Croatian International Relations Review
—
CIRR
—
XXIV (83) 2018, 34-51
—
DOI 10.2478/ cirr-2018-0013
—
UDC 355.01:323.282

Understanding Contemporary Asymmetric Threats

Nikola Brzica

Faculty of Political Sciences, University of Zagreb, Croatia

nikola.brzica@gmail.com

ORCID: http://orcid.org/0000-0001-9475-1793

Key words: *asymmetric warfare; unconventional warfare; terrorism; insurgency; asymmetry*

Abstract

In the 21st century, warfare has evolved into a challenge that many countries are ill prepared to face. In contrast to the warfare of yesterday, victory is not defined by defeating an opposing military force, but rather defeating their ability to pursue political objectives by violent, often unconventional, means. Increasingly, these unconventional means are based on asymmetries between the two opposing forces.

A plethora of definitions for the term 'asymmetric conflict' exist, but they can largely be summarized by a general idea that one side in a conflict, due to its own failings or its opponents' strength, is unable to achieve its political aims through conventional (i.e. symmetric) military means. Because of this, the weaker side uses new ideas, weapons and tactics in a manner that is not expected, exploiting surprise to undermine the relative strength(s) of their opponent (Lele, 2014). The character of contemporary asymmetric threats can be analyzed through a framework of several key characteristics, which will be described in this paper. Understanding this framework, particularly in light of the horizontal transfer of technology, tactics, organization structure and procedures between emerging asymmetric threats may contribute to better understanding of such threats.

Introduction

Developments since the end of the Cold War, especially in the peripheral areas of competition of the previously opposed ideological blocs, as well as the increasingly common manifestation of difficult to predict asymmetric threats have fundamentally changed the global security environment. This change has, in turn, defined a need for analysis driven strategies and policies which will effectively counter these emerging security threats. Accordingly, an objective evaluation of existing strategies and policies is necessary, as well as the development of new ones (Katzman and Thomas 2017: 26). Perhaps the best illustrations of the complexity of these ongoing cyclical processes of interdisciplinary analysis, strategy and policy development, followed by their final implementation in the area of operations are visible in the international counterinsurgency efforts in Afghanistan. Specifically, despite the fact that the international military presence in Afghanistan is entering its 17th year, the lack of decisive results indicates that the approach taken by the international community (and more specifically NATO) to address this security challenge has not been entirely effective. However, the wealth of strategic and operational insight resulting from the most significant multinational military operation of the 21st century (in terms of duration, lives lost and resources expended), may hold valuable lessons that may be applicable to other forms of asymmetric threats.

It is important to note that as of the writing of this article, contemporary wisdom regarding asymmetric threats has already been significantly influenced by multinational experiences in Afghanistan. Namely, contemporary approaches to asymmetric threats stress the need for unity of effort in a multinational context, as well as the careful application of significant diplomatic, intelligence, military and economic resources based on a high level of understanding of the historical and cultural context of the specific threat. Remarkably, this type of analysis (and consequent strategic approach) marked a significant departure from the early counterinsurgent efforts in Afghanistan, which were best characterized as shoring up local proxy forces (governmental or non-governmental), which were often of dubious quality and legitimacy.[1] Under pressure from a deteriorating security environment, however, counterinsurgent efforts in Afghanistan adapted and evolved to include complex interdisciplinary analysis that sought to better understand and evaluate the conduct of the counterinsurgency, and these efforts characterized the Anti-Taliban Military efforts from 2003-2009 in large measure. Thus, analysis driven strategy and policy was recognizable throughout the end of the NATO ISAF (International Security Assistance Force) mission in 2014, and has continued in the still operational Resolute Support Mission that started in 2015 (Katzman and Thomas 2017).

Recognizing the importance of understanding the historical and cultural context of emerging threats, NATO itself implemented joint multidimensional analysis of the operational environment into its doctrine in 2011, and first applied this form of comprehensive analysis during the initial attempts to find a solution to the then-raging Libyan conflict (Sokolsky 2017). Despite significant differences between the conflicts in Libya and Afghanistan, NATO's joint multidimensional analysis of the operational environment in Libya, which was based largely on experiences in Afghanistan, facilitated a better understanding of the specific regional context and implications of a potential intervention. This understanding encompassed important dynamics such as specific national legislation, tribal codes, religious structures and their influence, as well as local socioeconomic conditions (Dawoody 2016:169). Consequently, we can ascertain that insight resulting from years of experience in Afghanistan was applicable in unrelated and dissimilar unconventional asymmetric challenges. Moreover, in the period to come, the strategic and operational insights gained in Afghanistan may yet shed light on contemporary and future unconventional threats such as violent extremism, terrorism, insurgencies, or information warfare, and may hold the key to their timely and effective mitigation.

[1] Contemporary asymmetric military operations increasingly make use of traning and mentoring forces for host nation forces, which has previouly not been the case.

A brief overview of contemporary threats

Globalization, international agreements and economic benefits have influenced the development of a relatively stable and peaceful international environment for a majority of developed nations (Harris 2010). In the contemporary world, nation states have professional militaries and capable intelligence agencies, and are not overly concerned by the prospect of conventional invasion from their neighbouring states. In contrast with historical experience, it seems that in the 21st century, the main security threats are posed by non-attributable hostile acts by aggressive nation states, as well as violence perpetrated by extremists, terrorists and organized crime (non-state actors). These actors share a common characteristic in that they do not fall within established territorial and legislative boundaries (Rynegeart 2017: 156). Furthermore, these type of actors initiate conflicts and utilize unconventional tactics to achieve their political or other aims (Hartley 2017: 21). Some of the most common manifestations of these asymmetric threats in the past twenty years have been violent extremism, terrorism and insurgency, proliferation of weapons of mass destruction (WMD) and information warfare.

Violent extremism has been manifested through over 235 terror incidents around the world since November 2016. These attacks have left 2030 dead and 2348 injured (CACI International 2017). At the same time, the Islamic State (IS), Al Qaeda and other radical Jihadist organizations continue to spread their radical ideology and attempt to radicalize and induce followers to commit acts of terror (Shuck 2015: 2).

In light of these figures, terrorism is perhaps the manifestation of asymmetric threat that has garnered the most attention. It involves the calculated use of force with an aim of inspiring terror in order to coerce a government or society into adopting political, religious or ideological objectives. Terrorism and terrorist threats have changed dramatically in the last 15 years, primarily because of evolving terrorist motivations, the rise of information technology and the corresponding ease with which information is disseminated, the accelerating urban centralization of vital components of national infrastructure, as well as the proliferation of WMD technology (Smit 2017).

Insurgency, one of the forms of asymmetric conflict, is defined as an organized political and military revolt which has a goal of weakening or overthrowing a government or other political authority, with the complementary aim of increasing one's own control over a population (Black 2016). In contrast, counterinsurgency is defined as the combined political, economic, social and security measures which are taken to prevent and/or defeat armed violence, as well as to establish stable political, economic, social and security structures, as well as to address the fundamental causes of the insurgency, with an ultimate aim of establishing and defending stability in a given area (Hampsey 2010).

Weapons of mass destruction are weapons which can kill large numbers of people and cause catastrophic damage to cities, countries, nature and the biosphere, and are most commonly categorized as nuclear (to include 'dirty bombs'), biological and/or chemical agents (Hayoun and Goldstein 2017). In addition to traditional state actors, who have sought to acquire such weapons as a means of punching above their weight in local or regional international relations or as a means of guaranteeing the survival of their regime (i.e. Sadaam Hussein in Iraq, Moamar Ghaddafi in Libya), various non-state actors have increasingly undertaken efforts to acquire WMD's (i.e. Osama bin Laden first stated that his 'Islamic Duty' was to acquire WMD in 1998, then repeated his threat to use them in a 2007 video). Many consider a possibility of WMDs in the hands of these non-state actors as a particularly dangerous development, as the difficulty of attributing a WMD attack conducted by such an actor to the actual perpetrator might encourage their operational use.

Information warfare encompasses any activity directed against the information and value system of a targeted country, organization or group of people. Information warfare involves the use of superior methods of information development (from raw or unprocessed data) and decision making based on true (or better) understanding. This type of warfare has been developed by technologically advanced societies and militaries in order to undermine opponents' abilities to develop understanding from information. Generally speaking, information warfare operations can be used most effectively against opponents who are similarly technologically advanced, and enables its practitioners to achieve objectives remotely without the need for direct exposure and identification. Today, the Islamic State uses offensive information warfare to attack not only military targets, but civilian ones, too. In its eyes, there is no such thing as civilian status beyond the caliphate's boundaries (Frampton at al 2017: 31). Thus, media weapons are calibrated with a view to attacking disengaged publics as much as they are geared towards hitting engaged militaries (Winter 2017: 18).

Conventional vs. asymmetric conflicts

As Clausewitz famously wrote, war is the continuation of politics. Consequently, political conflict is the basis for all conflict, to include terrorism and insurgent asymmetric conflicts, especially as both terrorists and insurgents base their legitimacy and power on the support that they enjoy in the populace that they claim to represent. This central premise has traditionally been the main factor guiding the conduct of insurgent operations in contrast to conventional warfare and its focus on traditional military targets. Thus, it can be said that contemporary manifestations of asymmetric warfare have had pronounced socio-political significance, as opposed to specific social, economic or military benefits (Huba 2006). Fredholm stated that conflicts occur for personal, ideological or economic reasons, or a combination of these factors, yet the acquisition of power tends to be paramount as motive (Fredholm 2017: 7).

In conventional warfare, military action, supported by diplomacy, information operations and economic pressure, is the primary mechanism for achieving the end goal. Politics as a mechanism for objective realization dominates during the planning and preparation of conflicts, but becomes secondary during the conflict itself. In other words, politics in a conventional conflict is not dominant during the conduct of the war, which makes it possible to delineate among various actors: the government which guides operations, the population which provides the means, and the military which uses them (Galula 1964).

The role of politics in an asymmetric conflict is significantly different. Considering that both parties in the conflict seek to influence public opinion, a political position of the two sides is primary; the insurgents seek to gain the trust and allegiance of the populace while the counterinsurgents seek to prevent the populace from falling under the influence of the insurgents. It is not enough for the government to set political objectives, to determine the necessary force required to achieve these objectives, to enter alliances, and then to monitor developments in the conflict from a distance, hoping for a positive outcome. In an asymmetric conflict, because of the particularity of the objectives and the conduct of the conflict itself, politics is an active mechanism which ensures that each military act is viewed through a prism of potential costs and potential benefits.[2] To conclude, the key to successful counterinsurgency is effective governance, because the entire conflict and its outcome is largely decided by the success of each side in gaining and maintaining credibility among the populace (Military Review, 2014: 36). Quite often, the stronger governmental opponent's primary means for achieving this credibility is the ability to govern effectively.

	Conventional conflict	**Asymmetric conflict**	
		Guerilla warfare	**Terrorism**
Size of forces	Large	Medium (platoons, squads)	Small groups (usually less than 10 people)
Weaponry	Wide assortment of military equipment, aircraft, armor, artillery	Most often light infantry weapons	Small arms, bombs, improvised explosive devices, car bombs, etc.
Tactics	Joint operations which include multiple services	Commando tactics	Specialized tactics, kidnapping, assassinations, etc.
Targets	Military targets, industrial and communications infrastructure	Mainly military targets, police, political opponents	State symbols, political opponents, the public
Objective	Physical destruction	Mainly to render the opponent incapable of action	Psychological coercion
Control of territory	Yes	Yes	No
Uniforms	Uniforms are worn	Uniforms are often worn	Uniforms are not worn
Warzone status	Warfare is limited to a recognized geographic area	Limited to a single country	No borders, operations are conducted globally
Legality according to international law	Yes, if operations are conducted in accordance with international law	Yes, if operations are conducted in accordance with international law	No

Figure 1
The characteristics of conventional and asymmetric conflicts.

[2] Cost-Benefit analysis.

Characteristics of asymmetric actors structure

The operational structure of the opposing sides in an asymmetric conflict is fundamentally different. On one side, we have a traditional military and political hierarchy which relies on the economic, political and diplomatic power of the state whose interests it defends. On the other side, we have a heterogeneously structured and heterogeneously motivated group, which often adopts a non-hierarchical structure by choice or chance to pursue a common cause. Terrorist groups adopt a non-hierarchical, cellular and/or mesh structure on purpose in order to avoid detection and make identification of their members in case of the compromise more difficult. Because of this compartmentalization, members of a terrorist cell often know only other members of the same cell, and thus are unable to divulge information concerning the identities and work of other insurgent cells when discovered and interrogated (Fredholm 2017: 32).

Another similar form of asymmetric actor structure is one based on a tribal structure such as those in Afghanistan and the tribal areas of Pakistan, which can be described as an unintentionally formed non-hierarchical structure. In these structures, groups form on the basis of existing family and tribal ties, and the penetration of such groups, or the winning over members of these groups, is extremely difficult because of a high level of distrust for strangers and the strength of the social connections between group members.

Different organizational structures (which are often modular) have allowed once local, or in the best case regional, organizations to expand their operations into an international and global environment. Technology, to include web based technologies, have enabled the rise of globally connected actors, who have the ability to act quickly and effectively anywhere in the world. The fundamental functioning of these types of organizational strucutres is very simple yet effective. Precisely because of this, they represent a significant challenge for Intelligence and Law Enforcement entities, who have struggled to develop effective strategies for countering such asymmetric opponents. Namely, the traditional approach applied to hierarchically structured opponents enabled security forces to target the inner nucleus of an organization, the center of gravity in Clausewitzian terms, which resulted in a total degradation of the organization's ability to act. In the case of asymmetric actors, the destruction of one cell does not substantially effect the ability of the organization to conduct further operations. Another problem is that individual cells may not conduct independent attacks, but rather provide resources which are amalgamated in the final stages of preparation for an attack, giving security forces a tiny window for preventative action. A key characteristic of the matrix organizational structure is that the destruction of an individual actor or leader has minimal effect on the operations of the group while at the same time contributing to the radicalization of the group's members. The Afghan Taliban example illustrates the fact that most operational coordination occurs at the tactical level, while broad ideological and strategic guidance is issued from the highest levels of leadership located in Pakistani safe havens.

A similar phenomenon is recognizable in recent attacks in Europe. Namely, attacks have been carried out at broadly dispersed geographic locations, not only under the auspices of the IS, but also of several other Jihadist groups, with little or no operational involvement from the countries of origin of such groups. This suggests that a significant decentralization in operational terrorist structures has occurred and as a result, we have progressed to the current manifestation of Islamic terrorism — reciprocally independent radicalized groups and/or individuals, who are geographically and quite often logistically autonomous, and who are able to operationalize their intent with little or no external assistance (Brzica, 2017).

Use of contemporary information and communication technologies

The Information and Communication Technology (ICT) revolution has greatly enhanced the ease of communication, financing, distribution, planning, the recruitment of new members, as well as the propaganda efforts of asymmetric actors. In fact, access to and use of ICT technologies, in addition to the security and organizational vulnerabilities of traditional hierarchical organizations outlined above, has resulted in a relative decline of hierarchically structured organizations among asymmetric actors. In ICT facilitated, matrix (or cellular) structured terrorist organizations, penetration of a single cell does not produce spectacular results because of the distributed nature and mutually independent structure of the organization, thus guaranteeing greater operational survivability. In light of these developments, in recent years the Middle East has witnessed the appearance of tech savvy "techno-terrorists" (Hartman 2002). Recent operations in Afghanistan have also exposed advanced communication techniques used by asymmetric actors who use satellite telephones, mobile phones, computers, the Internet, e-mail and other web based technologies to a surprising degree to support ongoing operations, as well as to plan future operations. Hamas also provides a textbook example of the application of new technologies by a non-state asymmetric actor. Namely, Hamas plans the majority of its operation using communications via the Internet, but also makes use of the Internet for propaganda purposes as well as for communicating with its sympathizers in remote locations, exploiting the „safe" Internet infrastructure available in Gaza, the West Bank and Lebanon. Another non-state asymmetric actor, Hezbollah, uses its websites to describe and publicize information (to include video footage) of recently conducted attacks, as well as to disseminate news and propaganda to its followers and sympathizers (Miller 2014: 82).

Intelligence and security agencies have not been inactive in responding to the security implications of ICT advances. The beginning of 2016 was marked by grandiose claims that the IS would be obliterated from cyberspace by the end of the year (Forno and Joshi, 2016). However, almost two years later, it is apparent that the presence of the Islamic State and other extremist organizations on the Internet continues to be a major problem, primarily because it enables the Jihadist network to keep including new supporters and thus to constantly evolve and expand (Frampton et al. 2017: 31). It is irrefutable that the Internet facilitates rapid spread of information to broad audiences, while also enabling quick changes between communications platforms and almost instantaneous migration from one virtual location to another. In addition, the Internet has proven to be an excellent instrument in the hands of extremist organizations for propaganda dissemination, as well as the radicalization and recruitment of new adherents (Brzica 2017).

Despite the examples outlined above, it is a mistake to link contemporary terrorist operational and financial practices exclusively to new technologies. Some terrorist organizations are quite adept at working within established technologies and highly regulated economic environments. Paramilitary groups in Northern Ireland, for example, make use of legal entities such as hotels, pubs, taxi companies and other legitimate business to launder money and finance political activities.

Financing

The acquisition of financial means and their effective and timely allocation among individual elements (cells) of a group is of utmost importance for terrorist groups. Financing activities in the area of operations directly affect the costs of operations and survival, varying in degree from group to group and location to location. In virtually all cases, planning and execution of operations, financing of personnel and operations, as well as enabling activities such as bribing and recruitment, require large amounts of money which are collected from numerous sources, which are increasingly dispersed globally.

Regarding the financing of asymmetric actors, several trends are recognizable. The first trend relates to distributed financing by radical sympathizers, with the financing of the IRA by the large Irish diaspora in the US given as one of the earliest examples. Other comparable examples include the collection of finances in support of an attempt assassination of the former Egyptian President Mubarak, when millions of dollars were transferred from the National Commercial Bank of Saudi Arabia via banks in New York and London to Al Qaeda, whereas the banks were unaware of the true purpose of these transactions (Gunarathna 2003). A second trend in the financing of asymmetric actors is the widespread adoption of measures to avoid regulatory measures intended to prevent money laundering. Most recent studies show that everyone dealing in illicit markets, from the inane copyright infringers to brutal human traffickers, can find comfort in the anonymity of cryptocurrency—especially terrorists. As Telley states, as early as 2015, ISIS was suspected of having moved funds through Bitcoin and a Salafi-jihadist group in Gaza conducted a fundraising campaign, under the title Jahezona, or “Equip us” in Arabic (Telley 2018).

Socioeconomic considerations

Sociological considerations are very important in understanding the nature of asymmetric conflict. Peter A. Olsson has developed a "personal pathway model" to describe the evolution of insurgent conflict (Cunningham 2001). According to his model, individuals who suffer a specific threat to their ethnic identity and are motivated by ethnic nationalism rather than ideology, perceive themselves to be freedom fighters. Viewed from socioeconomic and sociocultural vantage points, the number of people who consider themselves to be abandoned, demonized, exploited and subject to unfair treatment increases over time, and their dissatisfaction transforms into violence, which then becomes the primary manifestation of this dissatisfaction (Najetović 2011). A recent example of this type of behaviour are the recent „Arab Spring" revolutions which deposed numerous authoritarian dictatorships in North Africa, including the Ben Ali regime in Tunisia which was sparked by the suicide of a street vendor after he was detained and humiliated by Tunisian police officers (Stradiotto and Guo 2014: 112).

Social stratification within countries and within the international order contribute to alienation in the contemporary world (Vukasović 2009), and it is precisely because of this that certain societal groups consider their own predicaments such to induce them to undertake some form of asymmetric conflict, be it terrorism, insurgency or something else. When examining asymmetric conflicts from a sociological vantage point, it is necessary to take into account the importance of the demographic underpinnings of the conflict. This aspect is quite evident in Afghanistan, where there is a large number of unemployed young men who face a decision on whether they wish to be perceived as a 'drain' on a society already hampered by limited resources, or be perceived as a 'hero' who is fighting for the 'freedom' of his ethnic and/or religious identity (Landinfo 2017:15). This same phenomenon could be readily recognized in Northern Ireland, where the Catholic community had a traditionally high rate of demographic growth, while at the same time having a high rate of unemployment, due in no small part to institutional discrimination. As in the period when the conflict in Northern Ireland was at its peak, also nowadays a high rate of unemployed young males see membership in terrorist organizations as a reasonable option. However, it is important to mention that demographic changes in Northern Ireland may soon result in a Catholic majority, which in turn will most likely destimulate the pursuit of political objectives with violence as the very same objectives should be attainable through legal democratic means.

Some theorists believe that social bonds, most often those related to family and clan, have the biggest impact on individuals who are facing a decision on whether or not to join an asymmetric actor. In these cases, traditional methods of winning 'hearts and minds' (a fundamental tenet of population-centred counterinsurgency) have limited results considering that arguments based on economic and/or political facts do not fall on fertile ground among the members of a tribal society (Springer 2008.)

Ideology

Ideology has an enormous influence in mobilizing populations. Political ideology refers primarily to ideas about common values and promotion of political behaviour which aligns with ideals or ideas about a desired state with the suggestion of creating, mobilizing, guiding, organizing or justifying a certain type of behaviour. The term also encompasses a definition of a certain societal actor's (group, class) interests, and the efforts to publicize and achieve these interests through political processes (Ravlić 2001).

Other theorists contend that ideology is a set of beliefs and positions which justify a certain action, and they identify the functions of ideology as follows:

- Ideology polarizes and mobilizes a populace, directing them towards common goals
- Ideology creates a sense of security, providing a set of rules and values
- Ideology represents the foundation for justifying and rationalizing human behaviour (Violence and Terrorism 2004).

Ideology can thus be considered a cohesive force which serves to unify and guide realization of an ideological objective.

Keeping this in mind, we can conclude that the ideology which is able to dominate in an asymmetrical conflict offers, through radicalization of its adherents, means that a relatively weaker party can effectively counter an economically, technologically and numerically stronger adversary. Viewed from this perspective, it is quite appropriate to conclude that ideology is one of the most important factors in asymmetric conflicts. Both Osama bin Laden and Mullah Omar were on top of allied priorities in the asymmetric conflict with radical Islam, primarily because of the ideological guidance that they issued to followers and sympathizers throughout the Islamic world and beyond (Neumann 2008:55). Neither of the two issued daily operational instructions to insurgent groups, or did they direct tactical operations. However, the influence of the two individuals mentioned was unquestionable while they were alive, as the influence of the Jihadi network is today. Interestingly, in the same manner that ideology plays a prominent role in shaping insurgent strategy, it must do so in counterinsurgency strategy. Counterinsurgents must always take care to ensure that their ideology is acceptable to the population whose "hearts and minds" they seek to win over.

Conclusion

It is becoming increasingly evident that unconventional asymmetric security challenges of today, such as violent extremism, terrorism, insurgencies, or information warfare require strategic and policy measures outside the realm of conventional approaches. Unlike relatively clear-cut procedures of a conventional *state vs. state* conflicts that marked the Cold War, nation states are increasinglyconfronting non state actors, ranging from terrorist organizations to radical ideological movements. Moreover, these types of threats cannot be fought by reactive measures alone. A mitigating strategy and policy must be based on extensive interdisciplinary analysis, which take into account specific historical, cultural and other aspects of each individual challenge. Perhaps the strategic and operational insights acquired in the largest counterinsurgency operation of the 21st century, in Afghanistan, can facilitate understanding of other, seemingly unrelated and dissimilar asymmetric threats as was the case with operational planning from the Libyan intervention in 2011. In light of this, it should be noted that matrix structures can be found in a broad range of discrete and geographically distant asymmetric actors, ranging from terrorist organizations to online producers and disseminators of radical Jihadist propaganda. Likewise, the rise of ICT, particularly the rise of mobile devices and their protected communication applications, allows for the facilitation of a range of activities which can enable everything from the proliferation of WMD and planning of terrorist attacks, to radicalization and recruitment of new generations of terrorists. Additionally, ideology, whether it be radical Jihadist or Anarchist and Anti-Western, will continue to play an important role in the motivations of individual asymmetric actors, particularly among those operating on the fringes of democracy. Perhaps the most poorly understood aspect of contemporary asymmetric threats is their financing, particularly in light of recent crypto currency advances. Namely, it is quite possible that intelligence and security agencies will face significant challenges in the future in piecing together global flows of illicit funds considering what block chain technologies seem to offer: anonymity, non-traceability, truly global outreach, and near instantaneous execution of transactions. Finally, socioeconomic considerations remain a central aspect of understanding the motivations of individual asymmetric actors, ranging from the lack of available meaningful employment which may push individuals along the path to criminally or politically motivated violence to acute perceptions of political, religious and identity alienation which seem to play an increasing role in the radicalization of Jihadists originating in Western countries. One must also keep in mind that in efforts to mitigate the asymmetric threats mentioned above, democratic states are often faced with obfuscated realities and conflicting objectives which directly contradict a goal of maintaining peace and security. Finally, in light of global trends toward deregulation and integration, open borders and the global economy, it is quite possible that characteristics of asymmetric actors once limited to specific geographic areas or operational forms, may soon appear in entirely different regions and contexts.

References:

Black, J., 2016. *Insurgency and Counterinsurgency: A Global History*. Rowman and Littlefield Publishing Group: Maryland.

Brzica, N., 2017. Potential Adherents of Radical Islam in Europe: methods of Recruitment and the Age of Perpetrators in Acts of Terror. *Politička misao:* časopis za politologiju, 54(4), 161-184.

CACI International, 2017., Global Snapshot, April 2017. Available on www.asymmetricthreat.net,

Cunningham, W., 2001. *Violent Conflict in Northern Ireland: Complex Life at the Edge of Chaos*. George Mason University: Fairfax, Virginia.

Dawoody, A. R., 2016. *Eradicating Terrorism from the Middle East*. Policy and Administrative Approach. Springer International Publishing: Switzerland.

Forno, R. and Joshi, A., 2016. America is Dropping Cyberbombs-but how do they work? Available on: https://scroll.in/article/807965/america-is-dropping-cyberbombs-but-how-do-they-work [accessed 12 June 2018].

Frampton, M., Fisher A. and Prucha, N., 2017. *The New Netwar*. Policy Exchange: Westminster, London.

Fredholm, M., 2017. *Transnational Organized Crime and Jihadist Terrorism. Russian-Speaking Networks in Western Europe*. Routhledge: New York.

Galula, D., 1964. *Counterinsurgency Warefare — theory and practice*. Praeger Security International: Westport, CT.

Gunarathna, Rohan. 2003. *Inside Al Qaeda*. Berkley Books: New York.

Hampsey, R., 2010. Rediscovering the Art of Psychological Operations in the Afghan Counterinsurgency. *Small Wars Journal*.

Harris, M., 2010. The use oft he Security Professionals in Counterinsurgency Operations. Available on: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA480183

Hartley, D., 2017. Descriptions of Unconventional Conflict. In: Unconventional Conflict. Understanding Complex Systems. Springer: Cham.

Hartman, W., 2002. *Globalization and Asymmetrical Warfare*. US Army. Maxwell Air Force Base, Alabama. Available on: www.dtic.mil [accessed 17 December 2017].

Hayoun, M. and Goldstein, S., 2017. *EMS, Weapons of Mass Destruction and Related Injury*. Einstein Healthcare Network, October 06 2017.

Huba, W., 2006. *Traditional and Irregular War*. US Army War College.

Katzman, K. and Thomas, C., 2017. Afghanistan: Post-Taliban Governance, Security and U.S. Policy. *Congressional Research Service Report*. Available on: www.fas.org. [accessed 29 December 2017].

Landinfo. 2017. Report Afghanistan: Recruitment to Taliban. Available on: https://landinfo.no/asset/3588/1/3588_1.pdf

Lele, A. 2014. Asymmetric Warfare: A State vs Non-State Conflict. *OASIS*, 20, 97-111.

Military Review. 2014. Command and General Staff School.

Miller, M., 2014. Momentary Memorials: Political Posters of Lebanese Civil War and Hezbollah. University of Colorado.

Najetović, Dž., 2011. Globalni terorizam i njegove implikacije na međunarodne odnose. Anali Pravnog Fakulteta u Zenici, 215-227. Available on: https://www.scribd.com/document/92074745/Terorizam

Neumann, P., 2008. *Joining Al Qaeda: jihadist Recruitment in Europe*. International Instutite for Strategic Studies: London.

Ravlić, S., 2001. Politička ideologija, preispitivanje pojma. *Politička misao*. 38(4):146-160.

Rynegeart, C., 2017. Non-state Actors in International Law: A Rejoinder to Professor Thirlway. *Netherlands International Law*. April 2017, Vol.66/1 64: 155-162.

Shuck, G., 2015. *Online Jihadism*. Global Security Studies. Baltimore, Maryland. Available on: https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/39436/SHUCK-THESIS-2015.pdf?sequence=1&isAllowed=y

Smit, T., 2017. Multilateral Peace Operations and the Challenges od Terrorism and Violent Extremism. *SIPRI Background Paper*. November 2017. Available on: www.sipri.org.

Sokolsky, R., 2017. The New NATO/Russia Military Balance. Implications for European Security. 17 March 2017. *Carnegie Institute*. Available on: http://carnegieendowment.org/2017/03/13/new-nato-russia-military-balance-implications-for-european-security-pub-68222. [accessed 17 January 2018].

Springer, N., 2008. Implementing Population Centric COIN. *Small Wars Journal* 2008/6.

Stradiotto, G. and Guo, S., 2014. *Democratic Transitions: Modes and Outcomes*. Routledge: New York.

Telley, C., 2018. A Coint for the Tsar: The Two Disruptive Sides of Cryptocurrency. *The Smallwars Journal*. January 15 2018. Available on: http://smallwarsjournal.com/jrnl/art/a-coin-for-the-tsar-the-two-disruptive-sides-of-cryptocurrency [accessed 20 January 2018].

Violence and Terrorism. 2004. 6th Ed. McGraw — Hill. New York.

Vukasović, B., 2009. *Nacionalna sigurnost i terorizam*. Ministarstvo obrane RH. Zagreb. Vojno učilište «Petar Zrinski».

Winter, C., 2017. *Media Jihad: The Islamic State's Doctrine for Information Warfare*. The International Center for the Study of Radicalization and Political Violence. Institute for Strategic Dialogue.