 11 September 2001 led to the first-ever invocation of the collective defense clause (Article 5.) of the Washington Treaty. Even though NATO's 1999 Strategic Concept already identified terrorism as one of the risks affecting alliance security, NATO primarily oriented itself towards combatting international terrorism, and particularly its forms connected to "religiously motivated terrorism" after the 9/11 attacks. By adopting the Prague package of counterterrorism measures in 2002, NATO gained a solid foundation for coordinated action against terrorism, further enhanced by the 2012 Chicago Summit decisions and drafting the NATO Military Concept for Counterterrorism. The Alliance got engaged in large-scale counterterrorism and stabilization missions in Afghanistan, in Iraq, and on the Mediterranean Sea, among others, to tackle the challenges of international terrorism, keeping both state and non-state actors' potential activities of terrorism under examination.[i]

The fundamental transformation of NATO's security environment that followed the crisis in Ukraine in 2014 resulted in refocusing Alliance activities on territorial defense. More than two decades after the end of the Cold War, a conventional war broke out in the European theatre, thus direct vicinity of NATO and has been going on ever since with varying intensity.

Despite the altered prioritization of allied agenda, it is important to note that NATO's counter-terrorism work spans across all three core tasks: collective security, crisis management and cooperative security. Meanwhile, for the purposes of the current study it is the field of collective security where the use of terrorism by a peer competitor primarily appears. The re-orientation of NATO towards territorial defense, however, did not mean either that the challenges of terrorism had disappeared. Moreover, combined with the potential threat of a conventional war against a peer-to-peer competitor in the East, NATO may well need to face a new form of terrorism, namely one that is organized and conducted by the very same competitor.

Hence, the present study intends to map out, how a peer-to-peer competitor may use methods and means of terrorism against NATO in case of a full-scale, conventional war either directly or indirectly through proxy actors. The authors intend to identify the objectives to be pursued by the adversary by such methods of terrorism, as well as the tools and means of attacks, together with their potential target spectrum. Importantly, evaluation of how Russia would pursue conventional military operations against a peer competitor falls beyond the scope of the study. The authors solely focus on how the tool of terrorism could be used by Russia to complement (and not substitute) its conventional warfighting efforts.

Concerning its structure, the study is composed of four main parts. Following an introduction that also clarifies the conceptual framework and terms used in the analysis, the second chapter discusses the role and place of terrorism in the military thinking and practice of NATO's most important peer-to-peer competitor, namely Russia. Particularly since 2014, Russia has been posing the most pressing military-related challenges to NATO, confirmed also by the recent Communique of the Brussels NATO Summit Declaration released on 15 June 2021.[ii]

The third chapter enumerates and studies the main possible types of terrorist attacks to be potentially committed by a peer-to-peer competitor in case of a conventional war, based on historical and recent examples of both successful and unsuccessful attempts. Finally, the study ends with a brief, concluding chapter.

In terms of sources, the paper relies on primary, secondary, as well as on tertiary sources. While the analysis relies on NATO's terminology as a conceptual framework to make the results fully compatible with the Alliance's policy and discourse, authors put great emphasis on presenting the Russian interpretation of warfighting and terrorism too. Consequently, a significant number of the sources used are from Russian authors, let the given materiel be published in Russia or abroad. The analysis is based solely and exclusively on open sources.

Concerning methodology, authors intend to reach their research objectives by studying both the theoretical works of the adversary on the use of terrorism, as well as historical examples of employing such methods. In addition to this, contemporary cases are going to be studied in detail as well, particularly to map out the ways of how and against what targets may the adversary employ methods of terrorism. Authors are aware of the limitations imposed by the 'fog of war' in this context, namely that one may hardly have full access to all relevant information on contemporary events. Therefore, it is important to note that the potential means and methods of terrorist attacks elaborated in this study do not necessarily reflect

actual Russian intentions. It is impossible to forecast based on open sources how Russia would use (if at all) terrorism in a peer-to-peer conventional war. Nevertheless, the authors are convinced that writings of Russian military thinkers as well as historical and contemporary examples of the use of terrorism may well illustrate both the objectives that the adversary may intend to reach, as well as the tools at its disposal.

The views described in this paper represent only the personal opinions of the authors and cannot be considered as official positions of any institutions, organizations or countries. All errors possibly remaining in the text are solely of the authors' responsibility.

Terms and definitions

In order to address the possible forms of terrorism NATO may need to counter in case of a conventional peer-to-peer war, it is necessary to define the exact content of the term 'terrorism' used in the present study. Terrorism does not have a single, unified definition that would be accepted globally. Many regional organizations have their own definitions, so do countries and think tanks, but a jointly agreed one is missing. Hence, the present analysis relies on the definition of terrorism as it is provided by the *NATO Military Committee Concept for Counter-Terrorism*,[iii] published in 2020, which is as follows:

> *„The unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives."*

It is worth comparing this definition to its predecessor, namely to the 'terrorism' definition used in the *NATO Glossary of Terms and Definitions*, published in 2013, so yet before the breakout of the crisis in Ukraine:

> *The unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives.* [iv]

The comparison of the two definitions reveals that following the breakout of the conflict in Ukraine, a new extension was added to the earlier term: '*or to gain control over a population*', which is an apparently clear reference to the events in Eastern-Ukraine.

This 2020 definition allows for the use of a wide, comprehensive interpretation of terrorism in the present study. First, the definition does not limit the occurrence of terrorism either to the times of peace or of war. In other words, terrorism may occur not only in peacetime, but also during a war.

Second, while reaching military goals is not specifically listed in this definition, as this analysis focuses on the context of a peer-to-peer conventional war, attacks against military targets need to be evidently included into the category of the political objectives. The reason is that in wartime the two are essentially inseparable, and anyone who attacks any military target affects the political situation too. In other words, attacks against targets of military significance will also need to be addressed here, together with other forms of terrorism. This is also in concert with NATO's understanding of *antiterrorism* defined in the same document of 2013 (and quoted below), that – unlike the definition of terrorism –presupposes the attack of not only civilian but military targets too. Similarly, while cyber is not listed either, due to its critical role played in the functioning of governments and militaries, cyber attacks directed against a target of any political, religious or ideological value cannot be spared from this analysis either. As it is unclear, whether cyber attacks count as terrorism, hereby only those ones will be assessed, that were used to sabotage elements of critical infrastructure.

Third, 'property' has no exact definition in the aforementioned *Glossary*. Hence, in the absence of an exact, narrow definition, terrorism may be directed against any elements of private property, critical or civilian infrastructure, vehicles, housing, other objects of value and against any other non-living targets as well.

Fourth, this definition permits to include terrorism committed both by state and non-state actors alike. From the perspective of the present study, this means that the problem of differentiating between state and non-state perpetrators of terrorist acts can largely be omitted. Once in case of a peer-to-peer conventional war the adversary decides to also employ methods of terrorism, and this can be credibly attributed, it will not be important anymore, whether the actual perpetrator is *de jure* a state or non-state organization. Instead,

along the definition above, all threatened or realized unlawful attacks against individuals or property will count as terrorism, regardless of who actually committed it. Consequently, all such attacks, once properly attributed, will need to be dealt with in the military, security, law enforcement and legal context of the peer-to-peer conventional war.

In other words, attribution will be much more important than the exact legal status of the perpetrator of a terrorist attack. This is particularly important to realize, because a peer-to-peer competitor may have a rich arsenal of proxies and other, formally unaffiliated actors (private military companies (PMCs), paramilitary formations, organized crime groups, etc.) that can also be employed in case of a conventional war. The readiness of the adversary to rely on formally unaffiliated actors in reaching political or military objectives has been demonstrated several times in the conflict in Ukraine, in the South Caucasus, as well as in Syria, Libya and in other parts of the world.

As the main task of the present study is to assess the risks and potential targets of terrorist attacks committed by an adversary in a peer-to-peer conventional war, it is also important to enumerate the definitions of antiterrorism and counterterrorism, as these are inherently necessary for providing a comprehensive assessment, even if this study focuses only on the potential forms of terrorist actions.

Antiterrorism was defined by NATO in the same 2013 document as:

> *All defensive and preventive measures taken to reduce the vulnerability of forces, individuals and property to terrorism. Note: Such measures include protective and deterrent measures aimed at preventing an attack or reducing its effect(s).*[v]

The definition of counterterrorism was as follows:

> *All offensive measures taken to neutralize terrorism before and after hostile acts are carried out. Note: Such measures include those counterforce activities justified for the*

> *defense of individuals as well as containment measures implemented by military forces or civilian organizations.*[vi]

However, the newer, 2020 *Concept for Counter-Terrorism*[vii] unified and extended the two earlier definitions under the term counter-terrorism:

> *All preventive, defensive and offensive measures taken to reduce the vulnerability of forces, individuals and property against terrorist threats and/or acts, and to respond to terrorist acts. In the frame of the NATO Comprehensive Approach (Reference J1), these measures can be combined with or followed by measures enabling recovery after terrorist acts.*

Noteworthy is that the new, comprehensive definition includes also military capabilities among the potential targets of terrorists, as one of the purposes of counter-terrorism is to 'reduce the vulnerability of forces'. This confirms the earlier assessment that even though the very definition of terrorism does not enumerate specifically military elements as subjects of terrorist attacks, de facto this analysis needs to consider them also as potential targets of terrorism.

An important content-related restriction of the study is that it does not analyze in detail the possible ways NATO and its member countries may defend themselves against the possible attacks enumerated below. The sole objective of the present analysis is to map out, how a peer-to-peer adversary may use means of terrorism against NATO. Hence, authors do not intend to assess either the likelihood of the possible attacks, nor the ways of preventing or countering them. Neither addresses the paper the dangers of WMD-terrorism, as it is focused on conventional war.

II. Russia as the main peer competitor of NATO

The security environment of NATO has drastically transformed since the spring of 2014, when the crisis in Ukraine begun. While earlier the Alliance was focusing on out of area operations and crisis management for more than a decade, events in the Crimea as well as in Eastern Ukraine pushed NATO to quickly change its focus.

Russia's illegal and illegitimate annexation of Crimea and the destabilization of Eastern Ukraine brought NATO to enhance its conventional deterrence and defense posture in several steps at the 2014 Wales (Readiness Action Plan) and 2016 Warsaw Summit (enhanced forward presence), reinforced by subsequent Brussels Summits (Readiness Initiative – 2018; NATO 2030 Agenda – 2021). This policy shift and resulting actions are also driven by concerns about Russia's continued destabilizing pattern of military activities and aggressive rhetoric that span well beyond Ukraine, including the military build-up close to NATO's borders, Russian hybrid actions, including disinformation campaigns, and its malicious cyber activities.[viii] Most recently, the 2021 Brussels Summit Communiqué precisely summarized those activities that are perceived as alarming or threatening by NATO as well as such examples of Russian assertiveness that had increased insecurity in recent years (primarily Par. 11&12):[ix]

- 'Russia's growing multi-domain military build-up, more assertive posture, novel military capabilities, and provocative activities, including near NATO borders, as well as its large-scale no-notice and snap exercises, the continued military build-up in Crimea, the deployment of modern dual-capable missiles in Kaliningrad, military integration with Belarus, and repeated violations of NATO Allied airspace, increasingly threaten the security of the Euro-Atlantic area and contribute to instability along NATO borders and beyond.'
- 'In addition to its military activities, Russia has also intensified its hybrid actions against NATO Allies and partners, including through proxies. This includes attempted interference in Allied elections and democratic processes; political and economic pressure and intimidation; widespread disinformation campaigns; malicious cyber activities; and turning a blind eye to cyber criminals operating from its territory, including those who target and disrupt critical infrastructure in NATO countries. It also includes illegal and destructive activities by Russian Intelligence Services on Allied territory, some of which have claimed lives of citizens and caused widespread material damage.'

The above enumeration of harmful and hostile Russian actions makes clear that in spite of the power asymmetry, Moscow has both the will and the capability to challenge NATO. Moreover, thanks to its nuclear arsenal Russia is able to pose an existential threat to the Alliance. Meanwhile, despite in the Brussels Summit Communique China was mentioned in a NATO document for the first time, due to its geographic limitations and its member states' altering views, it is unlikely that Beijing would appear as NATO's peer competitor in the foreseeable future. Consequently, it is Russia that is seen in the role of a peer competitor by the Alliance. While keeping in mind the full-spectrum threat landscape that reaches far beyond the military domain, NATO pursues a dual-track approach towards Russia: meaningful dialogue on the basis of a strong deterrence and defense posture. However, none of these would effectively force Russia to exclude the possibility of relying also on terrorist activities in a potential peer-to-peer conflict.

Russia's warfighting and terrorism: a theoretical background

To gain an in-depth understanding of how Russia may employ methods of terrorism in a conventional war, it is important to analyze the problem also in the context of Russian military thinking and on the Russian concepts of warfighting. As opposed to the conventional Western wisdom that often regards hybrid wars as grey zone conflicts (i.e., below the threshold of war), Russian authors' writings on the topic do not underline that hybrid warfare would necessarily stay under the level of conventional armed confrontation. All in all, this is exactly what happened in eastern Ukraine after non-military means used by Moscow failed to bring about the desired result. Moreover, in the Russian perception, Western way of war – generally described as new type war or more recently, hybrid – while seeks to carry out regime change with non-military means (a so-called color revolution), does not refrain from escalation to the level of open war either, if needed. Consequently, assuming that the use of terrorists and other proxy actors in the Russian strategy is centered around grey zone scenarios is an erroneous view. Russia would most likely also use these same means during a large-scale conventional war.

Contemporary Russian military thinking dedicates utmost importance to the role of asymmetric and indirect methods, including the use of terrorist formations both to defend the country against such actions and to utilize them for offensive purposes. Soviet military strategist Andrey Snesarev noted in 1926 that "war can be waged not only by the sword, but also by other means such as agitation, crushing of the enemy's economy, or the reconstitution of one's own forces"[x] Such a complex understanding of war is reflected in contemporary Russian military literature

as the Russian military elite had rediscovered Snesarev's and other less known Soviet military theoreticians' works in the past two decades. While the use of non-military means is not alien to Soviet/Russian strategy, their primacy over military force is a new phenomenon. As Bartles points out, Russian operational art until recently had been much more military oriented than its U.S. counterpart[xi]

Russian military thinkers acknowledge that the majority of today's wars lack clear frontlines and recognizable distinction between combatants and non-combatants. Therefore, violence against the civilian population is the very essence of contemporary conflicts.[xii] This conviction about the general character and rules of war legitimizes the use of immoral (and outright unlawful) means and methods by Russia, too. Russian military analysts thoroughly followed asymmetric conflicts of the past decades waged by insurgents and terrorists and drew the conclusions that might be relevant for Russia. One such lesson recurring in several military publications is that the United States and its Western allies are more sensitive to human losses and they possess various vulnerable objects that are crucial for the functioning of their economies and societies.[xiii] [xiv] Exploitation of such vulnerabilities is the core of Russian asymmetric strategy. Targeting civilian infrastructure and personnel seems to be fair game for Russian military thinkers in the circumstance of an all-out war with a peer competitor. They foresee the use of terrorists and other illegal formations for both operational and strategic purposes. Elimination of decision-makers and key military personnel through targeted killings on enemy soil is clearly contemplated by Russian military theoreticians as an asymmetric method to overcome the United States' technological advantage and superior C4ISR capabilities.[xv] Disguising such special operations as terror attacks can insulate Russia from the consequences of a retaliatory strike or an unwanted escalation. One Russian military expert stipulates attacking the "enemy's state structure and regular army with the help of local insurgents and separatists supported with weapons and money from abroad."[xvi]

Employing terrorist methods can also have strategic impact in as much as it can compel the leadership of the enemy state to concede to ones' political will – which is ultimately the goal of war according to Clausewitz's classical definition. Russia actively pursues to complement its nuclear deterrence with nonnuclear means to create a more flexible and credible deterrence posture. Russian authors point out that nuclear weapons no longer ensure a state's sovereignty and integrity amidst cyber, network-centric, psychological and biological warfare. They note that information, economic and terrorist warfare is becoming natural.[xvii] Nonnuclear means of deterrence include precision nonnuclear weapons, cyber, electronic and information warfare

capabilities, anti-satellite systems and weapons based on new physical principles to cause unacceptable damage to the enemy without escalating the conflict to the nuclear level. As Vladimir Putin put it, "these weapons systems [i.e., information, cyber, cosmic and weapons based on new physical principles] will be comparable in their impact to nuclear weapons however, more "acceptable" in political and military planning."[xviii] Logically, destroying elements of critical infrastructure by relying on terrorists, local criminal networks or special operations forces would constitute a nonnuclear means of deterrence too. Some Russian military thinkers argue, that threatening with the destruction of an ecologically hazardous object like a nuclear power plant could incite the enemy population to force its government to change its political goal.[xix] Inflicting unacceptable damage to the enemy's key economic objects and critical infrastructure with the use of proxies can coerce the adversary to end the war on terms acceptable to Russia.

There is also an incentive to use terror acts to provoke an overreaction by the enemy or as part of the information campaign. Russian military authors frequently point to the example of the ethnic cleansing in Kosovo that reasoned the NATO bombing of Yugoslavia in 1999. Russian military expert, Valery Kiselyev claims, that it was the Kosovo Liberation Army that chased the Kosovar Albanians away from their homes and drove them to the border where Western correspondents had been already waiting with their cameras.[xx] Russian military articles are less vocal in mentioning how the infamous apartment bombings in Russia throughout 1999 September – which many believe was an inside job of the FSB – facilitated public support for the Second Chechen War. Or how Moscow evoked fear in the Russian population of Crimea threatening with pogroms of the "Kiev junta" preceding the war in Ukraine. Russian academicians Aleksandr Selivanov and Sergey Chvarkov writing about the principles of asymmetric warfare, advise to present the enemy's excessive use of force to the international community as mass killing of the civilian population and war crime, by this turning an enemy advantage to our benefit.[xxi] Another prolific military author, Aleksandr Bartosh discusses how the use of terrorist groups, organized criminal networks and private military companies allow for carrying out the dirtiest provocations in a hybrid war.[xxii] These opinions are indicative with regard to how Russia would rely on the tools of terrorism to provoke the enemy into taking actions that actually serve Russian interests – a clear example of reflexive control.

The dominance of the logic described above is reflected also in Russia's official military discourse on terrorism. According to definition provided by the military dictionary available on the website of the Ministry of Defense of the Russian Federation, terrorism[xxiii] may be directed

at disrupting the security of the society, intimidation of the population and at influencing the authorities to make such decisions that are beneficial for the terrorists. Similarly, to the terrorism perception of NATO described above, the Russian definition also does not differentiate between state and non-state terrorism, or whether the act is perpetrated in times of war or peace.

However, in other aspects the Russian Ministry of Defense definition is more specific than the one of NATO: it includes attacks specifically against the lives of state leaders or leading social figures with the objective of hampering their activities, or in revenge for their earlier activities. Moreover, 'terrorism' may also imply attacks on the representatives of foreign states and international organizations with the objective of provoking a war or hampering international relations. Hence, apparently not only military theorists, but also practitioners of the Ministry of Defense endorse the concept that in certain cases means of terrorism may be used to provoke a war, and also to compel the leadership of the adversary to act in a certain way.

The concept of interstate terrorism

A core difference compared to the NATO definition of terrorism is that in the Russian military thinking specific attention is paid to the possibility of states using terrorist methods to achieve their political objectives. The official Russian term for this phenomenon is 'interstate terrorism' (*mezhgosudarstvenniy terrorizm*), which is fully different from 'international terrorism' (*mezhdunarodniy terrorizm*), as the latter expression means the international networks and functioning of terrorist organizations.

Interstate terrorism, however, means specifically those cases when the perpetrators of terrorism are states. As defined by the military-political dictionary[xxiv] edited by Dmitry Rogozin, Russia's former ambassador to NATO and Deputy Prime Minister responsible for defense industry in 2016, interstate terrorism[xxv] is:

> *...a method of intimidating* (may also mean *deterring* – authors) *an adversary state by an aggressor state influencing it with means of terrorism. The purpose of this kind of action is the physical elimination of the representatives of the political leadership and military command of the adversary state, or provoking mass panic*

and chaos via organizing terrorist acts against the civilian population.

As in 2016, when the book was published, Rogozin was still Deputy Prime Minister, it is safe to assume that his involvement as an editor may well be considered as an indicator that the terminology largely reflects the official position of the Russian state.

Noteworthy is that the Rogozin definition of interstate terrorism is very much in line with the Russian perception of contemporary armed conflicts described above. Terrorism is a form of state-level aggression, and the elimination of enemy political and military leaders is an integral part of the aggressor state's objectives, and so is the intimidation or disorganization of the adversary's society.

In fact, the concept of interstate terrorism is significantly older than the Rogozin dictionary. Salman Dukaev[xxvi] defined interstate terrorism already ten years earlier, in 2006, as an act of states using methods of terrorism. Interstate terrorism can be attributed to the secret services of states; hence, these actions are prepared and conducted with a high level of professionalism. Dukaev also defined the characteristics of interstate terrorism: a) it is generally of top secret nature; b) states deny their involvement in it, and blame the opposite state instead; c) terrorist actions are carried out either directly by the secret services of the given country, or via recruiting international terrorists; d) if successful, interstate terrorism may be more efficient in ensuring the realization of the interests of the given state than a conventional military operation. Examples of interstate terrorism may include the involvement of Afghan services in bombing attacks in Pakistan, and repeated U.S. attempts on the life of Fidel Castro and Saddam Hussein in order to change the political regimes in Cuba and in Iraq.[xxvii]

All in all, the concept of states using means of terrorism to realize their political and military objectives is an integral part of contemporary Russian military thinking. Hence, NATO needs to be aware that in case of a peer-to-peer conventional war it is highly unlikely that Russia would not rely on such tools and means, should it deem them necessary for realizing its desired interests and for countering the technological superiority of the Alliance.

III. Main possible types of terrorist attacks

In order to assess, what kind of terrorist attacks may NATO face in case of a peer-to-peer conflict against Russia, one may rely both on theoretical knowledge, as well as a on historical and actual examples from Russia's earlier wars.

The Soviet Union is known to have deployed arms, explosives and ammunition caches in the West in preparation for a full-scale war to break out. These supplies were supposed to be used against both civilian and military targets. While during the Cold War there was only sporadic information on the existence of these sites, after 1991 some of them could be identified. A key role in this was played by Vassily Mitrokhin, a defected archivist of the KGB, who smuggled out the copies of several thousands of documents from the archives of the Soviet secret service; later an important book was written from the collection with the help of Christopher Andrew: *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*[xxviii]. With the help of Mitrokhin's data, as well as of Oleg Gordievsky, a defected chief of station of the KGB's London *rezidentura*, two such arms caches could be identified in December 1998, one in Switzerland and one in Belgium.[xxix] In addition to these two sites, the memoirs[xxx] of Victor Cherkashin also support the existence of such plans to planting secret arms caches to the West, should a large-scale war against the Soviet Union break out.

Regarding contemporary examples, particular attention needs to be paid to the conflict in Ukraine and how Russia has been fighting there. The reason of this prioritized position of Ukraine is that this is the sole case, where it is possible to study Russia's actions in times of a conventional, albeit limited war. Limited war in the context of Ukraine means[xxxi] that the belligerents do not fight with their full capacities; from this perspective, limited war is the opposite of total war. The conflict is spatially confined to certain sections of the common Russian-Ukrainian border, while other sections are calm; diplomatic relations did not get severed, travel and logistical connections are still functional, while the limited intensity fighting also prevails. Still, despite these particularities, the conflict in Ukraine is the only war that Russia has been fighting against another state and has been doing so already for the seventh year.

Hence, if one intends to study Russia's likely moves in times of a full-scale conventional war, Moscow's actions in Ukraine probably constitute an indicative, lower threshold: what was done against Ukraine is highly likely to be done against any other, full-intensity adversary as well – and much more so. The reason for this difference is that while for Ukraine the war against Russia is a struggle that may well threaten the very existence and functionality of the Ukrainian state, for Russia it is only a regional conflict with limited effects on the Federation as a whole. However, should a large-scale, conventional war break out against the West, that conflict would be similarly crucial for Russia as the current war for Ukraine is. Hence, it is very likely that

Russia would not exercise any self-restraint but hit all the targets it can reach with all the strength it can mobilize.

The study identifies five major types of attacks Russia could carry out either via its own special services or proxies. The categorization of the types of attacks listed below reflect the organizational preferences of the authors; however, the text always indicates, if a given type of attack is also specifically mentioned in the Russian literature.

- Terrorist attacks with a strategic effect could either coerce the adversary into some political concessions, end the conflict in terms acceptable for Russia, or significantly undermine its political and/or operational capabilities. Such attacks could be also used to provoke the enemy to take actions that would actually serve Russia's interests.
- Attacks on the political/military leadership of the enemy could decapitate the adversary and slow down its reaction time in the beginning of the war. Disorganization of enemy decision-making during the initial period of war is a key element of Russian operational thinking. Targeted killing against the political leadership can also serve a geopolitical goal directly.
- Targeted killings abroad. In the past decades numerous citizens of its own as well as of other states fell victim of Russian targeted killings. The Russian state has carried out such operations for a variety of reasons not only on its territory but beyond the borders too.
- Sabotage attacks against various properties including objects of critical infrastructure could seriously hamper the mobilization of enemy forces, or undermine public support for the war. As events of the recent years demonstrated, cyber-attacks are a convenient way to cause serious disruption in vital services such as electricity or water.
- Finally, attacks aimed to stir up social tensions can push the enemy state into a political crisis, lead to regime change and can distract attention and resources to maintain internal order.

Terrorist attacks with a strategic effect

There have been no such known cases when Russia as a peer-to-peer competitor of NATO would have been involved in large-scale terrorist attacks against the Alliance. Nor are there any publicly known and independently verified examples of Moscow even planning to conduct such attacks against NATO. However, there are sporadic information, published in the memoirs of defectors from the Soviet/Russian security services, about Moscow's plans to conduct large-

scale terrorist attacks against the population of the U.S. by using biological weapons in case a full-scale war breaks out. Former GRU operative, Stanislav Lunev claimed in his memoirs that the Soviet Union had plans to poison River Potomac, as well as other water sources in the U.S. in case of a war.[xxxii] Lunev's claims were later substantiated by another defector, Alexander Kouzminov[xxxiii], a former employee of KGB's 12th Department, which was responsible for espionage on biological weapons. In his memoir Kouzminov claimed that the Soviet Union had detailed sabotage plans for a so-called Day-X, which was the code name of the breakout of a large-scale war against the West. Should that happen, according to him it was planned, besides hitting many other targets, to also poison drinking water supplies and water purification systems.[xxxiv] Such attacks, if realized, would clearly constitute massive, large-scale acts of terrorism. However, the existence of such plans, has so far not been verified by independent sources.

Until now, there has been only one case, when a terrorist attack with a strategic effect could be attributed to the Russian state with a sufficiently high veracity – however, this attack was conducted against Russia itself. This is the series of the so-called apartment bombings that rattled Russia in September 1999. The bombings had a strategic effect, because they were used by the first government of Vladimir Putin[xxxv] as a casus belli to launch the Second Chechen War. Altogether four attacks were conducted against large residential buildings – one in Buynaksk, two in Moscow and one in Volgodonsk - , killing altogether more than three hundred people. The high number of victims was due to the fact that all attacks happened at night, when most of the inhabitants were at home and asleep. A fifth attack was thwarted in Ryazan on 22 September 1999, where a vigilant resident of an apartment building spotted people at night, who were carrying sacks into the house. The police arrived rapidly and arrested the suspects, who turned out to be operatives of the Federal Security Service (FSB), Russia's internal security agency, the former head of which was actually Vladimir Putin. The packages contained explosives and were attached to a detonator that was set to explode at dawn. Later that day the Russian state media proudly announced that a terrorist attack had been prevented; Putin even praised the vigilance of Ryazan inhabitants. However, days later it was officially announced that the whole action was only an anti-terror drill, and the sacks contained only sugar. Regardless, Putin ordered the attack on the Chechen capital Grozny already on 23 September, in retaliation for the bombings.

While the attacks could never be credibly and unquestionably attributed to any organizations, there are important factors indicating that the bombings were perpetrated by the FSB. The

Chechen insurgents flatly denied the accusations about their involvement, claiming that this was not their style. A Russian parliamentary inquiry launched in 2002 by liberal MPs, led by Sergei Kovalev could not deliver any results, because the government failed to provide the requested materiel; moreover, two prominent members of the public commission, Yuri Shchekochikhin and Sergei Yushenkov were both assassinated in 2003, after which the commission ceased to work. The involvement of the FSB operatives in the Ryazan attempt was also an indicative sign. Moreover, the defected FSB operative, Alexander Litvinenko claimed in his 2002 book titled *Blowing up Russia*[xxxvi] that the apartment bombings were a false flag operation of the FSB, aimed at justifying the launch of the second Chechen war and thus elevating former FSB chief Putin to the presidency. Regardless of what exactly happened, the terrorist attacks clearly had a strategic effect, as they provided the reason for launching the Second Chechen War. Noteworthy is that attacks conducted with the objective of provoking a war are integral parts of the Russian military thinking on terrorism, as it was illustrated in Chapter 2.

Attacks on political/military leadership

Attempting to neutralize the political and military leadership of the adversary has long been an integral element of Moscow's way of waging an all-out conventional war. Both the Soviet and the Russian military intelligence have possessed the capabilities necessary for hitting high-profile targets abroad.

Already the Soviet invasion of Afghanistan commenced with an attack conducted by Soviet special operations forces disguised as local militias on 27 December 1979 against the Tajbeg palace in Kabul, which was the residence of Hafizullah Amin.[xxxvii] He was General Secretary of the Central Committee of the People's Democratic Party, an Afghan Communist politician whom the Soviet Union intended to replace with a more servient one. Soviet operatives captured and killed Amin on the spot, and thereafter Moscow installed a loyal Communist puppet politician, Babrak Karmal as the new General Secretary. This attack clearly had a strategic effect, as it decapitated the nationalist fraction of the Afghan Communist Party, thus enabled Moscow to prevent an anti-Soviet turn in Afghanistan; moreover, the killing of Amin significantly weakened initial Afghan resistance to the Soviet invasion.

Post-Soviet Russia has also attempted to kill foreign politicians to prevent undesired political turns in at least two instances. First in 2004, when Ukrainian pro-Western presidential

candidate, Viktor Yushchenko was poisoned with dioxin during the election campaign. While there is no proof the Kremlin ordered the attempt on Yushchenko's life, its unwillingness to cooperate in the investigation and the fact that granted Russian citizenship to the main suspect behind the poisoning, Volodymyr Satsyuk, the deputy head of the Ukrainian Security Service (SBU) at the time, all implicate Moscow's involvement. Russia likely feared that a Yushchenko presidency would drive Ukraine closer to the West.

Twelve years after the poisoning of Yushchenko, Moscow was planning to take out the Prime Minister of Montenegro in 2016 with largely similar means it used preceding the invasion of Afghanistan. In order to prevent the country's NATO accession, Russia intended to influence Montenegro's parliamentary election in October 2016. The alleged plan was composed of disguising Russian operatives and their local allies as Montenegrin policemen, who would shoot into the demonstrating crowds and thereafter would have killed also Prime Minister Milo Đukanovic. The attempted coup failed, and while the two Russian GRU operatives involved managed to flee, later their identities were revealed,[xxxviii] thus the effort could get attributed to Moscow. The Montenegro coup attempt is a clear indicator that not only the Soviet Union, but also the Russian Federation is ready to take a decision to eliminate the adversary's political leadership, should it deem necessary to do so.

Not surprisingly, this also applies to adversary non-state actors. During the first Chechen war Russia delivered an important blow to the insurgents, when in a targeted killing operation it managed to neutralize Dzokhar Dudayev, President of the self-declared separatist Republic of Ichkeria and de facto leader of the uprising on 21 April 1996. Russian special services managed to identify the satellite phone used by Dudayev, and thereby defined his location. Thereafter, while Dudayev was on the phone, a Russian jet launched two guided missiles, which hit the headquarters of Dudayev and killed him. The attack was an important success both in the military and domestic political terms for then Russian President Boris Yeltsin. A few years later the GRU also killed Dudayev's successor, Zelimkhan Yandarbiev in 2004, when he was already living in exile in Qatar, by using a car bomb.[xxxix]

In addition to historical experiences, the memoires of former GRU Colonel Stanislav Lunev also support the assessment that in case of an all-out conflict, one of the main tasks of the Soviet military intelligence, the GRU was to neutralize the political and military leadership of NATO countries.[xl]

All in all, one cannot exclude the possibility that in case of a peer-to-peer conflict against NATO, Moscow would indeed attempt to hit some of the political and military leaders of NATO, including both the ones of the organization itself, as well as of its member countries. It is also underlined by articles of Russian military journals as it was detailed in Chapter 2. For instance, Russian military thinkers openly advocate for the liquidation of key personnel enabling the planning and execution of an aerospace offensive.[xli] These methods also fit to the "strategy of active defense" announced by Chief of the General Staff Valery Gerasimov in his speech at the Russian Academy of Military Sciences in 2019. The strategy of active defense stipulates the use of complex measures for the preemptive neutralization of threats to the state.[xlii]

Targeted killings abroad

Conducting targeted killing operations abroad has long been an integral part of Russia's security and defense policy toolbox. Some of these actions were ordered in the framework of countering terrorism; for example, above-mentioned elimination of Chechen warlord Zelimkhan Yandarbiev in 2004 fits into this pattern. So does the killing of Zelimkhan Khangoshvili, a former combatant and field commander of the Chechen wars in Berlin's *Kleiner Tiergarten* park in 2019. In fact, since 2006 Russia has a law that permits the killing of 'extremists' abroad.[xliii] The German federal prosecutor clearly attributed the Khangoshvili-murder to Russia, and two Russian diplomats were subsequently expelled from Germany.[xliv]

Other actions took place against defectors of Russian secret services: the most famous one was the poisoning of FSB defector Alexander Litvinenko in 2006. One may argue the attack on Sergei Skripal (to be addressed in detail later) could also be put into this category, because even though Skripal was pardoned and handed over to the UK, he re-started working after a few years of passivity.[xlv]

Whatever the motivation on the Russian side may be, in the affected countries such actions may well qualify as terrorism, depending on the mode of attack, and particularly if they affect other people too. This happened both in the Litvinenko and Skripal-cases due to the careless handling of the fissile and toxic materiel (respectively) used.

In addition to hunting down defectors and political opponents, Russia has a track record of killing also critical journalists. While such actions take place mostly on Russia soil, the killing

of Belarus-born journalist and reporter Pavel Sheremet in Ukraine in 2016 was a powerful exception. Sheremet was highly critical to the functioning of the Russian regime, and was killed by a car bomb in Kyiv in bright daytime. While recently there have been information emerging about the possible involvement of Belarusian special services in the murder,[xlvi] taking into account the very cordial cooperation between Russia and Belarus in this field it is unlikely that Minsk would have moved without Moscow's at least passive consent.

Should attacks against journalists occur in higher numbers, it would probably affect the freedom of speech, as well as the public discourse in the given country or countries, thus would have also an indirect effect on the targeted society.

Noteworthy is that so far Russia has attempted targeted killings against citizens of NATO countries only in a very few cases. Bulgarian arms trader Emilian Gebrev was one of these few exceptions.[xlvii] Targets of such operations were almost exclusively citizens of Russia, Ukraine and – in the case of Sheremet – Belarus. However, taking into account the capabilities of Russian secret services to conduct such strikes also in the territory of NATO countries, technically there is not much that would prevent Moscow from striking citizens of NATO countries; for example, local leaders or journalists. Hence, the self-restraint Russia has exercised so far is most likely a result of political, and not operational considerations.

Sabotage attacks, including by cyber means

As it was described above, the Soviet Union's efforts to prepare for an all-out conflict against the West by forward-deploying arms caches are well-known. There is no public information, about whether contemporary Russia maintains these old depos, or plants newer ones. However, there have been many cases in Ukraine, when Ukrainian authorities managed to uncover both old and newly created sites, where stocks of weapons and explosives were hidden, supposedly for the purpose of future sabotage attacks. Cases from Ukraine may well indicate that the forward deployment of weapons and explosives necessary for future sabotage attacks is still an integral element of Russia's preparations for a large-scale war.

Terrorist attacks in the form of sabotage may affect elements of critical infrastructure, and the effect may vary considerably. While theoretically it is possible to sabotage such key elements of critical infrastructure that may have even a strategic effect, like a nuclear reactor, a major

hydro power plant or critical port infrastructure, so far there have been no such cases that could have been attributed to Russia.

However, on a lower, operational level Russian attempts of sabotage actions against important elements of infrastructure, nowadays increasingly often by cyber means, are well documented. Pipelines constitute a prominent target. Back in the summer of 2014, when the war between Russia and Ukraine was raging, a major explosion hit one of Ukraine's main gas pipelines delivering natural gas to Europe. Ukrainian authorities blamed Russia for the attack, arguing that by disrupting the pipeline Russia could further worsen Ukraine's image as a reliable gas transit country.[xlviii] Another, very recent case is the hacking attack against the Colonial pipeline in May 2021, which caused significant fuel shortages and massive economic loss in the affected regions of the United States. The Russian hacker group DarkSide claimed responsibility for the attack.[xlix] In Ukraine there have also been cases, when the Kyiv airport Boryspil was targeted by allegedly Russian hackers, once in January 2016[l] and second time in June 2017. The second incident was part of a major ransomware attack, which affected banks, TV stations and means of ground transport as well.[li]

The war in Ukraine has also provided several examples of sabotage attacks on a tactical scale. For example, during the battles around Donetsk in the summer of 2014, pro-Russian separatists have blown up a railway bridge, as well as two road bridges[lii] to hamper the advance of Ukraine's troops. The railway bridge was over the main road leading to Donetsk, and it was blown in such a way that its wrecks blocked also the road under, particularly because there was also a cargo train parked on the bridge, supposedly in order to make its removal even more complicated.[liii]

All in all, Russia has demonstrated several times that it is willing and able to commit acts of sabotage abroad against targets of varying significance. While it is unclear, whether such actions count as terrorism, due to their effects they also need to be factored in to the threats that NATO may face in case of a peer-to-peer conventional conflict against Russia.

Vrbetice depot explosion

Disguising special operations as accidents or terror attacks is a convenient way to avoid unwanted escalation or expansion of a conflict. Its aim is not necessarily to fully convince the opponent, but to merely provide it with a credible enough excuse not to take steps that it does not want to take anyway. When Russian special operations forces acted as local self-defense

militias during the occupation of Crimea was a good case in point. Special operations of this kind are not limited to the territory of the adversary state however.

Recent investigations of the Czech authorities and Bellingcat shed light on how the Russian military intelligence (GRU) tried to cut Ukraine off from crucial ammunition supply, not shying away from even bombing an arms depot on the soil of a NATO country. In the height of the war in 2014, Ukraine had become close to deplete its stock of ammunition. Therefore, Kyiv sought to import munition for its legacy Soviet artillery systems from any available sources. The GRU approached arms traders with competing offers to prevent Ukraine from buying their stocks.[liv] Though, when money failed to convince the arms traders, Russia's military intelligence resorted to other means. That's how Bulgarian arms dealer, Emilian Gebrev and his company, EMCO had ended up on GRU's target list. Russia's military intelligence detonated an arms depot in Vrbetice, Czechia in 2014, where EMCO was storing ammunition which the GRU believed was going to be shipped to Ukraine. It is not entirely clear if the Russian operatives intended to explode the shipment on site or once after it was delivered to Ukraine. Based on the fact that there was a second explosion one and a half month following the first one, however, it seems more likely that the first explosion had occurred prematurely due to an error and was intended to happen on Ukrainian soil. Nevertheless, prestigious military awards received subsequently by many of the participating GRU officers implies that the operation was a huge success in Moscow's point of view.[lv] Indeed, the explosion was widely believed to be caused by accident until the Czech investigation implicated Russia's GRU more than six years later. Some months following the explosions in the Czech Republic, Emilian Gebrev, his son, and EMCO's production manager had survived what was likely an assassination attempt of the GRU carried out with a nerve agent from the Novichok group in Bulgaria. As with the case of the explosions, Russia's hand in the poisoning was suspected years later and only due to another botched operation with the same chemical substance. The investigation into the attempt on Sergey Skripal's life identified Russian operatives who were present at both the Czech explosion and the Novichok poisonings in Bulgaria. Since the Kremlin perceives these missions as largely successful overall, there is no reason to expect Russia would not resort to the same methods even during peacetime, not mentioning a situation of an all-out war with a peer competitor. Even more troublesome is the fact that the above operations were tied to a unit specifically dedicated to carry out sabotage and destabilization activities; Unit 29155. Unit 29155 is believed to comprise of approximately 20 highly trained GRU operatives.[lvi]

Attacks aimed at stirring up social tensions

Inciting ethnic and social tensions within the adversary's society, including the use of terrorism, has long been present in Russian military thinking, dating way back to the Soviet times. A good example is the *myatezhvoina* concept of Evgeny Messner. Messner started his military career yet in the Tsarist Russian army, fought on the anti-Communist side in the civil war, and left Russia thereafter. He moved to Argentina in 1947, and published his most important theoretical work, *Myatezh – imya tretey vsemirnoy* (Mutiny - the Name of the Third World War) in 1960, in Buenos Aires.[lvii] Though Messner formally belonged to Moscow's enemies, his works were read and referred to by Soviet, as well as contemporary Russian military theoreticians, such as Andrei Manoylo and Andrei Budaev. [lviii]

According to Messner's concept, in a future conflict mostly unconventional methods will be used, such as subversion, criminality and especially terrorism. There are no definite frontlines, and apparently random, seemingly unrelated acts of violence all serve a grand strategic design. The objective of this form of war is to break the enemy's fighting morale, or shatter the political support and legitimacy the enemy is relying on. Regarding the actors of *myatezhvoina*, Messner suggested to rely on mobilized masses, i.e. on agitated civilians, who stage protests, and organize strikes and unrest, as well as on covert special forces and resistance movements, i.e. on typical irregular formations, while regular military would have only a marginal role to play.[lix]

Mobilizing masses to achieve political objectives is reflected also in Russia's contemporary military doctrine. The 2014 document specifically mentions in the description of contemporary armed conflicts[lx] that the adversary may rely on the protest potential of the population. While the Russian military doctrine describes this phenomenon as something that the enemy may use, it indeed indicates that the idea is well present in contemporary Russian military thinking.

Inciting ethnic tensions in Ukraine

Since the beginning of the war in Ukraine there have been a number of cases, when Russia employed methods of terrorism and violence in order to incite ethnic tensions within Ukraine. There have been many attacks of vandalism against Polish graves in Ukraine and Ukrainian graves in Poland, which fueled nationalist on both sides in certain elements of the two societies. Meanwhile, officials on both sides repeatedly warn that attacks against such symbolic targets, as cemeteries and monuments serve Russia's interests.[lxi]

Another prominent case is of the one of Ukraine-Hungary relations. In February 2018 there was an arson attack against the cultural center of the Hungarian minority in Ukraine's Zakarpattya region, in the city of Uzhgorod. The attack was conducted at night, so no one got injured, but the building sustained considerable damage. Both the Hungarian government, as well as Russia's propaganda channels were quick to blame Ukraine's radical nationalists for the attacks. However, the Polish investigation and trial revealed in 2019 that the attack was perpetrated by two Polish far-right activists, who were hired by a German journalist, Manuel Ochsenreiter, who has strong links to Russia. Their task was to make a false flag operation, with the objective of further worsening Hungary-Ukraine relations,[lxii] which has already been tense due to Ukraine's minority-related regulations. While the attack was never clearly attributed to Russia, it indeed served Moscow's interests. In addition to the Uzhgorod arson attack, there have also been a number of other, better attributed cases, where Russia intended to fuel ethnic hatred between Ukrainians and Hungarians in Ukraine.[lxiii] Developments of Ukraine-Hungary relations have a clear relevance for NATO as well, because due to Ukraine's regulations of minority and language rights, the Hungarian government keeps blocking high-level relations between Kyiv and NATO.

The Blackfist

Ukraine is not the only country, where Russia has tried to incite ethnic tensions. While a marginal operation on its own that largely went unnoticed, the case of the Blackfist is worthy of closer scrutiny as it provides useful insight into how Russia would stir up racial tensions in the U.S. Russia's Internet Research Agency paid for personal trainers in the United States from New York to Florida from early 2017 for holding free self-defense classes for African Americans, as part of a project called Blackfist.[lxiv] The Russian trolls suggested a connection between Blackfist and the Black Lives Matter movement and collected information of the participants through the trainers.[lxv] The Russian curators asked the trainers to document the trainings with photos and videos, likely to use the material later to provoke white supremacist groups. The turnout of the trainings was relatively low, however, the modus operandi is indicative of how Moscow would deepen the division within an already divided U.S. society even further.

The use of martial arts as a cover has not been limited to the United States. In 2017 EU-Observer reported that there have been more than sixty fight arts club set up in Germany, in which the

Russian fighting style *Sistema* is taught. *Sistema* is one of the close combat systems used by Russia's special services, and these clubs serve as bases for recruiting potential fifth column operatives for Russia's military intelligence, the GRU. [lxvi]

"American soldier" shooting at Quran

There is also at least one case, when Russia was trying to incite religion-related tensions. In a video that is likely a work of the Russian Internet Research Agency, a man in a U.S. uniform is shooting at the Quran to demonstrate the inaccuracy of an allegedly captured Russian Saiga 410 rifle.[lxvii] The fake video is a poorly made one, the soldier swearing in a fake-sounding African American accent. However, taking into account that previous (real) cases when American soldiers were indeed burning copies of the Quran incited several-day-long protests and havoc throughout Afghanistan with multiple deaths, such disinformation activities could result in severe consequences.[lxviii] This is especially so, when they are more realistic, which will be easier and cheaper to achieve as deep-fake technology will become more developed and available.

As the above examples illustrate, Russia is actively experimenting with the exploitation of social, ethnic and religious divisions not only in wartime but peacetime, too. Such actions either serve limited political goals, or support the long-term objective to weaken the West. It is reasonable to assume that in case of a conventional war perceived to be unavoidable, Russian active measures to stir up social tensions in the adversary state would significantly increase. So far, Russian actions of this sort mostly targeted properties and not individuals. However, in case of a threat of war it is likely that active measures would manifest themselves in more violent attacks against individuals or groups of people too. The perception that the West uses the same means extensively against Russia and others legitimizes these actions in Moscow's eyes. Russia's national security strategy states that "[d]estructive forces outside and inside of the country undertake attempts to exploit objective socio-economic difficulties in the Russian Federation for the goals of stimulation of negative social processes, exacerbation of interethnic and interreligious conflicts, manipulation in the information sphere."[lxix] Information weapons that enable the manipulation of the society are increasingly regarded by Russia a strategic nonnuclear weapon.[lxx]

Unintended scenarios and unforeseen side effects

While assessing, how a peer-to-peer competitor might employ tools of terrorism in a full-scale conventional war, one also needs to take into account that in some cases enemy actions may

have unintended consequences, and effects of these moves may differ fundamentally from the originally intended outcomes. Unintended consequences may occur due to plain miscalculations, composed mostly of underestimating the reactions of the other side to the given attack.

These situations may not necessarily help NATO to counter actions of the adversary; however, in some cases they might be helpful in raising overall awareness about a given form of threat. In other cases, they might provide NATO with the political and operational opportunity to downgrade the adversary's capabilities in response to an attack.

The case of MH17

While not an example of terrorism, the tragedy of a civilian airlines flight provides some important lessons for what risks the extensive use of proxies holds within itself. The downing of the Malaysia Airlines MH17 flight on 17 July 2014 was a tragic incident of the war in Ukraine, claiming the lives of all 298 people on board of the airliner. As of 2021 it is already clearly proven that the Boeing was shut down by an air defense missile that was launched from a Buk surface-to-air missile system, equipped with a 9N314M warhead.[lxxi] The Buk launcher, together with several other systems, was provided by Russia, in order to improve the protection of the separatist forces against Ukrainian air force.[lxxii] On the one hand, during July 2014 Ukraine's air forces suffered heavy losses from the Russia-provided air defense weapons; Ukrainian jets and attack helicopters got practically denied from the airspace of the separatist territories, so the primary objective of the Russian operation to empower the separatists with capable air defense was indeed reached.

On the other hand, however, the unintended[lxxiii] downing of the MH17 resulted in massive, unforeseen consequences. The European Union and the United States adopted a series of sanctions (more powerful ones than the measures adopted after the annexation of the Crimea, including financial restrictions[lxxiv]), and the 298 innocent deaths, combined with massive media publicity delivered a strong PR-blow to the whole separatist movement and also to Russia behind it. From this perspective, the tragedy of the Malaysia Airlines flight provided the necessary political impetus for the adoption of powerful sanctions against Russia for the first time.

The case of MH17 showed, that the use of proxies would not necessarily insulate their donors from repercussions. It also illustrated that while deniability is a great advantage of (and a major incentive for) using proxies, the lack of full control over them increases friction in war. This observation by Russian military thinker, Aleksandr Bartosh sounds all too familiar in the context of the tragic accident of MH17.[lxxv]

The Skripal-case

The unsuccessful Russian attempt on the life of former GRU officer Sergei Skripal and his daughter, Yulia on 4 March 2018 fits into the pattern of an act of state terrorism (a targeted killing) producing unforeseen, unwanted side effects. From Russia's perspective the operation went wrong in almost all possible ways. The targets survived the attack, while the Novichok nerve agent got exposed and identified. The two perpetrators, GRU officers Alexander Mishkin and Anatoly Chepiga got identified by the Bellingcat investigative website.[lxxvi] Moreover, due to the careless handling of the Novichok by Mishkin and Chepiga two British civilians in Amesbury got accidentally poisoned[lxxvii], and one of them, Dawn Sturgess did not survive.

Most importantly, following the attack the United Kingdom called for solidarity actions against Russia within the EU and NATO. As a result, until the end of March altogether more than 150 Russian diplomats (in practice: most of them were intelligence operatives who worked under diplomatic cover) got expelled from EU and NATO countries. This sudden loss of human capital significantly downgraded Russia's intelligence capabilities in the West. Even though inside Russia the Skripal-attack had a serious deterrent effect on the Russian opposition elites[lxxviii], the Russian Federation still had to pay a high price for it. Retrospectively, the Skripal-case provided NATO and EU countries with the opportunity to deliver a serious blow to Russia's HUMINT capabilities, because the attack made it possible to build up the necessary domestic political support.

The case of NotPetya

Risk for unintended escalation is nowhere as apparent as in the cyber space. In a domain that lacks physical boundaries transcending over nation states, it is difficult to cause significant harms without collateral damage, or even risking a major blowback. In Russia's ongoing hybrid war against Ukraine, Kyiv has become a test ground for some of the most potent cyber tools in the world. By 2016, Ukraine has seen two major cyberattacks against its electric grid – leaving

225 000 people without electricity for a few hours in 2015 – and 6,500 smaller scale attacks in just only two months in 2016.[lxxix] In June 2017 however, Ukraine was targeted by a cyberattack that has quickly escalated to be the most devastating one so far in history. The perpetrators belonging to the GRU exploited a Ukrainian accounting software, M.E.Doc – required by the state to be used by all businesses in Ukraine – to spread the malware. The malware named NotPetya by experts (due to its resemblance to the earlier ransomware *Petya*) used the penetration tool Eternal Blue, which was ironically developed by the U.S. National Security Agency and was obtained and leaked by Russian state hackers earlier that year. Unlike Petya, NotPetya was only a ransomware in appearance; payment by the victims was futile as it did not result in gaining back control over their computers. What made NotPetya so effective also caused to spread uncontrollably throughout the globe, crippling companies such as the international container shipping company Maersk. In total, the loss reached $10 billion globally. The malware has not left Russia untouched either, infecting numerous Russian companies, hitting its state oil conglomerate, Rosneft, too.[lxxx] Exact scale of the damage inflicted on Russia is unknown.

NotPetya stands in stark contrast with another Russian intelligence service, the SVR's operation of 2020. As opposed to NotPetya, the supply-chain attack infiltrating Solar-Winds' Orion software was extremely targeted and sophisticated. The hackers even built in a kill-switch to relief all those computers that were not deliberately targeted by the operation, thus decreasing the risk of detection.[lxxxi] While NotPetya intended to cause massive economic damage to Ukraine, the Solar-Winds hack was part of a cyber-intelligence operation, that aimed to hold access to the data stored on the infiltrated networks for as long as possible without being detected. While there is no rock-solid, public evidence on any causality, it is still safe to assume that developers behind the Solar-Winds hack have learned from the errors of NotPetya and made it sure that the software does not backfire in a way like NotPetya did.

IV. Conclusions

Mapping out, how a peer-to-peer competitor is likely to act in case of a full-scale conventional war is a methodologically uneasy task. There is hardly any primary, publicly available official source one could rely on. The relevant plans understandably constitute well-guarded state secrets, not only in Russia, but in other countries too. Moreover, the adversary may even spread deliberate disinformation about its plans, actions, and readiness to act in order to disorient, confuse and possibly deter the other side.

However, regardless of this secrecy, it is still possible to draw certain conclusions on how Russia may use tools of terrorism in times of a conventional war by combining the studying of Soviet and Russian theoretical literature on the subject, Russia's history of employing terrorism in earlier armed conflicts, as well as the lessons learnt from the ongoing war in Ukraine. The latter is the sole ongoing, high-intensity, interstate military conflict that Russia is currently engaged in, thus it deserves special attention, while mapping out the ways Russia may use methods of terrorism in a large-scale, conventional war.

However, it is important to note that what Russia has been doing in Ukraine is probably an indicative, lower threshold of Moscow's capabilities of using means of terrorism, not the full spectrum of those. The reason is that while for Ukraine the war against Russia is a struggle that may threaten the very existence of the Ukrainian state and already damaged its territorial integrity, for Russia it is only a conflict of limited scale and intensity, which has only very small effects on the Federation as a whole. Hence, using the Ukraine conflict as a possible analogy for Russia's likely actions of terrorism needs to be done while this particularity in mind.

Based on these, one needs to realize that in case of a conventional war against the West it is unlikely that Russia would make much distinction between the front zone and the hinterland, or between the means used to attack military and civilian targets. Instead, Russia would probably employ a fully holistic approach and try to hit all such targets that it deems necessary to break the enemy's ability to resist, regardless of whether they are military or civilian ones. Besides, in order to counter-balance the technological and economic superiority of the West, Moscow is likely to employ a wide range of asymmetric tools and means. This is implied by Russia's announced strategy of active defense that would complement traditional defensive operations with a complex set of preemptive actions.

Using, among other means, methods of terrorism is perfectly aligned with this logic. This is particularly so, because in Russian military theory the use of terrorism constitutes such an integral part of warfighting that there is even a special term for it. The expression *mezhgosudarstvenniy terrorizm* (inter-state terrorism) means that a country uses methods of terrorism in its war against another country. In inter-state terrorism the secret services of the aggressor country play a key role, as attacks are both prepared and conducted by them, either directly, or via various proxies they employ. Using secret services to conduct acts of terrorism abroad is something Russia has excelled in the post-Soviet era, and particularly in the last two decades. Russian services have been involved in killing dissidents and exiled enemies of the Russian state abroad, conducting sabotage actions, inciting ethnic hatred by organizing false flag attacks, and in several hacking incidents also.

Hence, should an all-out armed conflict break out between the NATO and its peer competitor, the Russian Federation, Western decision-makers need to be aware of the fact that targeting the enemy's political and military leadership, sabotaging its critical civilian and military infrastructure, creating chaos and political instability by terrorist attacks, inciting ethnic or religious hatred, as well as using disruptive cyber operations are most probably all integral parts of Moscow's military plans prepared for such scenarios.

One may divide the possible forms of attack into two main categories along their complexity and likely effects. The first group consist of paralyzing/decapitating attacks, composed of small-scale, non-attributable strikes against hard, protected targets (critical infrastructure, key members of the administration, military leaders, C2 elements, etc.) conducted by secret services. This requires small, but highly professional individuals or teams. The aim of such strikes is to achieve the short-term paralyzation of the adversary.

The second group consists of large-scale, hybrid activities against systemic elements of the enemy's society. Actions may include targeting minority groups and vulnerable social actors, inciting internal tensions, possibly inducing unrest and violence. These bind down massive law enforcement capabilities of the adversary and divert its political attention. Such attacks require larger networks, as well as internal proxies. The aim is to generate large-scale destabilization, and thereby decrease the adversary's potential to act, limiting its available resources, as well as possibly debilitating its state functions in specific locations. It is important to note that while the two main categories of attacks can be conducted also parallel, if the adversary intends to employ an escalation dominance logic, it is more likely that it would employ the two forms of

attacks in a sequenced way, depending on the exact objectives it intends to achieve. All the more so, as asymmetric means are regarded as nonnuclear ways of deterrence, which apparently has a prominent place in Russian military strategy. Therefore, their sequenced and tailored application, including the use of terrorism, could likely constitute a form of coercion and deterrence during a conventional war.

Regarding the overall scale of probable terrorist attacks conducted by a peer-to-peer competitor, it is important to realize that while it is possible to map out certain likely forms of attacks, the overall, combined intensity of such strikes is hard to fathom. All the rogue behavior and the various acts of terrorism the West has already seen from Russia took place in peacetime. Even the conflict in Ukraine is not something that would require Russia to use its full power. With other words: no one has ever seen post-Soviet Russia fighting a high-intensity, peer-to-peer conventional war. Hence, the only safe assumption to make is that the scale and intensity of terrorist activities from Russia in case of an all-out war would considerably exceed anything that the West has seen so far.

All in all, in case of a full-scale conventional war, NATO, its member countries, including both the militaries and the civilian population are highly likely to become subject of a wide variety of terrorist attacks conducted by the Alliance's peer-to-peer competitor. Hence, NATO decision-makers need to assess not only their own vulnerabilities and the ways of strengthening the Alliance's resilience against possible forms of terrorism. As in interstate terrorism the secret services of the aggressor country are to play a crucial role, a rapid and decisive degradation of the adversary's human intelligence capabilities, as well as preventively denying the adversary from deploying new assets on Alliance territory should constitute parts of the ways of prevention and damage control. However, countering the threat of terrorism originating from a peer-to-peer competitor is beyond the focus of the current study. Nevertheless, it is important to realize the essential importance of assessing these possibilities in detail, because the threat is very real, and the likely intensity is much higher than the West has ever experienced.

List of abbreviations

EU	European Union
FSB	Federal Security Service (Russia)
GRU	Main Intelligence Directorate (Russia)
HUMINT	human intelligence
KGB	Committee for State Security (Soviet Union)
NATO	North-Atlantic Treaty Organization

Bibliography

[i] https://www.nato.int/cps/en/natohq/topics_77646.htm
[ii] https://www.nato.int/cps/en/natohq/news_185000.htm
[iii] REVIEW AND UPDATE OF MC 0472/1 - MILITARY COMMITTEE CONCEPT FOR COUNTER-TERRORISM, 21 August 2020.
[iv] https://www.jcs.mil/Portals/36/Documents/Doctrine/Other_Pubs/aap6.pdf 2-T-5.
[v] ibid, 2-A-17
[vi] ibid, 2-C-17
[vii] REVIEW AND UPDATE OF MC 0472/1 - MILITARY COMMITTEE CONCEPT FOR COUNTER-TERRORISM, 21 August 2020., p.4.
[viii] https://www.nato.int/cps/en/natolive/topics_50090.htm
[ix] https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en
[x] Timothy Thomas, *Russian Military Thought: Concepts and Elements,* MITRE, 2019 August, p. 9-8
[xi] Charles Bartles, "Russia's Indirect and Asymmetric Methods as a Response to the New Western Way of War", *Special Operations Journal,* 2, 2016, p. 4
[xii] A. V. Kartapolov, "Уроки военных конфликтов, перспективы развития средств и способов их ведения. Прямые и непрямые действия в современных международных конфликтах" (Lessons of Military Conflicts, Prospects of Development of Means and Methods of Administering Them, Direct and Indirect Action in Contemporary International Conflicts), *Voennaya Misl' (Military Thought)*, No. 2 (51) 2015
[xiii] A. Selivanov, S. Chvarkov, "Методологический подход к определению асимметричного конфликта" (Methodological Approach for the Definition of Asymmetric Conflict), NVO, https://nvo.ng.ru/realty/2020-03-27/1_1087_methodology.html March 27, 2020
[xiv] S. G. Chekinov, S. A. Bogdanov, "Asymmetrical Actions to Maintain Russia's Military Security," *Military Thought,* No. 1. 2010
[xv] A. V. Glebov, O. Yu. Mikheev, V. M. Oleinik, "От воздушной обороны – к системе комплексной борьбы с воздушно-космическим противником" (From the Air Defense System to the Complex System of the Fight with Air-Space Enemy), Vestnik Akademii Voyennih Nauk (Journal of the Academy of Military Science), No. 4 (57) 2016
[xvi] A. Bartosh, "Гибридная война – переход от неудач к победе" (Hybrid War – Transition from failure to victory"), NVO, https://nvo.ng.ru/realty/2018-06-01/1_998_hybryd.html, June 1, 2018
[xvii] Thomas, 2019, p. 9-2
[xviii] V. Putin, "Быть сильными: гарантии национальной безопасности для России", RG, https://rg.ru/2012/02/20/putin-armiya.html, February 20, 2012
[xix] P. Doulnev, V. Orlyansky, "Основные изменения в характере вооруженной борьбы первой трети XXI века" (Basic Changes in the Armed Struggle Character of First Third of the XXI-st Century), *Vestnik Akademii Voyennih Nauk (Journal of the Academy of Military Science),* No. 1 (50) 2015 p. 45
[xx] V. Kiselyev, "К каким войнам необходимо готовить Вооруженные Силы России" (What Wars the Russian Armed Forces Should Prepare For), *Voennaya Misl' (Military Thought),* 2017
[xxi] Selivanov, Chvarkov, 2020
[xxii] A. Bartosh, "Гибридная война – новый вызов национальной безопасности России" (Hybrid War – New challenge for Russia's national security), *Национальная Оборона*, https://2009-2020.oborona.ru/includes/periodics/maintheme/2017/1016/154222573/detail.shtml 2017
[xxiii] Military Dictionary, Ministry of Defense of the Russian Federation, http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=10967@morfDictionary
[xxiv]
[xxv] Rogozin, p. 26.
[xxvi]
https://books.google.hu/books/about/%D0%A2%D0%B5%D1%80%D1%80%D0%BE%D1%80_%D1%82%D0%B5%D1%80%D1%80%D0%BE%D1%80%D0%B8%D0%B7%D0%BC_%D0%B8_%D0%BF%D1%80.html?id=YAe-AgAACAAJ&redir_esc=y
[xxvii] Dukaev, ibid.
[xxviii] https://www.amazon.com/Sword-Shield-Mitrokhin-Archive-History/dp/0465003125
[xxix] http://commdocs.house.gov/committees/security/has299010.000/has299010_0f.htm
[xxx] Spy Handler, p. 168.
[xxxi] https://www.tandfonline.com/doi/full/10.1080/00396338.2014.985432

[xxxii] Stanislav Lunev. Through the Eyes of the Enemy: The Autobiography of Stanislav Lunev, Regnery Publishing, Inc., 1998.
[xxxiii] Biological Espionage: Special Operations of the Soviet and Russian Foreign Intelligence Services in the West
[xxxiv] https://web.archive.org/web/20050425151231/http://www.calitreview.com/Interviews/int_kouzminov_8013.htm
[xxxv] Putin first served as Prime Minister of the Russian Federation from 9 August 1999 until 7 May 2000, when he was sworn in as President.
[xxxvi] https://libertypublishinghouse.com/shop/english-language/blowing-up-russia-terror-from-within-english/
[xxxvii] https://web.archive.org/web/20070926015902/http://www.wilsoncenter.org/topics/pubs/WP51_Web_Final.pdf
[xxxviii] https://www.bellingcat.com/news/uk-and-europe/2018/11/22/second-gru-officer-indicted-montenegro-coup-unmasked/
[xxxix] https://fas.org/sgp/crs/intel/R46616.pdf , p.11.
[xl] Lunev: Through the Eyes of the Enemy
[xli] Glebov, Mikheev, Oleinik, 2016, p. 59
[xlii] "Векторы развития военной стратегии", Krasnaya Zvezda, http://redstar.ru/vektory-razvitiya-voennoj-strategii/, March 4, 2019
[xliii] http://news.bbc.co.uk/2/hi/europe/6188658.stm
[xliv] https://www.bbc.com/news/world-europe-50659179
[xlv] https://www.amazon.com/Skripal-Files-Life-Death-Russian/dp/1250207738
[xlvi] https://euobserver.com/foreign/150486
[xlvii] https://www.nytimes.com/2021/04/24/world/europe/arms-merchant-russia-assassination-squad.html
[xlviii] https://www.bbc.com/news/world-europe-27891018
[xlix] https://www.nbcnews.com/tech/security/colonial-pipeline-hack-claimed-russian-group-darkside-spurs-emergency-rcna878
[l] https://www.euractiv.com/section/digital/news/ukraine-says-russian-cyber-attacks-targeted-its-main-airport/
[li] https://techmonitor.ai/techonology/cybersecurity/chaos-ukraine-ransomware-cyber-attack-hits-airports-banks-government
[lii] https://www.bbc.com/news/world-europe-28191833
[liii] https://www.voanews.com/europe/bridges-donetsk-destroyed-ukraine-battles-separatists
[liv] "How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine", Bellingcat, https://www.bellingcat.com/news/uk-and-europe/2021/04/26/how-gru-sabotage-and-assassination-operations-in-czechia-and-bulgaria-sought-to-undermine-ukraine/, April 26, 2021
[lv] "Senior GRU Leader Directly Involved With Czech Arms Depot Explosion", Bellingcat, https://www.bellingcat.com/news/2021/04/20/senior-gru-leader-directly-involved-with-czech-arms-depot-explosion/, April 20, 2021
[lvi] "The Dreadful Eight: GRU's Unit 29155 and the 2015 Poisoning of Emilian Gebrev", Bellingcat, https://www.bellingcat.com/news/uk-and-europe/2019/11/23/the-dreadful-eight-grus-unit-29155-and-the-2015-poisoning-of-emilian-gebrev/, November 23, 2019
[lvii] Adam Klus, "Myatezh Voina: The Russian Grandfather of Western Hybrid Warfare", Small Wars Journal, https://smallwarsjournal.com/jrnl/art/myatezh-voina-the-russian-grandfather-of-western-hybrid-warfare
[lviii] Quoted in detail by Ofer. Fridman: "Hybrid Warfare or Gibridnaya Voyna? Similar, But Different," The RUSI Journal, Vol. 162 – 2017, Issue 1, p. 43-45.
https://www.tandfonline.com/doi/pdf/10.1080/03071847.2016.1253370?needAccess=true
[lix] In a more details form, see:
http://www.coedat.nato.int/publication/reports/COE%20DAT_study_on_the_role_of_irregular_forces_in_Russia_hybrid_warfare_final.pdf p. 12.
[lx] https://rusemb.org.uk/press/2029 Point 15/a).
[lxi] https://www.irishtimes.com/news/world/europe/history-wars-strain-ukraine-poland-relations-again-1.3279262
[lxii] https://www.theguardian.com/world/2019/jan/27/polish-far-right-trial-raises-spectre-of-false-flag-tactics-german-journalist-russia-ukraine-fire-court
[lxiii] See, for example, see these two cases, when anti-Hungarian posters were put up in Zakarpattya: https://hungarytoday.hu/new-attacks-have-occurred-against-the-hungarian-community-in-ukraine/ and https://ssu.gov.ua/novyny/sbu-vykryla-zlochyntsiv-yaki-poshyriuvaly-antyuhorski-lystivky-na-zakarpatti?fbclid=IwAR3xzdKdUMX8iyZMiDk65e9jlSWjkbP3miNUhoYS9lPKyjM8Kr3PqATcg8Q The incorrect use of Ukrainian language in both cases probably indicates that the perpetrators were not Ukrainian nationalists. In the second case Ukrainian authorities managed to apprehend the suspects, who were from Eastern Ukraine and were hired by an individual from Russia.

[lxiv] "In attempt to sow fear, Russian trolls paid for self-defense classes for African Americans", CNN, https://money.cnn.com/2017/10/18/media/black-fist-russia-self-defense-classes/index.html, October 18, 2017
[lxv] "Расследование РБК: как «фабрика троллей» поработала на выборах в США" (Investigation of the RBK: how the "troll factory" operated during the US elections), RBK, https://www.rbc.ru/magazine/2017/11/59e0c17d9a79470e05a9e6c1, October 17, 2017

[lxvi] Andrew Rettman, „Fight club: Russian spies seek EU recruits", EU-Observer, https://euobserver.com/foreign/137990, May 23, 2017,
[lxvii] "'I'm going to shoot this mother****er': Shock footage of a 'US soldier' blasting the Koran with a machine gun is FAKED by Vladimir Putin's anti-West 'troll factory'", Daily Mail, https://www.dailymail.co.uk/news/article-3515146/I-m-going-shoot-mother-er-Shock-footage-soldier-blasting-Koran-machine-gun-FAKED-Valdimir-Putin-s-anti-America-troll-factory.html, March 30, 2016
[lxviii] "Qur'an burning protests: two US soldiers shot dead by Afghan colleague", The Guardian, https://www.theguardian.com/world/2012/feb/23/quran-burning-afghanistan-us-soldiers-dead, February 23, 2012
[lxix] "Указ Президента Российской Федерации О Стратегии национальной безопасности Российской Федерации", http://publication.pravo.gov.ru/Document/View/0001202107030001, July 2, 2021, p. 15
[lxx] Timothy Thomas, "Information Weapons: Russia's Nonnuclear Strategic Weapons of Choice", *The Cyber Defense Review,* 2020 Summer
[lxxi] https://www.onderzoeksraad.nl/en/media/attachment/2018/7/10/debcd724fe7breport_mh17_crash.pdf p. 131-135.
[lxxii] https://www.bellingcat.com/news/uk-and-europe/2019/06/19/identifying-the-separatists-linked-to-the-downing-of-mh17/
[lxxiii] The first messages
[lxxiv] https://www.consilium.europa.eu/en/meetings/fac/2014/07/22/
[lxxv] Krisztián Jójárt, "Revising the Theory of Hybrid War. Lessons from Ukraine", Center for European Policy Analysis, https://cepa.org/cepa_files/2019-04-Revising_the_Theory_of_Hybrid_War.pdf, April 2019
[lxxvi] https://www.rferl.org/a/bellingcat-second-novichok-suspect-also-honored-by-putin-as-hero-of-russia-/29534185.html
[lxxvii] https://www.bbc.com/news/uk-england-wiltshire-44707052
[lxxviii] Interview with competent Russian sociologist, Moscow, May 2019.
[lxxix] David Sanger, *The Perfect Weapon. War, Sabotage, and Fear in the Cyber Age.* Crown, New York, 2018, p. 192
[lxxx] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", WIRED, www.wired.com%2Fstory%2Fnotpetya-cyberattack-ukraine-russia-code-crashed-the-world%2F&usg=AOvVaw1YiR1jhe17pTyF5vQu4VR5, August 22, 2018
[lxxxi] "Evolution of Russian Cyber Tactics and Operations", https://www.csis.org/events/evolution-russian-cyber-tactics-and-operations, March 25, 2021


COE-DAT