Vol.9 • 2017

ISSN. 1307 - 9190

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
2004
TURKEY

Defence Against Terrorism Review

DATR

The Uniqueness of Hybrid War and Evaluation of PKK's Hybrid Capability
Emre DEMİRALP

Hacking Back Against Cyberterrorists: Could you? Should you?
Alan BRILL & Jason SMOLANOFF

The Use of Social Media for Terrorism
Erdal ÖZKAYA

Islamic State of Iraq and Syria's Terrorism: A Universal Instrument of Asymmetric Warfare and the New Battlefield in Europe
Thomas MAURER

COE-DAT

Centre of Excellence Defence Against Terrorism

Defence Against Terrorism Review – DATR **ISSN 1307 - 9190**

DATR is an international peer-reviewed journal that is abstracted and indexed in EBSCO Publishing.

DATR 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 or COE-DAT. The views presented in articles are those of the authors.

Defence Against Terrorism Review – DATR **ISSN 1307 - 9190**

DATR dergisi uluslararası hakemli bir dergidir ve EBSCO Host veritabanı tarafından taranmaktadır.

DATR dergisi Terörizmle Mücadele Mükemmeliyet Merkezi (TMMM)'ne ait bir yayındır. NATO, NATO Üye Ülkeleri, NATO Ortaklık Ülkeleri, ilgili özel kuruluşlar ile kamu kurumları ve ilgili kişilerin kullanımı için hazırlanmaktadır.

DATR dergisinde yayınlanan yazılarda belirtilen fikirler yalnızca yazarına/yazarlarına aittir; TMMM'yi, NATO'yu ve NATO'nun fikir ve politikalarını temsil etmez, bağlamaz.

Yayın Sahibi: Mehmet Aslantaş
Sorumlu Yazı İşleri Müdürü: Kemal Olçar
Yayın Türü: Yerel Süreli Yayın
Yayın Şekli: Yıllık İngilizce

Defence Against Terrorism Review – DATR
Terörizmle Mücadele Mükemmeliyet Merkezi (TMMM)

Devlet Mahallesi İnönü Bulvarı
Kirazlıdere Caddesi No:65 06582
Çankaya/ANKARA

Tel: 0 (312) 425 8215
Faks: 0 (312) 425 6489
E-posta: datr@coedat.nato.int

Baskı: Başak Matbaacılık
Anadolu Bulvarı Meka Plaza No:5/15 Gimat
Yenimahalle/ANKARA
Tel: 0 (312) 397 1617

Basım Tarihi: Aralık 2017

Defence Against Terrorism Review

DATR

Vol. 9, 2017

ISSN. 1307-9190

CONTENT

The Defence Against Terrorism Review (DATR) is calling for papers for coming issues. The DATR focuses on terrorism and counterterrorism. All of the articles sent to DATR undergo a peer-review process before publication.

For further information please contact datr@coedat.nato.int

REFEREES SERVED IN THIS ISSUE

Andrew MUMFORD, Ph.D. - *University of Nottingham*

Aşkın İnci SÖKMEN ALACA, Ph.D. - *İstanbul Arel University*

Gordon WOO, Ph.D. - *Risk Management Solutions (RMS)*

Serhan TATAR, Ph.D. - *Turkish Air Forces*

Serhat ERKMEN, Ph.D. - *Ahi Evran University*

Sezgin KAYA, Ph.D. - *Uludağ University*

Uğur GÜNGÖR, Ph.D. - *Başkent University*

This Page Intentionally Left Blank

Editor's Note

Dear Defence Against Terrorism Review (DATR) readers,

It is a pleasure for our team to present you with a new issue. DATR Volume 9 includes four articles; in these articles we will be examining two different terrorist organizations, namely the PKK and ISIL/DAESH. Additionally, two other articles focus mainly on cyberspace with one discussing the exploitation of social media and the other raising the issue of possibility and applicability of hacking back against cyberterrorists.

This issue starts with *The Uniqueness of Hybrid War and Evaluation of PKK's Hybrid Capability* written by *Emre Demiralp*, 1st Lieutenant working at the Turkish Gendermarie. In his article, he discusses the term 'hybrid' and how to define a hybrid war. 1st Lt. Demiralp also emphasizes the significance of identifying a hybrid adversary. In this regard, the author underlines that although many terrorist organizations were analyzed and examined in terms of their hybrid character, the PKK, a dangerous terrorist organization, has never been examined in such a manner.. Therefore, the author analyzed and examined PKK's hybrid capacity by utilizing Bowers' Model to fill a gap in the literature.

The second article in this issue is *Hacking Back against Cyberterrorists: Could you? Should you?* It was written by *Alan Brill* and *Jason Smolanoff*, both Senior Managing Directors at Kroll Cyber Security and Adjunct Professors at Texas A&M University School of Law and Loyola Law School, respectively. The authors highlight that given the developments in cyberspace, the availability of resources on social media, and the improvements of techniques and tactics that cyberterrorists use, currently an environment exists in which cyberterrorists could easily operate. On the basis of this assumption, the authors raise the question whether any organization – be it governmental or non-governmental, public or private – would like to launch a counterattack, a 'hack back' as authors proposed, and start to engage in a war in cyberspace instead of a real battleground. In the article, the authors state and discuss the potential advantages and risks related to 'hack back' operations.

The next article is *The Use of Social Media for Terrorism* written by *Erdal Özkaya*. He works as a Cybersecurity Architect at Microsoft Services. In his article, Mr. Özkaya addresses the exploitation of social media by terrorist in terms of spreading their narrative, supporting the propaganda, recruiting new members, and so forth. Apart from that, the author also analyzes the issue of 'dark web' in which terrorists could achieve their goals that were hard to reach on social media.

The last article of this issue is the *Islamic State of Iraq and Syria's Terrorism: A Universal Instrument of Asymmetric Warfare and the New Battlefield in Europe*. It was written by *Thomas Maurer*. He has completed his master's degree at Helmut-Schmidt-University. In his article, the author gives an overall assessment of ISIL/DAESH. Mr. Maurer highlights that ISIL/DAESH conducts terrorist attacks to fulfill different aims ranging from gaining territory to destabilizing closer regions. At the same time, it continues to strengthen its status of a 'self-claimed' caliphate and spread fear and horror particularly in Europe by specific targeted attacks.

As the world changes every day; so does terrorism. It evolves according to developments in technology, while adjusting itself to new trends, techniques, and tactics. As a result, it continues to exist and resist all countering endeavors with a significant effort. Also, we must pay great attention to the changing environment of terrorism so that we can cope with future attacks and/or threats in various dimensions.

As a last word, we would like to convey our regards to the distinguished authors, vigilant referees, and mostly to our precious readers without whom this journal would be worthless to publish. We hope you enjoy this issue, and we are looking forward to meeting you on the next one.

Atasay ÖZDEMİR, Ph.D.
Editor-in-Chief

DATR, 2017; 9: 09-33

ISSN 1307 - 9190

The Uniqueness of Hybrid War and an Evaluation of PKK's Hybrid Capability[1]

Emre DEMİRALP[2]

Abstract: *Russian involvement in Crimea and Hezbollah's activities during the Second Lebanon War brought 'hybrid war' into the literature of Western militaries. The academic ambiguity to define hybrid war emerged as an important problem for modern militaries. Identifying a hybrid adversary was of utmost importance to prevent threats before they come into existence. Although terrorist organizations like Hezbollah, Al-Qaeda and Taliban have been analyzed in light of their 'hybrid character,' the PKK, as one of the most dangerous terrorist organizations, has never been examined for its 'hybrid character'. This article, with using the model of Bowers, a military strategist in the US, aims to explore PKK's hybrid capacity.*

Keywords: *PKK, Hybrid, War, Warfare, Turkey*

[1] Submitted on 09 June 2017. Accepted on 08 August 2017.

[2] *1st Lieutenant, Turkish Gendarmeria General Command, eemredemiralp@gmail.com*

Introduction

For the last 50 years, the world's greatest military powers have been involved in low level conflicts rather than full-scale wars. In these conflicts, where conventional means and methods of engagement have lost their superiority, threat perception has become more complex – what is perceived as harmless could be used as the deadliest weapon against an enemy. The American 'Vietnam Syndrome' and the 'Soviet Adventure' in Afghanistan constituted the initial case studies of such wars. Additionally, American intervention in Iraq and Afghanistan proved to be a new dimension to the changing character of war. In time, terrorist organizations displayed enormous enthusiasm to adapt to the changes in warfare. Along with their irregular character, terrorist organizations have also tried to be effective in economic, social and psychological methods of warfare in order to be able to have a regular capacity as conventional armies. Many different names such as 'compound war', 'unrestricted war', and 'new generation wars' have been used to define the emerging warfare in the literature. Lastly, Hezbollah's display of advanced tactics during the Second Lebanon war against the Israeli Defense Forces proved how quickly terrorist organizations can adopt evolving technologies to improve their threat capacity. Following the Russian involvement in Ukraine conflict (Crimea specifically), which contained multidimensional and complex methods of engagement, such wars have been frequently called 'hybrid' in the literature of warfare.

In this context, the Syrian Civil War is very important considering how it caused both the emergence and reorganization of some of the terrorist organizations in the region. For sure, the Kurdistan Workers' Party (often abbreviated PKK for its Kurdish name, *Partiya Karkeran Kurdistan*) is one of the terrorist organizations that has seized this opportunity and changed its strategic policies in the region. In an unprecedented way, PKK accelerated its armed activities inside and outside of Turkey. In Turkey, PKK's activities included 'calling people for civil disobedience' and launching of 'urban conflict' in some city centers by digging holes, digging trenches, building barricades, and etc. Along with its decision to carry the conflict into cities (which the PKK had never tried before), the PKK also improved its armed presence in Syria thanks to its Syrian offshoot, the PYD (Partiya Yekîtiya Demokrat). Since the summer of 2015, the PKK has been using every tool at its disposal and taking every advantage to achieve its long-living dream of establishing an independent Kurdish state. The PKK's increasing financial supplies in Europe and in Syria/Iraq, the availability of weapon stocks for the PKK that have been supplied to the PYD in Syria and its increasing political activities in the region are the main sources of concern for Turkey. In this respect, evaluating the variable methods of conflict that PKK has been employing since August 2015 proves important to determine the organization's hybrid character and whether it will become a more dangerous threat in the future.

Research Methodology

The modules of hybrid war and other different modes of warfare/conflict all focus on the complexity of the emerging new methods of warfare which are of utmost importance for conventional armies. Considering the academic inability to compromise on how to define these potential complex and nested threats, it has been almost impossible to create a concrete model of future enemies.

The first module designed to define an emerging hybrid adversary has been created by Major Bowers and first published in 2012[3]. Bowers's module, which is termed a method for 'Identifying a Hybrid Adversary' uses three core variables and additional sub-variables to determine a terrorist group's capacity to pose a hybrid threat or will be likely able to pose a hybrid threat in the future. The model, by using three core variables - Maturity, Capability, and Complex Terrain - aims to evaluate the potential to materialize as a hybrid threat. These core variables divide into sub-variables within themselves, as shown in the Figure 1.

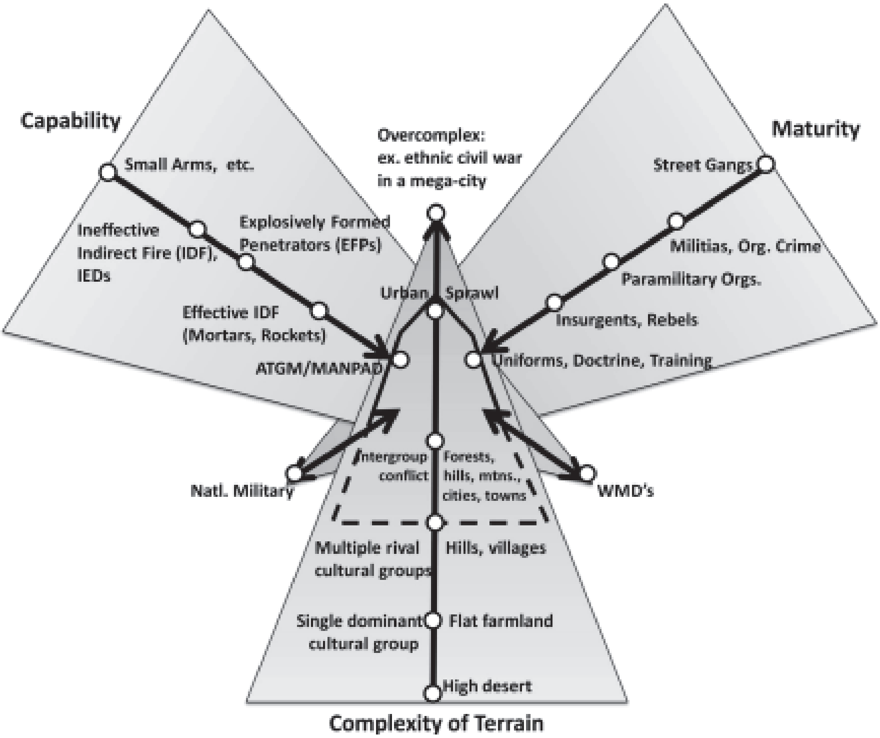
Capability
Small Arms, etc.
Ineffective Indirect Fire (IDF), IEDs
Explosively Formed Penetrators (EFPs)
Effective IDF (Mortars, Rockets)
ATGM/MANPAD
Overcomplex: ex. ethnic civil war in a mega-city
Urban Sprawl
Maturity
Street Gangs
Militias, Org. Crime
Paramilitary Orgs.
Insurgents, Rebels
Uniforms, Doctrine, Training
Natl. Military
WMD's
Intergroup conflict
Forests, hills, mtns., cities, towns
Multiple rival cultural groups
Hills, villages
Single dominant cultural group
Flat farmland
High desert
Complexity of Terrain

Figure 1: Bowers first used the model 'Hybrid Threat Intersection'[4]

[3] Christopher O. Bowers, "Identifying Emerging Hybrid Adversaries", *PARAMETERS*, Spring 2012, p.41

[4] Ibid, p.42.

After the Bowers model, Huovinen further developed a model to create a more visualized version of it in his research[5] (Figure 2). As shown in the Figure 2, every sub-variable has its own qualities that help to determine the strength of it in light of hybridity. The closer a quality of the group gets to the center of the circle, the more dangerous it will be. To qualify as hybrid, a group's qualities must be in the light red area, darker red area or within the center of the circle. Otherwise the group has lost its identity as a hybrid kind. After modifying Bowers model, Huovinen analyzed 'Hezbollah' and 'Al-Qaeda' in light of the 'Modified Model of Identifying a Hybrid Threat' to determine whether they are hybrid threats or not. For this reason, in this paper the same model is applied to the PKK to analyze the hybrid quality of the terrorist organization.

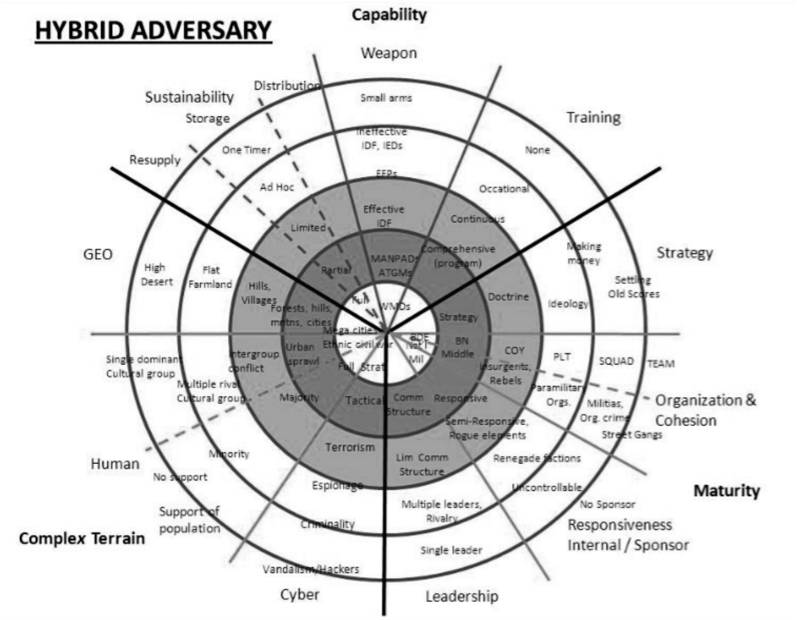

Figure 2: Huovinen's model is called the"Modified Model of Identifying a Hybrid Adversary" and is inspired by the works of Bowers.[6]

1- Hybrid War and Its Friends

To understand what means to have a hybrid adversary, one needs to know what hybrid war looks like. This requires a better understanding of the familiar forms of combats/wars that are mentioned in the hybrid war literature. Irregular war is one of the main components of hybrid conflicts. It is defined as the "violent struggle among state and non-state actors for legitimacy and influence over

[5] Petri Oskari Huovinen, "Hezbollah and Taliban; Hybrid Adversaries in Contemporary Conflicts", (Published MA Thesis, National Defense University, Finland, 2013).

[6] Ibid.

a population" in the Joint Operating Concept of the US Department of Defense published on 11 September 2007. Irregular wars, especially after the collapse of Soviet Union, are predominantly led by sub-state groups (non-state actors) that are trying to avoid a state's military superiority by using guerilla tactics.[7] Furthermore, insurgency movements have applied terrorism as an irregular warfare tactic to bring about a change in the political order without weakening the support of the population.[8] Classical irregular adversary, according to Kiras, would try to spread the conflict in 'time' and in 'space' to seek 'internal support' and 'legitimacy'.[9]

As the non-state/state actors have started to apply interconnected means and methods in their tactics, new questions arise over the qualification of new modes of warfare. That is how terms like 'compound warfare', 'unrestricted warfare' and 'hybrid warfare' have developed in the literature of warfare. Within these, the term 'compound warfare' that is put forward by Thomas Huber, is the first academically used description to define this emerging, complex form of warfare. Huber defines compound warfare as the "simultaneous use of regular or main force and an irregular or guerilla force against an enemy."[10] It is generally preferred by states/actors with lesser power against a states/ actor with relatively superior power by using irregular forces in coordination with regular forces to pressure the occupying state to both mass and disperse at the same time.[11] The People's Liberation Army of South Vietnam, by organizing itself on two levels (full military units and paramilitary/guerilla units which have regional and local guerilla sub-units), is one of the earliest examples of how compound warfare has been carried out on the battlefield.[12] Another point in compound warfare that was asserted by Baumann was that an irregular adversary may opt to compensate for its weakness of not having a conventional character by having close economic, political and training support with its allies. According to him, Afghan mujahideens simply applied this method while taking advantage of the safe havens in Iran and Pakistan to defend themselves against the Soviet Army.[13]

Apart from that, unrestricted warfare, as put forward by Chinese Colonels Qiao-Liang and Wang Xiangsiu, also has an appealing character to define the emerging nature of complex warfare. In their view, next generation warfare will "transcend all boundaries and all limits" and will be governed by an adversary that utilizes all possible means at its disposal.[14] The future wars will not only take

[7] Frank G. Hoffman, "Conflict In the 21st Century: The Rise of Hybrid Wars", (Potomac Institute For Policy Studies And The Center For Emerging Threats and Opportunities, Arlington, 2007), pp. 2-9

[8] James D. Kiras, "Irregular Warfare: Terrorism and Insurgency", *Strategy in the Contemporary World* (Baylis et al, eds, Oxford University Press, 2013), p. 188.

[9] Ibid, pp. 189-194.

[10] Thomas M. Huber. "Compound Warfare: The Fatal Knot", (U.S. Army Command and General Staff College Press, Fort Leavenworth, Kansas, 2002), p. 1.

[11] Ibid, p. 2

[12] Ibid, pp. 229-230

[13] Robert F. Baumann, "Compound War Case Study: The Soviets in Afghanistan", *Compound Warfare: The Fatal Knot* (Tomas Huber, ed., 2002), p. 302

[14] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, (PLA Literature and Arts Publishing House, Beijing, 1999), pp. 19-24.

place on the physical battlefield with regular armies fighting one another, but it will expand into different domains such as economics, information networks, religion and culture. According to the Chinese, every tool and tactic used by an adversary will become a new Chinese weapon and this weapon will be pointed first at the most commonplace things that the enemy has.[15]

Within this academic environment, the term 'hybrid warfare' was used first after the Second Lebanon War. Following that, Russia's war with Georgia and Russian armed activities in Crimea made 'hybrid war/conflict' more common and brought the subject into NATO's agenda as top priority. During the Second Lebanon war, according to Hoffman, who is one of the leading figures of the "hybrid war" concept, Hezbollah demonstrated what a hybrid adversary looks like. Considering it to be a "fusion of militia units, its use of information warfare, and its success in using specially-trained fighters who have expertise in using antitank guided missiles and antiship cruise missiles,[16] Hezbollah manifested the important characters of an hybrid adversary. However, the academic world did not reach a consensus on either the authenticity of 'hybrid war' as a term or on Hezbollah's hybrid character. According to Simpson, hybrid conflict is neither new nor identical to existing forms.[17] Moreover, Nemeth characterize hybrid war as the contemporary form of guerilla warfare.[18] In addition to that, Huber acutely criticized Hoffman's example, which qualifies Hezbollah as an emerging hybrid threat, claiming that these armed groups are 'robust insurgencies' that are using 'insurgent methods with new technologies.' However, Hoffman asserted that hybrid war is identical to conventional warfare in terms of its complexity, fusion, and simultaneity at the operational level and even possibly at the tactical level. His most crucial point is that in hybrid wars "one or both sides is blending and fusing the full range of methods and modes of conflict," while compound wars only "offers synergy and combinations at the strategic level."[19]

Despite the fact that Huber and Hoffman have competing ideas on the dynamics of hybrid wars and their relation to compound wars, both agree on the fact that future conflicts/wars will employ a combination of regular and irregular tactics. A hybrid threat can be defined as a multidimensional threat born out of different challenges that are carried out by different actors.[20] The enemy that poses such a threat could be either a state or a non-state actor that can employ a wide range of means (political, military, economic, social and informational techniques) by using conventional, irregular, catastrophic and terrorist methods of warfare.[21] Although NATO identified hybrid war as

[15] Ibid, p. 26.

[16] Frank G. Hoffman, "Hybrid vs. Compound War: The Janus choice: Defining today's multifaceted conflict", *Armed Forces Journal* (1 October 2009).

[17] Erin M. Simpson, "Thinking About Modern Conflict: Hybrid Wars, Strategy, and War Aims" (Paper presented to the Annual Meeting of the Midwest Political Science Association Chicago, IL, 7-11 April 2005), p. 22

[18] William J. Nemeth, "Future War and Chechnya: A Case For Hybrid Warfare", (Published MA Thesis, Naval Postgraduate School, 2002), p. 29.

[19] Frank G. Hoffman, "Hybrid Warfare and Challenges", *Joint Forces Quarterly* 52, (1st quarter 2009), p. 36.

[20] Patryk Pawlak, "Understanding Hybrid Threats", (European Parliamentary Research Service, June 2015), p. 1.

[21] Russel W. Glenn, "Thoughts on 'Hybrid' Conflict", (Small Wars Journal, 2009), p. 2.

an emerging threat for its security, it is the U.S. Government that described what a hybrid adversary/threat looks like. The U.S. Armed Forces defines a hybrid threat as "the diverse and dynamic combination of regular forces, irregular forces, criminal elements, or a combination of these forces and elements all unified to achieve mutually benefiting effects."[22] A hybrid adversary, appreciating and using the cover that urban terrain provides, purposefully carries the conflict into established areas and cities to maintain disorder by using criminality.[23] Irregular and asymmetric battles fought within the areas of "conflict zone population, the home front population and international community population" are definitely key to the result of a hybrid war.[24] In that sense, what makes hybrid war distinct is its requirement of "simultaneous rather than sequential success in these diverse but related population battlegrounds."[25] In this context, Russian involvement in Ukraine and Hezbollah's armed activities against Israel are extremely relevant and leading to understanding what 'hybrid wars/conflicts' look like.

2- Prototype Hybrid Wars of the Twenty-First Century

In his article, Russian Chief of General Staff Valery Gerasimov mentioned the lessons of "Arab Spring" and pointed out that "the typical warfare of the 21st century involves non-military means of achieving political and strategic goals" along with "military means of concealed character."[26] According to him, "asymmetrical actions have come into widespread use" and "open use of force is resorted only at a certain stage, primarily for the achievement of final success in the conflict." While Russia arose as the most influential state user of these methods in its armed activities in its region, Hezbollah on the other hand won the title at the beginning of 21st century as the non-state armed group that best applied multidimensional methods of warfare that are labeled 'hybrid' by some scholars.

A- Second Lebanon War:

If Hezbollah's position in Lebanon is evaluated, one can easily understand that Hezbollah's armed strength should not be underestimated. The Israeli-Lebanese conflict and the continuing disagreements between these two states provided the necessary conditions for Hezbollah to win the hearts of the Lebanese people.[27] Today, in addition to having extensive civilian participation, Hezbollah is said to have 8,000-10,000 military units in the Lebanese Resistance Brigades, of

[22] Field Manual 3-0, "Operations", *Headquarters: Department of The Army* (February 2008), pp. 1-5.

[23] Hoffman, "Conflict In the 21st Century: The Rise of Hybrid Wars", pp. 15, 28.

[24] John. J. McCuen, "Hybrid Wars", *Military Review* (March-April 2008), p. 107.

[25] Ibid.

[26] Valery Gerasimov, "The Value of Science for the Future", *Military-Industrial Kurier*, 8 (476), (2013).

[27] Bryan R. Early, "Larger Than a Party, yet Smaller than a State: Locating Hezbollah's Place Within Lebanon's State and Society", *World Affairs* 168 (3) (2006), p. 124.

which 2,000-4,000 is said to have expertise in guerilla warfare and advanced weaponry.[28] Although Hezbollah and its armed activities have a long history, the Second Lebanese War has a special importance since it brought the issue of 'hybrid war' into view. The conflict between Hezbollah and Israel started on 12 July 2006 after Hezbollah attacked Israeli border forces and kidnapped two Israeli soldiers. Israel first responded with an air campaign, than followed that with a ground invasion and a naval blockade of Lebanon. During the thirty-four-day war, Hezbollah surprised Western military strategists (especially the Israeli Defense Forces (IDF)) with its tactics, weapons and strategies. First of all, the result of the conflict showed that Hezbollah had studied the earlier combat in detail. Hezbollah, while mining the alternative retreat routes of IDF tank teams, had also equipped its special units with antitank missiles.[29] Moreover, during the conflict, Hezbollah fired over 4000 rockets into Israel. This had the important effect of distracting the IDF's attention.[30] Hezbollah's capability to employ different modes of armed attacks simultaneously showed its ability to carry out not only defensive but also offensive complex operations.[31] Many armed terrorist groups are said to have high-tech weapons and what frightens militaries is the possible use of these weapons in a way that will cause heavy casualties. This nightmare almost came true in the Second Lebanon War as Hezbollah used an antiship cruise missile to hit an Israel Saar-5 Class destroyer. In addition to that, cyber warfare tactics, such as making drone flights[32] over the Israeli border, were used by Hezbollah frequently during the conflict. With such tactics, they were able to neutralize an Israeli drone by using cyberattacks to its network and listen to the cell phone conversations of IDF officers.[33] All of these prove the fact that Hezbollah has successfully applied operational-level warfare. Also, Iran's economic and logistical support to Hezbollah contributed to the organization's hybrid character because it had a foreign state sponsor supplying a safe haven. [34]

B- Russia/Ukraine Conflict

According to international reporting, Russia has claimed to be conducting a hybrid war in Crimea. As the uprisings in Crimea that began at the end of February 2014 were led by pro-Russian separatists, Russia started to play its cards. In the subsequent days, armed men in green uniforms without any insignia (known as the 'little green men') appeared in Crimea and seized control of

[28] Marcin Andrzej Piotrowski, "Hezbollah: The Model of A Hybrid Threat", *The Polish Institute of International Affairs Bulletin* 24(756) (2 March 2015), p.1.

[29] Andrew Exum, "Hezbollah at War: A Military Assessment", *Policy Focus* (63), *The Washington Institute For Near East Policy*, p. 11.

[30] Daniel Byman and Bilal Y. Saab, "Hezbollah In a Time Of Transition", *Center for Middle East Policy at Brookings*, Atlantic Council, (November 2014), p. 4

[31] Timothy McCuulloh and Richard Johnson, "Hybrid Warfare", Joint Special Operations University Report 13-4, (August 2013), p. 23.

[32] Hamza Hendawi, "Israel: Hezbollah Drone Attacks Warship", *The Washington Post*, (14 July 2006), p.1

[33] Ze'ev Schiff, "Hezbollah Listened in on IDF Beepers Cell Phones", (04 October 2006), *Haaretz*, available at http://www.haaretz.com/hezbollah-listened-in-on-idf-beepers-cell-phones-1.200526, (accessed 09 March 2016).

[34] McCuuloh and Johnson, p. 5.

the Crimean parliament building.[35] The international public had serious suspicion that the Russian Spetsnaz (special forces) provided these armed groups to execute guerilla-type operations in order to overthrow the government in Ukraine.[36] A hacker tool popular across underground Russian crime networks has been used in cyberattacks against Ukrainian governmental infrastructure, both to prevent the functioning of the daily routine of state mechanism and to gain intelligence.[37] Detection of the distribution of a targeted malware called 'Black Energy,'[38] which originated in Russia and targeted the Ukrainian government, was very similar to the Russian attacks on Georgia's command and control systems during the 2008 Russia-Georgia War.[39] Although Russia never accepted responsibilities for these activities in the field in Crimea, at a later time President Putin of Russia acknowledged that the annexation of Crimea had been planned earlier, as the unofficial polls conducted by Putin showed the majority of Crimeans would back reunification with Russia.[40] Moreover, the Russian parliament approved Putin's plan to use force in Ukraine.[41] What Gerasimov referred to as "military means of concealed character: use of informational conflict and the actions of special-operations forces" has brought to mind the fact that Russia may have adopted similar tactics in Crimea, such as denial and deception of its military actions in the field. Thus, disinformation worked to conceal the real objectives of Russia on the field.[42] In addition to that, Russian privilege on Ukrainian social media and broadcasting channels helped Russia to have an upper hand in the information warfare.[43] Russia Today (RT) and Sputnik News were the primary Russian propaganda channels that aimed to lead loyal Russian communities in Ukraine. Television programs that portrayed the ethnic Russians as second-class citizens and polls that expressed the discontent of the pro-Russian minorities were all used as efforts for reunification.[44]

[35] Harriet Salem, Shaun Walker, and Luke Harding, "Crimean parliament seized by unknown pro-Russian gunmen", (27 February 2014), *The Guardian*, at http://www.theguardian.com/world/2014/feb/27/crimean-parliament-seized-by-unknown-pro-russian-gunmen (accessed: 17 March 2016).

[36] John R. Davis Jr. "Continued Evolution of Hybrid Threats: The Russian Hybrid Threat Construct and the Need for Innovation", *The Three Swords Magazine* 28, (2015), p. 21.

[37] Ibid, p. 22

[38] Tom Fox-Brewster, "Russian malware used by 'privateer' hackers against Ukrainian government", (25 September 2014), *The Guardian*, available at http://www.theguardian.com/technology/2014/sep/25/russian-malware-privateer-hackers-ukraine (accessed: 28 March 2016).

[39] Eve Hunter and Piret Pernik. "The Challenges of Hybrid Warfare", *International Centre For Defense And Security* (April 2015), p. 5.

[40] "We did what we had to do: Putin opens up on Crimea reunification plan", (10 March 2015), *Russia Today*, available at https://www.rt.com/news/239197-putin-crimea-referendum-decision/, (accessed 12 January 2017). See also "Putin reveals secrets of Russia's Crimea takeover plot", (09 March 2015) *BBC*, at: http://www.bbc.com/news/world-europe-31796226 (accessed 17 March 2015).

[41] "Russian Senators vote to use stabilizing military forces on Ukrainian territory", (01 March 2014), *Russia Today*, available at https://www.rt.com/news/russia-ukraine-approve-miltary-371/, (accessed:10 January 2017).

[42] Maria Snegovaya, "Putin's Information Warfare In Ukraine", *Institute For The Study of War* (September 2015), pp. 7-11.

[43] Eve Hunter, and Piret Pernik. "The Challenges of Hybrid Warfare", pp. 4-6.

[44] Michael Kofman, and Matthew Rojansky, "A Closer Look At Russia's 'Hybrid War'", *Kennan Institute Wilson Center* 7 (2015), pp. 4-5.

At the strategic level, Russia seemed like a compatible international actor for reconciliation. It seemed to obey the precepts of international law, promoted cease-fires and reviewed its policies as the conflict expanded in time.[45] Economic sanctions and destabilization of energy prices all worked in Russia's favor at the strategic level.[46] Russian exercise of military training and mass mobilization of Russian troops on the Ukraine-Russia border were all timely measures that distracted Ukrainian attention.[47] Russian activities in the industrial region of Donbas, which already had sensitive legal ties with the central government in Ukraine, contributed to the escalation of tensions in the region.[48] During all the phases of the conflict, Russian broadcast channels pressured the Ukrainian government to declare autonomy for the pro-Russian areas of eastern Ukraine. Further analysis of the ongoing conflict between the two sides reveals one fact very clearly: the annexation of Crimea, as Russian President Putin admitted, was planned earlier and implemented step by step.

The problems between Russia and Ukraine over the annexation of Crimea and Russia's military presence in the Donbas region still continue. In addition to its tactics in Georgia, Russian activities in Ukraine proved that Russia was and is willing to adopt multidimensional strategies towards its adversaries when needed. In that sense, Russia's employment of a wide variety of instruments of power including military, economic, informational, and diplomatic force represents how 'hybrid wars' come into being when carried out by a state actor.[49]

Is the PKK Demonstrating Hybrid Skills?

The PKK, which has Marxist-Leninist roots, was founded in Turkey by Abdullah Öcalan in 1974. The group launched terrorist activities against the Turkish state in the middle of 1980s and in later periods pursued a separatist policy based on Kurdish nationalism. The PKK, in general, aims to establish an independent Kurdish state in the territories of Iran, Iraq, Syria, and Turkey. The organization went through a period of crisis following the capture of its leader Öcalan in Nairobi by Turkish Special Forces in 1999. Additionally, following the political crisis between Turkey and

[45] John R. Davis Jr. "Continued Evolution of Hybrid Threats: The Russian Hybrid Threat Construct and the Need for Innovation", p. 22.

[46] Ibid.

[47] Deborah Hastings, "At least one person crushed to death in Ukrainian stampede; Putin orders massive military exercises", (26 February 2014), *New York Daily News*, available at http://www.nydailynews.com/news/world/putin-calls-military-exercises-ukraine-border-crimean-protester-crushed-death-article-1.1702586, See also "Russia leader Vladimir Putin says he'll protect Russians in Ukraine by any means, but hopes force not required", (04 March 2014), *CBS News*, available at http://www.cbsnews.com/news/putin-reportedly-orders-troops-near-ukraine-border-back-to-bases-after-military-exercises/, (accessed: 18 March 2016).

[48] Tatyana Malyarenko, "Playing a Give-Away Game? The Undeclared Russian-Ukrainian War in Donbas", *Small Wars Journal*, (23 December 2015), pp. 1-5.

[49] John R. Davis Jr. "Continued Evolution of Hybrid Threats: The Russian Hybrid Threat Construct and the Need for Innovation", p. 19.

Syria over the PKK's existence in Syria, the PKK was forced to leave its safe haven in the Syrian-controlled Bekaa Valley and for a second setback. However, the terrorist organization managed to easily diversify its foreign sponsors and stepped up its presence in northern Iran as well as in northern Iraq.[50]

When the 'peace process'[51] between Turkey and PKK reached an end after August 2015, the PKK had already started more severe terrorist activities. The PKK's struggle to carry the conflict into urban areas and its endeavor to obtain modern weapons arose as new problems. Additionally, Turkey had serious concerns regarding direct links between the PKK and the PYD/YPG[52] under the organizational structure of the 'Koma Civaken Kürdistan (KCK), the Kurdish Societies Assembly. The PYD's armed advancement in Syria signaled that the PKK was trying to expand its political and geographical impact in the area.[53] In particular, its military and political activities inside Turkey proved that the PKK is trying to adapt its activities to the changing nature of conflict in the region by prolonging the conflict by frustrating the government attempts to leverage protracted political pressure. The increasingly "militarized grey area", according to Olliviant, is now being dominated by "hybrid warriors" as the new non-state actors that have the "capacity of an industrial/post-industrial nation-state army retaining their ties to the population and a devotion to the 'propaganda of the deed.'"[54] Although the PKK terrorist organization does not have the potential to qualify as an 'industrial/post-industrial' army, the Syrian civil war will definitely have a positive effect on PKK credentials for the future. For this reason, this article aims to analyze the PKK with regards to the variables of hybrid warfare by applying Bowers's 'Identifying a Hybrid Adversary' Model.

3- The Model and the PKK

A- Capability

In this model, the first core variable that will be used to evaluate the PKK is 'capability'. The core variable will be scrutinized with three sub-variables: 'weapons', 'training', and 'sustainability'. According to Bowers, the main constitutive logic behind core variable of 'capability' is that for

[50] Martin von Bruinessen, "Kurdish ethnonationalism versus nation-building states", The ISIS Press, Istanbul, pp. 278-280

[51] The process began with important reforms towards Kurdish population and at later stages military operations, especially cross-borders military operations to the Iraq, decreased and came to a halt. This period has generally been called as the 'peace process' in the eyes of the public and media.

[52] AlthoughTurkey designates PYD/YPG as a terrorist organization and the PKK's Syrian offshot, The PYD/YPG is not listed as a terrorist organization by the European Union and United Nations.

[53] Selen Temizer, Halit Süleymand and Levent Tok, "PKK/PYD captures 8 villages in Syria's Aleppo province", (17 November 2016), *Anadolu Agency*, available at: http://aa.com.tr/en/middle-east/pkk-pyd-captures-8-villages-in-syria-s-aleppo-province/687663, (accessed 12 February 2017).

[54] Andrew Mumford, "The Role of Counter Terrorism in Hybrid Warfare", (COE-DAT, November 2016), p. 6.

an armed group, acquiring complex and high-tech weapons is not itself enough to be classified as a hybrid threat. Additionally, the level of training of the armed group and the level of sustainability to maintain their stocks are also vital elements of becoming a hybrid threat.[55]

In Bower's model, the sub-variable 'weapon' is categorized in different levels of density: the strength of the sub-variable is determined as the weapons get more sophisticated in the following order: small arms ineffective indirect fire (IDF) and improvised explosive devices (IEDs), explosively formed penetrators (EFPs), effective IDF (mortars, rockets) and ATGM/MANPADs. Evaluating the PKK capability with regard to the weapon sub-variable, one can easily conclude that the PKK has the ability to easily obtain small arms like the AK-47, the AK-74, the M-16, the Dragunov, and the PK machine gun, the DShK. On the other hand, the PKK takes advantage of the mountainous and harsh terrain in the eastern part of Turkey, using IEDs and IDFs frequently in their attacks against security forces. Additionally, the PKK prefers to use mortars and rockets when launching extensive attacks on military bases and police/gendarmerie stations. Although the organization's capability to acquire high-tech weapons fall short of being able to acquire weapons of mass destruction (WMD), it is obvious that the PKK has been both acquiring and using sophisticated weapons like MANPADs and ATGMs for a long time. Examples like the downing of Turkish Armed Forces helicopters by the PKK terrorists in the Qandil mountains in 1997,[56] proves that the organization has the capability to acquire such weapons. However, this does not mean or prove that the PKK is frequently renewing its supply channels and acquiring these weapons. Considering that the 1997 operation took place within the Iraq territories where the PKK has their stronghold, there is a chance that the terrorists decided to use MANPADs as their last card to protect their bases. Such weapons have not been used in Turkish territory, thus far.

With regard to its training capability; it would not be wrong to say that the PKK, for 15 years following its establishment, had a safe haven in Syria and build many of its shelters, bunkers and training facilities there.[57] While some documentaries on Abdullah Öcalan (PKK's founder and imprisoned leader) have revealed his comfortable lifestyle in Syria, other video footage have shown him as he attends training exercises and spiritual ceremonies of the terrorists.[58] These videos, along with the confessions of terrorists, show that the organization is trying to conduct regular training exercises in fields that are designed for this purpose. However, at the end of the 1998, the PKK was forced to evacuate its comfortable existence in Syria and seek safe haven in Iraq.[59] While

[55] Christopher O. Bowers, "Identifying Emerging Hybrid Adversaries", *PARAMETERS* (Spring 2012), p. 41.

[56] "Cobra ve Cougar'ı PKK Füzesi Vurdu", (07 June 1997), *Sabah*, available at http://arsiv.sabah.com.tr/1997/06/07/p01.html, (accessed 18 January 2017).

[57] Carolyn C. James and Özgür Özdamar, "Modeling Foreign Policy and Ethnic Conflict: Turkey's Policies Towards Syria", *Foreign Policy Analysis* 5, (2009), p. 25.

[58] Mehmet Ali Birand, a well-known Turkish news anchor and journalist, broadcasted his documentary about Öcalan in the Bekaa Valley of Lebanon in 1992. Video includes a private interview with Öcalan and some video recordings at the PKK camp named Mahzun Korkmaz Academy.

[59] Carolyn C. James and Özgür Özdamar, "Modeling Foreign Policy and Ethnic Conflict: Turkey's Policies Towards Syria", pp. 24-28.

these developments have caused some problems, the organization kept its capabilities alive with doing opportunity training in small groups within/outside of Turkey until it settled down again in Northern Iraq at the beginning of the 2000s. When the PKK's training level is examined, it can be realized that it uses its singular weapons in concert with rockets and mortars. However, it has no capacity to use ATGMs and MANPADs as a part of a larger operation. In addition to that, while PKK has used IEDs as an effective weapon for years, it has recently increased this capability. PKK's postulated ties with the PYD may have helped the organization to develop its deadly skills quickly, thanks to the Syrian Civil War.[60] PKK activities during curfew operations (after the break-down of the peace process) in Nusaybin, Sur and Cizre districts of Turkey, resembles the activities with regard to the type of techniques and tactics that have been used by ISIL/DAESH against the PYD in Syria.[61] Turkey claims that the weapons provided by the US to PYD/YPG have ended up in PKK armories in Northern Iraq.[62] Weapon stocks that have been captured inside the PKK's hideouts both in Iraq and Turkey have raised further questions.[63] Russia-PYD rapprochement in October 2015 in the Azez region was another factor that created discomfort for the Turkish State.[64] Additionally, there is a strong possibility that the PYD not only shared its weapon stocks with the PKK, but also shares the know-how to use the sophisticated weapons it acquired from the countries intervening in the Syrian Civil War. Despite the fact that the PKK's standard unit structure contains an IED expert even in the smallest units, usage of weapons such as mortars, MANPADs and ATGMs are very rare in numbers. When preparing for an ambush, the PKK adopted a system containing several units made up of two-three terrorists that includes an ambush unit, explosive unit, look out unit, and a rearguard unit. Although such an organizational structure could only be developed through regular training, it is not hard to keep it continuing as it becomes perpetual without much renewal.

The fact that PKK has the capacity to obtain and use different levels of weaponry is certainly a considerable threat but this needs to be permanent. An organization will either have a state sponsor or will feed itself. At this point, the PKK's financial resources from the illegal trafficking of drugs, weapons, cigarette, and people create a considerable source of income for the organization.[65] These

[60] Andrew Self, Jared Ferris, "Dead Men Tell No Lies: Using Killed-in-Action (KIA) Data to Expose the PKK's Regional Shell Game", *Defence Against Terrorism Review* 8 (2016), p. 26.

[61] ISIL/DAESH uses human shields, lone snipers are left behind in public places when they leave, use suicide bombers to break the enemy line. These tactics have been started to be used by PKK since the break down of the 'peace process' in Turkey. For a brief analyze of ISIL/DAESH's strategy see Tom Wyke, "Taking cover with sandstorms, hiding snipers in trees...", *Daily Mail*, (08 July2015).

[62] Yahya Bostan, "US Supplied PYD weapons found at PKK hideouts in northern Iraq", (16 October 2015), *Daily Sabah*, available at https://www.dailysabah.com/politics/2015/10/16/us-supplied-pyd-weapons-found-at-pkk-hideouts-in-northern-iraq, (accessed: 02 January 2017).

[63] Ibid.

[64] "Russian support for PKK's Syrian Arm PYD", (27 November 2015), *Anadolu Agency*, available at http://aa.com.tr/en/turkey/russian-support-for-pkks-syrian-arm-pyd-/482307, (accessed: 03 March 2017).

[65] Glenn E. Curtis and Tara Karacan, "The Nexus Among Terrorists, Narcotics Traffickers, Weapons Proliferators, And Organized Crime Networks in Western Europa", (West European Nexus, Federal Research Division of Library of Congress, December 2002), pp. 19-20.

financial resources help the PKK to rebuild its weapons stocks and buy new technologies at a regular rate. Additionally, Turkish authorities have had serious reservations about the transfer of arms from the PYD to the PKK from the beginning of Syrian Civil War. Under these conditions, as long as the Syrian Civil War continues and Iraq exists as an 'unstable state', the PKK will probably try to find alternative supply channels for its needs. Taking into account the possibility that arms and ammunition, supplied from different state actors to a variety of non-state actors/terrorist organizations that take part in the Syrian Civil War, may change hands in this fragile conflict environment is another factor that PKK will want to take advantage of.

This situation appears to be an important factor which supports the thesis that the PKK, which has gone through a 'weapons shortage' in Turkey as a result of comprehensive counterterrorism operations conducted by security forces since the summer of 2016, will try to recover its wounds in the near future from Syrian territory. As Turkish Armed Forces commenced comprehensive air-strike operations from the beginning of August 2015 in the Qandil Mountains, the PKK started to move its training camps and logistical resources to the PYD-controlled areas in Syria. For this reason, the organization will probably renew its resources quickly and continue its training programs as planned.

To sum up, PKK has access to the variety of weapons that is mentioned in Bowers's model (small arms, IDF/IEDs, EFPs, mortars, rockets and ATGM/MANPADs) except WMD. There is no proof that the PKK has substantial amounts of complex weapons like ATGM/MANPADs. However, the PKK's 'training' abilities and 'sustainability' as explained in Huovinen's charter is as follows: its training is 'continuous' (training program) and has 'partial' sustainability. In light of this information, PKK does not fit the qualification criteria for a 'hybrid threat' for the sub-variable 'capability'.

B- Maturity

The other variable that Bowers used in his model to identify a hybrid adversary is 'maturity'. As is evident from the name, it identifies a threat's maturity by analyzing it with regards to the following sub-variables: strategy, degree of organization, responsiveness to internal leadership and foreign state sponsors, depth of leadership.

In general, the PKK's strategy is based on the idea of creating an independent Kurdish state by combining Kurdish dominated territories in Iran, Iraq, Syria, and Turkey. It uses Kurdish nationalism as its most strategic propaganda tool to identify itself as the armed representative of the Kurdish people.

Today, it is possible to observe that the Syrian Civil War is keeping the PKK's strategic hopes alive as the organization is shifting its presence to Syria. The PYD, considered to be the Syrian offshoot of the PKK by Turkey,[66] is supported on the ground by the US.[67] Today, the PYD controls an important amount of territory in northern Syria and shares approximately 550 km of border with Turkey. The PYD's announcement of a federal system as soon as it occupied the town of 'Kamışlı' (Qamişlo)[68] in Syria proves the thesis that PYD will seek territorial gain before the Syrian Civil War ends. The PKK/PYD armed struggle on the ground with ISIL/DAESH has been used as a very important propaganda tool so far by these organizations. Additionally, recent video footage showing PKK/PYD terrorists displaying a large banner of jailed PKK leader Abdullah Öcalan in an iconic square in the Syrian city of Raqqa[69] shows the mutual relationship between them. It is obvious that the PYD has accelerated its efforts for territorial gain and will try to settle down in places where it occupied earlier, before the Syrian Civil War ends (see Figure 3). On the other hand, the PKK's advancement and settlements in the town of Sinjar in Iraq, which has created discomfort for the Iraqi government,[70] is another sign that the terrorist organization will seek additional territorial gain in Iraq, as well.

There are also significant strategic changes in the way that the PKK conducts armed struggle in the field. Apart from its usual methods, the PKK has started to use suicide bombers at an increasing rate and has tried to initiate urban wars in residential areas inside Turkey. The PKK's tactical changes on the ground, which proves the hypothesis that terrorist organizations learn from each other, resemble the type of offensive tactics that were adopted by ISIL/DAESH in Syria against PYD. Especially after December 2015, the PKK's top executives aimed to adopt 'hybrid warfare-like techniques' by carrying the war into residential areas.[71]

[66] "Turkey's Erdogan denounces US support for Syrian Kurds", (10 February 2016), *BBC*, available at: http://www.bbc.com/news/world-middle-east-35541003 (accessed: 08 March 2017).

[67] Spokesperson for the United States Department of State John Kirby said: "We don't recognize PYD as a terrorist organization bu the Turks do, even the best friends aren't going to agree on everything. Kurdish fighters have been some of the most succesful going after DAESH in Syria, we have provided a major support mostly through the air, and that support will continue." "USA: PYD is not a terrorist organisation, they are our friends and we support them", (10 February 2016), *Youtube*, available at: https://www.youtube.com/watch?v=SM36LHVdono. See also "YPG not a terrorist organization for US, spokesman says", (22 September 2015), *Hürriyet Daily News*, available at http://www.hurriyetdailynews.com/ypg-not-a-terrorist-organization-for-us-spokesman-says.aspx?PageID=238&NID=88832&NewsCatID=359 (accessed on: 10 March 2017). US Secretary of Defense Ashton Carter during testimony befora a Senate panel to Senator Lindsay Graham confirmed the link between PYD and PKK. "ABD Savunma Bakanı Ashton Carter ile Senatör Lindsey Graham: PKK / PYD - YPG konusu", (29 April 2016), *Youtube*, at https://www.youtube.com/watch?v=AOHeOKaybcc.

[68] Rodia Said, "Syrian Kurds set to announce Federal System in northern Syria", (16 March 2016), *Reuters*, available at: http://www.reuters.com/article/us-mideast-crisis-syria-federalism-idUSKCN0WI0ZT (accessed 13 January 2017).

[69] "Pentagon condemns display of PKK symbols in Raqqa", (20 November 2017), *TRT World*, available at https://www.trtworld.com/mea/pentagon-condemns-display-of-pkk-symbols-in-raqqa-11529 (accessed 23 November 2017).

[70] Paul Iddon, "Pressure mounts on PKK over Sinjar presence", (27 December 2016), *Al Monitor*, available at: http://www.al-monitor.com/pulse/originals/2016/12/pkk-iraq-sinjar-turkey.html, (accessed 15 January 2017).

[71] İlnur Çevik, "PKK trying to challenge Turkey in Diyarbakır...", (03 December 2015), *Daily Sabah*, available at http://www.dailysabah.com/columns/ilnur-cevik/2015/12/03/pkk-trying-to-challenge-turkey-in-diyarbakir, (accessed 17 January 2017).

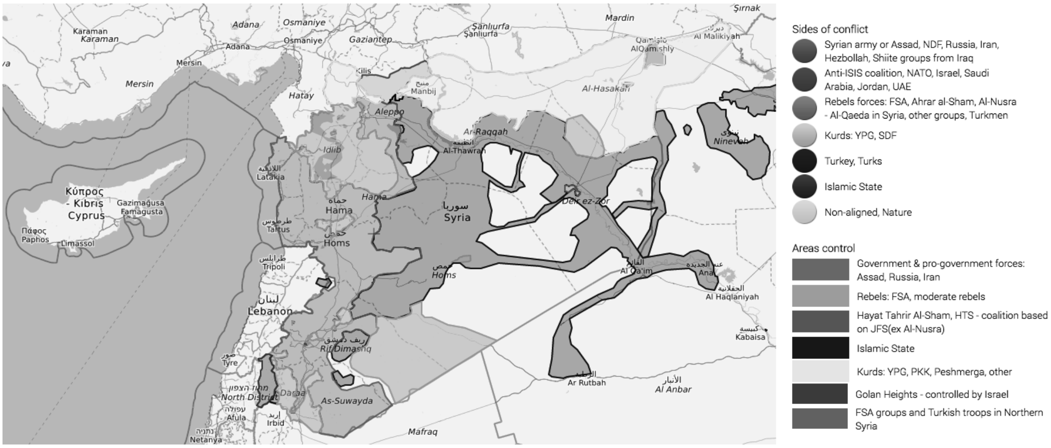
Adana
Osmaniye
Şanlıurfa
Mardin
Şırnak
Karaman
Gaziantep
Al Malikiyah
Qamishly
Mersin
Kilis
Manbij
Al-Hasakah
Hatay
Aleppo
Ar-Raqqah
Al-Thawrah
Nineveh
Idlib
Latakia
Κύπρος - Kıbrıs Cyprus
Gazimağusa Famagusta
Πάφος Paphos
Limassol
Hama
Syria
Deir ez-Zor
Tartus
Homs
Tripoli
Al Qa'im
Anah
Al Haqlaniyah
Lebanon
Kabaisa
Rif Dimashq
Tyre
Ar Rutbah
Al Anbar
North District
Daraa
As-Suwayda
Afula
Irbid
Netanya
Mafraq
Sides of conflict
Syrian army or Assad, NDF, Russia, Iran, Hezbollah, Shiite groups from Iraq
Anti-ISIS coalition, NATO, Israel, Saudi Arabia, Jordan, UAE
Rebels forces: FSA, Ahrar al-Sham, Al-Nusra - Al-Qaeda in Syria, other groups, Turkmen
Kurds: YPG, SDF
Turkey, Turks
Islamic State
Non-aligned, Nature
Areas control
Government & pro-government forces: Assad, Russia, Iran
Rebels: FSA, moderate rebels
Hayat Tahrir Al-Sham, HTS - coalition based on JFS(ex Al-Nusra)
Islamic State
Kurds: YPG, PKK, Peshmerga, other
Golan Heights - controlled by Israel
FSA groups and Turkish troops in Northern Syria

Figure 3: Map[72]

Compared to previous years, the PKK started using suicide bombers at an unprecedented rate in 2016. Many of these terrorists were uneducated and young Kurdish people who had been abused by the PKK. In addition to their usual method of targeting military/police establishments in rural areas with these suicide bombers, they have started to target state military/police buildings in urban areas as well as public areas in big cities that are crowded and frequently used by civilians in their daily routine. Especially for its sensational attacks in big cities, where civilian casualties fuel fear in public, PKK used proxy organizations and names to mislead public perception.[73]

PKK's most decisive strategic decision was the initiative to start urban conflict. Especially at the beginning of 2016, the PKK tried to accelerate its armed activities in some highly populated towns and city centers including Diyarbakır, Şırnak, Mardin, and Hakkari. To be able to create havoc in public, PKK members dug trenches, erected barricades, fired at security forces and exploited civilians as shields. For the PKK, prolonging the conflict was the key to being successful. This would enable the organization to have enough time to seek for foreign political support.

To restore public order, curfew was imposed in particular cities in the southeastern part of Turkey. Following the curfew, Turkish security forces (including mainly gendarmerie and police forces) launched operations at these urban areas to clean out the terrorists. Curfew operations took substantial time to finish; some of them lasted more than three months, considering that security forces paid a lot of attention to avoiding civilian casualties and collateral damage. However, the

[72] Available at https://syria.liveuamap.com (accessed 10 February 2017).

[73] Benjamin Harvey and Onur Ant, "PKK-Linked Group Tak Claims Istanbul Bombing That Killed 38", (11 December 2016), *Bloomberg*, available at https://www.bloomberg.com/news/articles/2016-12-11/turkey-says-signs-show-pkk-probably-behind-istanbul-bombings, (accessed 18 January 2017); See also Ceylan Yeginsu, "Bomb in Istanbul Killls 11 Near Tourist District", (07 June 2016), *New York Times*, at https://www.nytimes.com/2016/06/08/world/europe/istanbul-turkey-bomb.html (accessed 18 January 2017).

security forces, together with the support of the local population, performed well and knocked the terrorist organization out of the urban areas. The PKK has long been willing to start urban havoc and it showed its ability to exploit regional crises, but due to lack of support from the local population, the terrorist organization failed to achieve its long-term plans in the southeastern part of Turkey. However, this does not mean that PKK will not plan to carry out 'urban conflict' in the future. This situation will become clearer as the Syrian Civil War ends.

From the time it was established, the PKK has changed its name several times (KADEK, KONGR-GEL, KKK). Lastly in 2007, KCK has been established as a multidimensional entity to put into practice the long term plan to create an independent Kurdish state by claiming territories from Turkey, Iran, Iraq, and Syria. For this reason, PKK's and KCK's organic and hierarchical links are important to understand the PKK-PYD ideological relationship in Syria. While the KCK organizes the ideological, social, political, economic plans of the PKK as a whole, different armed wings of the organization conduct armed assaults in both Turkey and in the neighboring countries: the YRK in Iran, the PYD in Syria, and the HPG in both Iraq and Turkey.[74] In the light of this information, although the PKK's strategy is very fragile and is closely linked with the result of the Syrian Civil War, it is obvious that it is adopting changing strategies, depending on the regional crisis. Although these strategies are not planned in detail or long-lasting, they somehow have allowed the organization to survive thus far. For this reason, in the light of the model applied here, the PKK qualifies as a terrorist organization that has a strategy.

As for the degree of organization and cohesion, the PKK is more than organized crime. Deadly and savage attacks can obviously have greater impact on the population targeted, but this can alienate the popular support an armed organization has.[75] For this reason, the PKK uses proxy organizations (armed groups) in its deadly attacks: the YPS (Civil Protection Units), the TAK (Kurdish Freedom Falcons), and the OSB (Self Defense Units).[76] Apart from that, the most basic and 'core' unit structure of the PKK is a squad size, ranging from five to eight terrorists composing an IED specialist, sniper, RPG-7 carrier and machine gun carriers. These units work in their areas of responsibility that are clearly divided by the upper echelon of the terrorist group. Although the way they communicate with each other and with their superiors is very limited (because they use two-way radio for communication, nearby Turkish troops can easily detect their location via signal tracking systems), they use code words and ciphers, with limited transmission. They generally wear the same type of clothes. In the light of the model applied in this research, the PKK resembles the type of an organization that is termed 'middle' (does not have conventional military skills but is more than an organized criminal group) in the model of Huovinen.

[74] See official page of the Ministry of Foreign Affairs for basic description of the organizational and non-linear structure of the terrorist organization with other organizations, at: http://www.mfa.gov.tr/pkk.en.mfa,

[75] Christopher O. Bowers, "Identifying Emerging Hybrid Adversaries", p. 44.

[76] "PKK's Organization Game", (18 March 2016), *Anadolu Agency*, available at http://aa.com.tr/en/todays-headlines/pkks-organization-game/539390. (accessed: 18 March 2016).

As for the leadership; since Öcalan's imprisonment in 1999, the PKK has gone through several leadership and pathway crises, especially at the beginning of the 2000s. Öcalan still represents the symbolic leadership of the KCK. Considering that Öcalan's life in the prison is always under scrutiny by Turkish intelligence, he cannot actively take part in the political life of today's PKK. Today, Cemil Bayık is the head of KCK's executive council.[77] Murat Karayılan, Duran Kalkan, Sabri Ok are the other known figures, who take part in the KCK's executive council, along with some other old-hand terrorists. It is no longer a secret that, following the general elections in Turkey on 1 November 2015, Öcalan criticized the PKK for continuing armed resistance without listening to the Kurdish people's needs while conducting armed assaults. [78] In his previous interviews with journalists, Bayık said that neither the HDP nor Öcalan can decide PKK's disarmament. This decision will be given by the KCK itself.[79] The PKK still accepts Öcalan as their only leader. They use Öcalan's posters to decorate their walls and flags, and quote his ideas. Although Öcalan and KCK leaders have a different agenda,[80] this has not reached a level of a 'make or break' point for the PKK. On the other hand, the PYD's announcement that they have changed the name of 'Menagh Air Base'[81] (PYD seized the control of the Syrian Air Base on 18 February) to "Serok Apo" (Leader Apo) shows Öcalan's popularity and leadership in the KCK. Additionally, in the long run, the political future of the PYD's leading figure Salih Muslim and his relations with the KCK Council stands as an important determinant for the future organizational structure of the PKK. As a result, it can be said that the PKK has multiple leaders who are responsible for different agendas within the organization. However, their command structure seems limited. For sure, the reason why the leaders have different agendas has a considerable impact on the morale of individual terrorists. In the coming period, if this difference grows, this may result in separations within the PKK itself. In the light of these evaluations, the PKK's position, in the model applied in this research, seems somewhere between 'multiple leaders and limited command structure'.

Although the terrorist organization was been established in Turkey in the 1970s, it found a considerable space in neighboring countries in the 1990s. Following the founding of the PKK, the terrorist organization exploited the Iran-Iraq war to expand its structure and weapon stocks.[82] The capture of Öcalan by Turkish Special Forces in Kenya and the following successful cross-border

[77] Bese Hozat (a female terrorist) also shares the title: 'head of the executive council' with Cemil Bayık in the lists of PKK. But this seems like an 'eyewash' since Cemil Bayık takes part in every public speech and announcement. Also, the the expressions of the captured/surrendered terrorists acknowledges this opinion.

[78] "Öcalan'dan HDP ve PKK'ya eleştiri", (07 November 2015) ,BBC Türkçe, available at http://www.bbc.com/turkce/haberler/2015/11/151107_ocalan_elestiri, (accessed 06 April 2016); See also "Öcalan PKK'yı Eleştirdi", Milliyet, (24 December 2015).

[79] Mahmut Hamsici, "Bayık: Artık Tek Taraflı Ateşkes Olmayacak", (30 October 2015), *BBC Türkçe*, at http://www.bbc.com/turkce/haberler/2015/11/151130_bayik_mulakat_1, (accessed: 06 April 2016).

[80] "PKK 'not listening' to Öcalan: Turkish Official", (26 February 2016), *Yahoo News*, at https://www.yahoo.com/news/pkk-not-listening-ocalan-turkish-official-180554061.html, (accessed: 07 April 2016).

[81] "Times: YPG, Minnağ Hava Üssünün adını 'Serok Apo' yaptı". (18 February 2016), *BBC Türkçe*, at http://www.bbc.com/turkce/haberler/2016/02/160218_minnag_times, (accessed: 07 April 2016).

[82] Nigel Ashton and Bryan Gibson, The Iran-Iraq War: New International Perspectives, (Routledge, 2013, Abingdon), pp. 132-138.

operations of the Turkish Armed Forces made the organization go through a crisis at the beginning of 2000s. However, the US intervention into Iraq, resulting in the overthrow of Saddam Hussein in 2003, created an authority gap in Iraq. This provided PKK a considerable area of influence, especially in northern of Iraq. Although Iraq is not classified as a 'foreign state sponsor of the PKK, it is obvious that the political instability in Iraq had a positive indirect effect on the long-term existence of the organization. Today, none of the states in the international arena have taken over foreign state sponsorship of the PKK. For this reason, the PKK's relations with foreign states or other organizations do not meet the requirements of a 'foreign state sponsor' sub-variable. However, the acts of arming the PYD by the countries intervening in the Syrian Civil War is ascribed by Turkish officials as having a direct contribution to the efforts of PKK in the long run. In addition to that, BBC has uncovered details of a "secret deal that let hundreds of DAESH/ISIL fighters and their families escape from Raqqa, under the gaze of the US and British-led coalition and PYD forces that control the city."[83] Collaboration between DAESH/ISIL and PKK/PYD in this situation increases the chances that DAESH/ISIL, in the likely future, will try to use PKK networks both in Turkey and in Europe. As these terrorist organizations become non-state sponsors of each other, foreign fighters who have been fighting for ISIL/DAESH or PKK/PYD in Syria, will be moving comfortably between Syria and Europe and this will pose a severe threat to NATO's security.

C- Complex Terrain

In light of the model that is applied in this article, the last core variable taken into account is 'complex terrain'. In this core variable, 'human', 'geography' and 'cybercapabilities' form the level of complexity of the 'terrain'. Human terrain examines the relationship between the insurgent/terrorist group and the people whom the armed group claims to represent. Geographical terrain focus on the convenience of the geographical feature of warfare and cyberspace analyzes efficiency of a potential hybrid adversary in using cybercapabilities as a threat.[84]

Turkey shares 384 km of border with Iraq, 911 km with Syria, and 550 km with Iran. Except a small portion of the Syrian border, Turkey's borders with these countries have a mountainous character – covered with blocks of huge rocks, trees and deep stream beds. Such geography allows both terrorists and smugglers to infiltrate into the country despite many prevention efforts that Turkish military takes. In time, the PKK has become very experienced in using the geography for its own interests. The PKK has been using fortified networks of caves and tunnels, shelters and underground bunkers for a long time to deploy its logistical equipment and terrorists. Additionally, the majority of the mountains and the valleys the PKK uses are densely forested and can help the terrorists move unobserved. Such geographic features in the eastern part of Turkey and the northern part of Iraq

[83] Quentin Sommerville and Rian Dalati, "Raqqa's Dirty Secret", (13 November 2017), *BBC News*, available at http://www.bbc.co.uk/news/resources/idt-sh/raqqas_dirty_secret, (accessed 13 November 2017).

[84] Christopher O. Bowers, "Identifying Emerging Hybrid Adversaries", p.45. See also Petri Oskari Huovinen, "Hezbollah and Taliban; Hybrid Adversaries in Contemporary Conflicts", National Defense University, (2013), p. 55.

contribute to PKK's efforts on a tactical level. Terrorists take advantage of the rough, bumpy mountains to set up an ambush for security forces, with IEDs in particular. Moreover, the geographical layout makes the PKK's work easier for hit-and-run tactics when terrorists attack military bases. They utilize stream beds as a cover against UAVs when escaping. In years, as the Turkish Army acquired and produced advanced military technologies, the PKK's mobility and privacy in terrain has decreased significantly. In response to that, the PKK changed their operational terrain from mountains to urban areas, hoping that Turkish security forces will have difficulty combating them.

While the dream of 'urban chaos' whet the appetite of the terrorist organization, it requires a complex form of counterterrorism strategy, which the security forces want to avoid. Cities are places where crowded human populations live together and this provides a terrorist organization with very good cover and concealment. For approximately ten months, the PKK tried to take advantage of the geographical features and architectural structure of cities as a deadly weapon against the Turkish security forces following the breakdown of the so-called 'peace process'. Everything that is accepted as routine in a house or in a street like a cooking pot, doorknob, wall fence or paving stones have been used as deadly weapons by the terrorists. Despite the fact that security forces had a high number of casualties at the beginning of curfew operations, they gained experience in later weeks and months. The PKK could not maintain its strategy successfully and turned to the old one, where mountains were the primary zone of conflict. However in general terms it must be admitted that the PKK terrorist organization meets the requirements of hybridity under the sub-variable 'geographic terrain'.

The most important reason behind PKK's failure in its 'urban chaos' strategy was the lack of support from the Kurdish people for the organization. At this point, 'human terrain' needs to be analyzed in the light of the population support. So far, the PKK has recruited terrorists in two ways: either they brainwashed young and vulnerable Kurds or they forced and threatened people to join the PKK. In the public eye, such activities of the PKK decreased its popularity and created a repulsive image of the terrorist organization. Kurdish people living in the eastern part of Turkey were satisfied after the 'democratic reforms' that the government has carried out since the 2000s. Original Kurdish village names were restored and the ban on the letters q, w and x- used in Kurdish but not in Turkish- were lifted. Economic reforms have been made and first Kurdish language radio and television broadcasting channels (TRT-Kurdi), as part of the Turkish Radio and Television Corporation (TRT), have been established as part of the democratic reforms. Lastly, the Peoples' Democratic Party (HDP), which is generally seen as a party representing Kurdish people, surpassed the 10% threshold needed to enter the parliament in both of the elections in 2015. Although there were such democratic reforms and changes, the PKK never laid down its arms and continued its illegal activities like smuggling, arms trafficking and collecting extortion from local nomads and merchants.[85] Following the general elections in November 2015 in Turkey, the PKK accelerated its

[85] "PKK Kendi Maliyesini Kurdu Vergi Topluyor", (23 July 2013), *Sözcü*, available at http://www.sozcu.com.tr/2013/gundem/pkk%E2%80%88kendi-maliyesini-kurdu-vergi-topluyor-340306/ , (accessed 23 March 2016).

armed activities by carrying the conflict into urban areas. This strategy was brought to the table by the PKK, assuming that the local population would support it. This way, the PKK was planning to abuse 'human terrain to organize local people for 'civil disobedience'. According to this plan, all places including houses, streets, public places and etc. are reshaped to create a convenient battlefield. Some people have been forced to leave their houses or have been forced to help the organization, some others have been used by terrorists as human shields by the PKK.[86] As a result, the growing hatred for PKK has increased and the organization never found the necessary population support in times of its activities.[87]

Lastly, speaking of PKK's cyberspace capabilities, we need to point out the fact that drone usage by terrorist groups has become very common. ISIL/DAESH has shown the latest examples of 'unconventional' use of drones by dropping grenades and poisonous gas over the military bases in Syria. However, the PKK has not reached such a level of use of drones in targeted killing or suicide bombing. However, reports from the security forces have shown that the PKK has started using drones for surveillance activities, especially of military bases near the Iraq/Syria border of Turkey.

The PKK's cybercapabilities are restricted. The PKK, just like Taliban,[88] uses the internet frequently for recruitment and propaganda activities and uses social media platforms to gather open source intelligence for target detection. In addition to that, there were several low-level attempts by PKK to hack the official websites of some of the governmental institutions in the past. However, the PKK's cybercapacity is not so developed that it could penetrate any of the governmental or military classified information networks. For this reason, there is no evidence that the PKK possesses or will likely to possess hybrid level cyber capabilities defined in Bowers's model in the future.

Conclusion

The conflicts that took place in Crimea and Lebanon in the last decade proved that hybrid war encompasses different dynamics of interaction at the operational level compared to its counterparts like unrestricted warfare, compound warfare and irregular warfare. Hezbollah's success to conduct hybrid warfare and ISIL/DAESH's demonstration of hybrid capabilities during its expansion in Iraq and Syria in 2014 meant that these types of wars/conflicts have become a model for other terrorist organizations. In this context, the PKK's changing policy and adaptation of new tactics is so important that it poses a set of unique challenges to Turkey and also NATO's Southern Flank, as well. For this reason, PKK's hybridity has been evaluated within Huovinen's model (Huovinen modified

[86] "Turkish Foreign Minister Accuses PKK of Using Civilians as 'Human Shields'", (07 February 2016), *Sputnik News*, available at https://sputniknews.com/middleeast/201602071034351356-kurds-civilians-shield/, (accessed 07 February 2016).

[87] Galip Dalay, "PKK's War of Choice Lacks Kurdish Public Support in Turkey", (04 January 2016), *Middle East Eye*, at http://www.middleeasteye.net/columns/pkk-s-war-choice-lacks-public-support-turkey-1494317341 (accessed 24 February 2016).

[88] Petri Oskari Huovinen, "Hezbollah and Taliban; Hybrid Adversaries in Contemporary Conflicts", p. 79.

Bowers's model) under three core variables: capability, maturity and complex terrain. In general, although the PKK has shown important tactical shifts, it does not fit the definition of a 'hybrid adversary' as it does not meet the requirements of several important sub-variables.

First of all, although PKK has not been experiencing problems for the last couple of years about the training and sustainability sub-variables, its capability under the weapon sub-variable is still limited. However one must take into account the fact that the PKK has been increasing its activities both in Syria and in Iraq to take advantage of the crisis in these countries. Especially the PYD's territorial gains in Syria and the support (supply of armed vehicles, weapons, ammunitions) given by some coalition countries to PYD have the potential to be exploited by the PKK.

On the other hand, the fact that the PKK has been experiencing problems in finding a permanent partner for sponsoring its activities (its sponsors are variable and changing) have decreased its chance to become a hybrid threat in the near future. This is the most important obstacle that the PKK faces on its way to hybridity under maturity variable of the model.

The most important character of PKK's overall policy change was its decision to call to the public for civil disobedience and its endeavor to carry the armed conflict into city centers. The PKK wanted to use this as a 'domino effect' for its further activities on the way to establishing an independent Kurdish state. Therefore, the PKK has satisfied the geographical terrain sub-variable. However, due to the lack of public support (human terrain) in the eastern part of Turkey following its 'urban chaos' strategy and its insufficiency in cyberspace capabilities, the PKK has failed to meet the standards of a hybrid adversary in the complex terrain variable as a whole.

In the likely future, the PKK will probably try to find a foreign state sponsor that supports its territorial ambitions. To reach that aim, the terrorist organization may try to launch the 'urban chaos' strategy again, but this time seeking the support of the majority of the local population. Although these factors are very important for PKK's future capabilities, today the organization cannot qualify as a "hybrid adversary".

BIBLIOGRAPHY

"ABD Savunma Bakanı Ashton Carter ile Senatör Lindsey Graham: PKK / PYD - YPG konusu", (29 April 2016), *Youtube*.

Andrew, Self, and Jared, Ferris, "Dead Men Tell No Lies: Using Killed-in-Action (KIA) Data to Expose the PKK's Regional Shell Game", *Defense Against Terrorism Review* 8, 2016.

Ashton, Nigel and Gibson, Bryan, *The Iran-Iraq War: New International Perspectives*, (Routledge, 2013).

Baumann, Robert F., "Compound War Case Study: The Soviets in Afghanistan", (Thomas Huber ed. The Fatal Knot), 2002.

Bostan, Yahya, "US Supplied PYD weapons found at PKK hideouts in northern Iraq", (16 October 2015), *Daily Sabah*.

Bowers, Christopher O., "Identifying Emerging Hybrid Adversaries", *PARAMETERS*, 2012.

Byman, Daneil and Saab, Bilal Y., "Hezbollah In a Time Of Transition", (Center for Middle East Policy at Brookings, Atlantic Council, November 2014).

"Cobra ve Cougar'ı PKK Füzesi Vurdu", (07 June 1997), *Sabah*.

Curtis, Glenn E. and Karacan, Tara, "The Nexus Among Terrorists, Narcotics Traffickers, Weapons Proliferators, And Organized Crime Networks in Western Europe", (West European Nexus, Federal Research Division of Library of Congress, December 2002).

Cunningham, Erin, "Kurdish Militants Reportedly Shoot Down Turkish Security Forces Helicopter", (14 May 2016), *Washington Post*.

Çevik İlnur, "PKK trying to challenge Turkey in Diyarbakır...", (03 December 2015), *Daily Sabah*.

Dalay, Galip, "PKK's War of Choice Lacks Kurdish Public Support in Turkey", (04 January 2016), *Middle East Eye*.

Davis Jr., John R., "Continued Evolution of Hybrid Threats: The Russian Hybrid Threat Construct and the Need for Innovation", *The Three Swords Magazine* 28, 2015.

Early, Bryan R., "Larger Than a Party, yet Smaller than a State: Locating Hezbollah's Place Within Lebanon's State and Society", *World Affairs* 168(3), 2006.

Exum, Andrew, "Hezbollah at War: A Military Assessment", *Policy Focus* (63), *The Washington Institute Fo Near East Policy*.

Fox-Brewster, Tom, "Russian Malware Used by 'Privateer' Hackers against Ukrainian Government", (25 September 2014), *The Guardian*.

Gerasimov, Valery, "The Value of Science for the Future", *Military-Industrial Kurier*, 8(476), 2013.

Glenn, Russel W., "Thoughts on 'Hybrid' Conflict", *Small Wars Journal*, 2009.

Hastings, Deborah, "At least one person crushed to death in Ukrainian stampede; Putin orders massive military exercises", (26 February 2014), *New York Daily News*.

Harvey, Benjamin and Ant, Onur, "PKK-Linked Group Tak Claims Istanbul Bombing That Killed 38", (11 December 2016), *Bloomberg*.

Hamsici, Mahmut, “Bayık: Artık Tek Taraflı Ateşkes Olmayacak”, (30 October 2015), *BBC Türkçe*.

Hendawi, Hamza, “Israel: Hezbollah Drone Attacks Warship”, *The Washington Post*, 14 July 2006.

Hoffman, Frank G., “Hybrid vs. Compound War: The Janus Choice: Defining Today’s Multifaceted Conflict”, *Armed Forces Journal*, 2009.

Hoffman, Frank G., “Hybrid Warfare and Challenges”, *Joint Forces Quarterly 52*, 2009.

Hoffman, Frank G., “Conflict In the 21st Century: The Rise of Hybrid Wars”, (Potomac Institute For Policy Studies And The Center For Emerging Threats and Opportunities, Arlington, 2007).

Huber, Thomas M. *Compound Warfare: The Fatal Knot*, (U.S. Army Command and General Staff College Press, Fort Leavenworth, 2002).

Hunter, Eve, and Pernik Piret. “The Challenges of Hybrid Warfare”, *International Centre For Defense And Security*, 2015.

Huovinen, Petri Oskari, “Hezbollah and Taliban; Hybrid Adversaries in Contemporary Conflicts”, (Published MA Thesis, National Defense University, Finland, 2013).

Iddon, Paul, “Pressure mounts on PKK over Sinjar presence”, (27 December 2016), *Al Monitor*.

James, Carolyn C. and Özdamar, Özgür, “Modeling Foreign Policy and Ethnic Conflict: Turkey’s Policies Towards Syria”, *Foreign Policy Analysis* 5, 2009.

Kiras, James D. et al, *Irregular Warfare: Terrorism and Insurgency “Strategy in the Contemporary World”*, (Oxford University Press, 2013).

Kofman, Michael and Rojansky, Matthew, “A Closer Look At Russia’s ‘Hybrid War’”, *Kennan Institute Wilson Center* 7, 2015.

Liang, Qiao and Xiangsui, Wang, *Unrestricted Warfare*, (PLA Literature and Arts Publishing House, 1999).

Malyarenko, Tatyana, “Playing a Give-Away Game? The Undeclared Russian-Ukrainian War in Donbas”, *Small Wars Journal*, 2015.

McCuen, John. J., “Hybrid Wars”, *Military Review,* 2008.

McCuulloh, Timothy and Johnson, Richard, “Hybrid Warfare”, (Joint Special Operations University Report 13(4), August 2013).

Mumford, Andrew, “The Role of Counter Terrorism in Hybrid Warfare”, (CEO-DAT, November 2016).

“Öcalan’dan HDP ve PKK’ya eleştiri”, (07 November 2015), *BBC Türkçe*.

Pawlak, Patryk, “Understanding Hybrid Threats”, (European Parliamentary Research Service, June 2015).

“Pentagon condemns display of PKK symbols in Raqqa”, (20 November 2017), *TRT World*.

Piotrowski, Marcin Andrzej, “Hezbollah: The Model of A Hybrid Threat”, *The Polish Institute of International Affairs Bulletin* 24(756), 2015.

“PKK”, Republic of Turkey Ministry of Foreign Affairs.

“PKK Kendi Maliyesini Kurdu Vergi Topluyor”, (23 July 2013), *Sözcü*.

“PKK ‘not listening’ to Öcalan: Turkish Official”, (26 February 2016), *Yahoo News*.

"PKK's Organization Game", (18 March 2016), *Anadolu Agency*.

"Putin reveals secrets of Russia's Crimea takeover plot", (09 March 2015), *BBC*.

"Russia leader Vladimir Putin says he'll protect Russians in Ukraine by any means, but hopes force not required", (04 March 2014), *CBS News*.

"Russian Senators vote to use stabilizing military forces on Ukrainian territory", (01 March 2014), *Russia Today*.

"Russian support for PKK's Syrian Arm PYD", (27 November 2015), *Anadolu Agency*.

Said, Rodia, "Syrian Kurds set to announce Federal System in northern Syria", (16 March 2016), *Reuters*.

Salem, Harriet, et. al., "Crimean parliament seized by unknown pro-Russian gunmen", (27 February 2014), *The Guardian*.

Schiff, Ze'ev, "Hezbollah Listened in on IDF Beepers Cell Phones", (04 October 2006), *Haaretz*.

Snegovaya, Maria, "Putin's Information Warfare In Ukraine", *Institute For The Study of War*, 2015.

Sommerville, Quentin and Dalati, Riat, "Raqqa's Dirty Secret", (13 November 2017), *BBC News*.

Simpson, Erin M., "Thinking About Modern Conflict: Hybrid Wars, Strategy, And War Aims", (Paper presented to the Annual Meeting of the Midwest Political Science Association Chicago, IL, 7-11 April 2005).

Temizer, Selen, Süleyman, Halit and Tok, Levent, "PKK/PYD captures 8 villages in Syria's Aleppo province", (17 November 2016), *Anadolu Agency*.

"Times: YPG, Minnağ Hava Üssünün adını 'Serok Apo' yaptı". (18 February 2016), *BBC Türkçe*.

"Turkey's Erdogan denounces US support for Syrian Kurds", (10 February 2016), *BBC*.

"Turkish Foreign Minister Accuses PKK of Using Civilians as 'Human Shields'", (07 February 2016), *Sputnik News*.

"USA: PYD is not a terrorist organisation, they are our friends and we support them", (10 February 2016), *Youtube*.

von Bruinessen, Martin, *Kurdish ethno nationalism versus nation-building states*, (The ISIS Press, 2000).

"We did what we had to do: Putin opens up on Crimea reunification plan", (10 March 2015), *Russia Today*.

William J., Nemeth, "Future War and Chechnya: A Case For Hybrid Warfare" (Published MA Thesis, Naval Postgraduate School, Monterey, 2002).

Yeginsu, Ceylan, "Bomb in Istanbul Kills 11 Near Tourist District", (07 June 2016), *New York Times*.

"YPG not a terrorist organization for US, spokesman says", (22 September 2015), *Hürriyet Daily News*.

This Page Intentionally Left Blank

DATR, 2017; 9: 35-46

ISSN 1307 - 9190

Hacking Back Against Cyberterrorists: Could you? Should you?[1]

Alan BRILL[2]

Jason SMOLANOFF[3]

Abstract: *Cyberterrorists have become adept at using cybertools to modify or deface websites, steal information, and use social media. It is also expected that they will increasingly use the tools and techniques developed and used by cybercriminals, which are widely available. Add to this the nation-state-level tools released by sources like Wikileaks, and it becomes obvious that cyberterrorists are gaining increasingly sophisticated and dangerous weaponry. When an organization – whether that organization is part of a nation's critical infrastructure or not, and whether that organization is part of a nation's public or private sector, is attacked, a natural reaction to that attack is a desire to identify the attacker and to launch a counterattack. This desire is no different in the warfighting domain of cyberspace than in the real world. But is it a good idea? Are there differences between this kind of counterattack if carried out by a private sector organization or a government agency? In this article, the authors look at the potential advantages and risks associated with what's called 'hacking back', and conclude that the risk/reward equation can be complex and must be carefully considered before taking action.*[4]

Key Words: *Cyberterrorism, Hacking back, Cyberwarfare, International Law, Critical Infrastructure.*

[1] Submitted on 18 August 2017. Accepted on 05 October2017.

[2] *Senior Managing Director, Kroll Cyber Security, New York and Adjunct Professor, Texas A&M University School of Law, Fort Worth, Texas. e-mail: abrill@kroll.com*

[3] *Senior Managing Director, Kroll Cyber Security, Los Angeles and Adjunct Professor, Loyola Law School. e-mail: jason.smolanoff@kroll.com*

[4] This article, which was specifically written for Defense Against Terrorism Review, is based, in part, on prior research carried out and published by the co-authors including Mark Raymond, Greg Nojeim, and Alan Brill, "Private Sector Hack Backs and the Law of Unintended Consequences," Center for Democracy and Technology (December 15, 2015), available at https://cdt.org/insight/private-sector-hack-backs-and-the-law-of-unintended-consequences/ on (accessed 31 July 2017); see also Alan Brill and Jason Smolanoff, "When You Have Suffered a Data Breach, Attribution may be Useful, But Hacking Back? Not So Much", *Florida Bar Association International Law Quarterly*, (Spring 2017).

Introduction

Unauthorized intrusions into computer-stored and computer-processed data, with theft of information, encryption or destruction of data and release of stored data (Wikileaks being an example) has, unfortunately, become commonplace, with victims in both the public and private sectors. Once an incident is identified, investigators often try to determine the identity – or at least the network location – of the hackers. What if a government or organization could launch an counterattack directed against the hacker? While such an action – called 'hacking back' – might seem to be a simple matter of justice, the problem is more complex than it appears.

Imagine that you are the duty officer in your nation's cyberincident reporting and response center, and you receive an urgent email message from the Chief Information Security Officer (CISO) of a power generation and distribution company that is an important part of your nation's critical infrastructure.

The message states that the database containing crucial information about the company's industrial control systems, the configuration of those systems, the hardware and software in use, and the security measures used to protect those crucial systems from attack and compromise was compromised, with sensitive information uploaded to servers believed to be under the control of the attackers. It further states that the CISO has traced back the source of the attack to a non-state actor, a terrorist group located in an unfriendly nation in your region.

The message states that the company is preparing to launch a cybercounterattack to attempt to both destroy the stolen data before it can be misused and to 'teach them not to attack us in the future' by damaging the terrorist's information technology infrastructure. (The use of hacker tools and techniques to reach into the infrastructure of an attacker is called 'hacking back.') They are finalizing their plans and the computer code necessary to carrying out the attack, and they expect to launch their counteroffensive in approximately one hour. What should you do?

Hacking Back

This scenario, while artificial, is not unrealistic. Hacking back against attackers has been an area of interest to both governments and private sector organizations in recent years. In the United States, for example, bills have been introduced in Congress to legalize private-sector hack-backs – effectively immunizing corporations from prosecution under U.S. law for what would otherwise be criminal hacking (potentially subjecting the corporation and its employees to criminal charges and imprisonment). Do such laws make sense? Are they workable when the Internet is global, and attacks (and counterattacks) can traverse physical space and hardware of multiple nations as they travel through cyberspace?

From the viewpoint of terrorist organizations, the use of cyberspace is highly attractive. It is highly asymmetric. Great damage can potentially be caused by a few talented men or women. It also usually represents a form of attack that can be carried out remotely. There may well be no need to have people cross borders or take physical actions in the target nations.

Cyberattacks are also subject to various forms of obfuscation designed to obscure that true source of the attack. During a presidential campaign debate in September 2016, then Republican presidential candidate (now President of the United States) Donald J. Trump, acknowledged this. Discussing the hacking of the Democratic National Committee and of senior officials of then Democratic presidential candidate Hillary Clinton, while the U.S. intelligence community had concluded with "high confidence" that Russian military intelligence service operators were behind those attacks, candidate Trump said "Maybe it was. It could be Russia, could also be China, could also be lots of other people. Could also be someone sitting on their bed who weighs 400 pounds, okay? "[5]

Obviously, because of data classification, we do not know the evidence that was behind the US intelligence community's evaluation. But Trump was certainly correct in saying – whether it was true in this particular case of not – that definitive attribution of an attack is very difficult.

Simply put, the Internet was never designed to provide positive authentication or identification of the information that traverses it. This fact was made famous in a cartoon by Peter Steiner which appeared in The New Yorker magazine on July 5, 1993. In the cartoon, a dog sitting in front of a computer is talking to a dog sitting on the floor next to the desk. The dog sitting at the computer says "On the Internet, nobody knows you're a dog."[6]

The difficulty of attributing a cyberattack was extensively analyzed by Thomas Rid and Ben Buchanan in their paper, "Attributing Cyber Attacks" which appeared in the Journal of Strategic Studies in 2014.[7] What that article and many others that could be cited make clear is that from a technical and legalistic viewpoint, definitive attribution is difficult and may be impossible.

Consider that a hacker need not directly attack you. They can compromise an ineffectively protected computer in a public or private sector setting, and then can remotely control that computer to carry out their attack. Or they can establish a chain of compromised computers, putting multiple layers of machines – often in different countries, some of which may be hostile to the country in which the ultimate target exists – to make tracking down the real source of the intrusion much more

[5] Kevin Rose, "Trump Says that the DNC Hacker Could Be 'Somebody Sitting on their Bed Who Weighs 400 pounds'", (26 September 2016), *Fusion*, available at http://fusion.kinja.com/trump-says-that-the-dnc-hacker-could-be-somebody-sittin-1793862253 (accessed 05 May 2017).

[6] Glenn Fleishman, "Cartoon Captures Spirit of the Internet", (14 December 2000), *The New York Times*, available at http://web.archive.org/web/20141030135629/http://www.nytimes.com/2000/12/14/technology/14DOGG.html (accessed 05 May 2017).

[7] Thomas Rid & Ben Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies*, 38 (2015), pp. 1-2, 4-37.

difficult. They can also compromise machines to take over portions of their data storage so that stolen information can be stored in some unknowing third party's computer network. They may move copies of the stolen data around the world to assure their ability to access it while disguising that they are the ones who stole it. In fact, they may never actually store the stolen information on one of their own machines.

Add to this another layer of complication: The hacker (or hacking group/collective) that is actually carrying out an attack against you may not be the group underlying the attack. It has become known that nation-states and non-governmental groups can 'outsource' the actual technical operation of hacking to paid cybercriminals (or to supporters in nations unrelated to the actual location of the actual perpetrators) who carry out the attack, often, of course, using all of the tools of obfuscation at their command. Indeed, it is reasonable to believe that hackers (and those who sponsor such hacking) are fully aware of the potential actions their targets (or law enforcement acting on behalf of a target) may take to trace their activities. In fact, not only may an adversary take steps to make it difficult to attribute an attack to them, but in fact, may design the attack to cause suspicion to fall on actors or nations that actually have no involvement in the action.

This form of misdirection is not new. It is a version of 'false flag' tactics in the age of cybercrime. This form of deception has likely existed since biblical times. In regard to cyberspace, it has been defined as follows: "Cyber false flags refer to tactics used in covert cyberattacks by a perpetrator to deceive or misguide attribution attempts including the attacker's origin, identity, movement, and/or code/exploitation. It is typically very hard to conclusively attribute cyberattacks to their perpetrators and misdirection tactic can cause misattribution (permitting response and/or counterattack as a *condicio* 'sine qua non' under international law) or misperception which can lead to retaliation against the wrong adversary."[8]

Hacking Back: Private Sector Considerations

Government and military organizations can use any lawful form of warfare, including those involving cyberoperations. In fact, NATO has recognized cyberspace as a "domain of operations"[9] and nation-states must be prepared to deal with operations in that domain. It is also clear that private sector organizations must defend themselves against attacks. What is problematic is when private sector organizations consider launching offensive cyberoperations.

For attacks targeting organizations in the private sector, there are a number of issues that mitigate against carrying out such operations. This is not to say that senior executives in the private sector

[8] "False Flag," Wikipedia, at https://en.wikipedia.org/wiki/False_flag (accessed 31July 2017).

[9] Tomáš Minárik, "NATO Recognizes Cyberspace as a 'Domain of Operations' at Warsaw Summit", *CCDCOE Incyder* (21 July 2016), at https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html (accessed 31 July 2017).

who have been victims of cyberattacks would not be enthusiastic supporters of such actions, but that there are, regardless of their desires, potential roadblocks to doing so.

While this article is not intended to be a treatise on national or international law, it is important to understand that activities like hacking – and hacking back, may be regulated by law. For example, in the United States, federal law explicitly bans many of the retaliatory activities that companies might like to carry out (or, outsource to others to carry out.) The key law in the US is the Computer Fraud and Abuse Act (codified at 18 U.S.C.1030). The main points of this law were well described by Charles Doyle, Senior Specialist in American Public Law at the Congressional Research Service.[10] He identified seven major prohibitions set forth in this law:

- Computer trespassing (e.g., hacking) in a government computer. 18 U.S.C. 1030(a)(3)
- Computer trespassing (e.g., hacking) resulting in exposure to certain governmental, credit, financial, or computer-housed information. 18 U.S.C. 1030(a)(2)
- Damaging a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce (e.g., a worm, computer virus, Trojan horse, time bomb, a denial of service attack, and other forms of cyberattack, cybercrime, or cyberterrorism). 18 U.S.C. 1030(a)(5)
- Committing fraud, an integral part of which involves unauthorized access to a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce. 18 U.S.C. 1030(a)(4)
- Threatening to damage a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce. 18 U.S.C. 1030(a)(7)
- Trafficking in passwords for a government computer, or when the trafficking affects interstate or foreign commerce. 18 U.S.C. 1030(a)(6); and
- Accessing a computer to commit espionage. 18 U.S.C. 1030(a)(1).

While this law appears on its face to be limited in scope to governmental computers, bank computers and those used in, or affecting, interstate or foreign commerce, it must be recognized that because of the global reach of the Internet, virtually all computers are, at least arguably, accessible between U.S. states and between the U.S. and other countries. Thus realistically, this law covers virtually all computer systems.

There are other U.S. federal laws and state laws that prescribe criminal penalties for activities that these laws define as being criminal. In addition, as discussed below, carrying out these actions may provide a basis for a civil action (i.e. a lawsuit.)

[10] Charles Doyle, "Cybercrime: A Sketch of 18 U.S.C 1030 and Related Federal Criminal Law", *Congressional Research Service Report* 7-5700, 14 October 2014, available at https://fas.org/sgp/crs/misc/RS20830.pdf (accessed 31 July 2017).

When hackers operate from another country, the digital information that goes between their computers and their target's computers flows across legally defined international borders. By definition, for example, an Internet inquiry from a computer in France to a computer server in the U.S. must cross between France and the U.S. However, because the Internet provides global routing of messages and parts of messages, that signal does not necessarily go directly from France to the U.S. It's not unlike commercial air transportation. Sometimes you can get a non-stop flight from your originating airport to your destination airport. Other times, you might have to have flights that connect in intermediate cities or countries. For example, flying from New York to Istanbul, you could take a nonstop flight, but you could also take flights with changes of planes in Canada, France, Germany or many other countries.

Just as the laws of those countries apply while you are there, the laws relating to cybercrime may apply at the origination and destination, as well as the laws of countries through which the signals pass. This is made even more complex when it is recognized that the multiple packets which constitute a single message may travel over different paths, crossing into different countries as they travel between origination and destination. And the responses to those messages may travel over completely different paths, potentially involving additional nations.

Even if a country were to pass laws permitting private-sector organizations to hack back, such laws would in no sense provide immunity from the laws of other nations for such activity. For example, on May 25, 2017, U.S. Congress Member Thomas Graves introduced a bill called the "Active Cyber Defense Certainty Act" which would authorize certain hackback measures by private sector organizations and which would allow them to avoid prosecution under U.S. law that would otherwise be possible.[11] But no U.S. law can immunize against cyber-related laws in other countries. Were such a bill to be signed into law, and a company take action against a computer in France (which has a range of cybercrime laws), those who took the actions might be considered criminals under French law regardless of any immunity provided in U.S. law. Of course, there are many opposed to this bill, including Admiral Mike Rogers, who heads both the U.S. National Security Agency (NSA) and the U.S. Cyber Command. At a recent congressional hearing before Congress's Armed Services subcommittee, Admiral Rogers said "My concern is be leery of putting more gunfighters out on the street in the Wild West."[12]

Even in situations where some hackback action might not be defined as a criminal act, it might still result in a lawsuit brought under civil laws. And the lawsuit could be venued in a court in a location where the defendant has no operations. For example, if a hackback is alleged to cause damage to the computer of an innocent third party in the Republic of Korea, an action could be brought before a Korean court under the laws of South Korea. Defending such an action for a

[11] Tim Starks, "Scoop: 'Hack back' Bill Gets Version 2.0", (25 May 2017), *Politico* at http://www.politico.com/tipsheets/morning-cybersecurity/2017/05/25/scoop-hack-back-bill-gets-version-20-220506 (accessed 31 July 2017).

[12] Ibid.

company with no operations or personnel in Korea could be expensive and complex, with the need to instruct local counsel, the potential for being ordered to have executives and technical specialists travel for depositions or trial testimony, and potentially substantial judgements, such suits can be strong motivators not to engage in such behavior.

Even in cases where immunity is granted under local law, such immunity is unlikely to provide protection against private-sector-initiated lawsuits. Take for example, the case of two companies – we will call them Company One and Company Two – both located in the same nation.

Company One determines that they have been the target of an intrusion which resulted in the loss of both valuable intellectual property (trade secrets) and customer data, including credit and debit card information (often referred to as "personally identifiable information or PII".) An investigation provides information that identifies Company Two as the source of the hacking. Company One initiates action to see if it can find the stolen information on any servers within Company Two's systems. It does this using multiple techniques designed to hide Company One's identity.

Company Two's IT department receives a call from the company to which they had outsourced real-time computer security monitoring operations. The monitoring company reports that Company Two is under attack by actors trying to break into the Company Two network without authorization. Company Two's internal cybersecurity team verifies the report within minutes and informs management. Both external and internal analysts agree that the attack is coming from an IP (Internet Protocol) address in another country. Company Two's security staff assures management that it is not part of a drill or test that they are carrying out – it is the real thing.

With this information, management initiates its response plan. It assigns a number of IT security and IT operations employees to a special task force to address the attack. Through its insurance broker, it immediately notifies the issuer of its cyberinsurance that it is under attack, and requests authorization to bring in a forensic consulting firm that has been pre-approved by the insurer, and with which Company Two has a stand-by agreement in place. The insurer approves, and the forensic company is called in to assist. Company Two also notifies law enforcement that it is under attack.

At some point, Company One notifies Company Two of what is going on. They say that they now believe that Company Two was also a victim, but that they haven't been able to get into their network to verify that. They request access.

Company Two determines that it has spent the equivalent of US$ 50,000 on internal resources focused on dealing with the 'attack' and an additional US$ 25,000 on the forensic consultant. It asks Company One for reimbursement. The general counsel of Company Two, in a letter to Company One, points out that "had you chosen to approach us before you tried to hack us, we would have gladly cooperated with you and with law enforcement. But by hacking us – particularly through another country to hide your identity – you are, in our view, hackers yourselves, and you cost us

$75,000. You can pay it voluntarily and we'll consider the matter closed, or we will sue you for the money and call a news conference to explain it to the media."

Certainly, basic principles of justice would not suggest that Company Two should bear the financial burden of dealing with Company One's hackback. Even if Company One argues that they thought it was Company Two's fault, the alternative of contacting them and seeking cooperation should have at least been considered.

Companies worry about their reputations. As was pointed out in the earlier article published by the Center for Democracy and Technology,[13] a company's reputation could be hurt if it is revealed that in their quest to hack back, they caused disruptions in radiation therapy for pediatric cancer patients at a medical center whose computers had – without the hospital's knowledge or consent – been hacked by intruders who used it to attack another company. No company can afford to ignore the potential issues of reputational risk associated with hacking.

An increasing number of organizations have taken or are at least considering transferring some of their cyberrisk to insurance companies by purchasing what is referred to as "cyberinsurance." The contracts associated with these policies often require the company to coordinate actions taken in response to an attack or actual breach with the insurer. The insurer may well conclude that whatever claim they may face as a result of the incident will not be dependent on actually identifying the source of the hack, and may tell the insured that they will not cover the costs associated with identifying the source of the intrusion or any "hacking back" activity. This can certainly discourage any such actions, as the costs of those activities may well be substantial.

Terrorists can exploit hackback laws

A sophisticated terrorist group can use hackback laws to their advantage, although one might initially think that such laws would be used *against* terrorist cyberactors.

A smart cyberterrorist can use hackback laws to the terrorist group's advantage. They can launch attacks that are deliberately designed to be noticed, with the hope of encouraging targets to hack back, not against the terrorists, but against the organizations through which they launched the attack. The scenario of a company victimized by hackers by having its servers compromised and used for attacks, then being itself attacked by the terrorist group's ultimate target, is appealing. The target could be the subject of criminal charges, civil actions and reputational damage, all of which are objectives of the terrorist group behind the false flag attack.

Further, to the extent that such false flag attacks result in criminal or civil litigation, or bad publicity, potential attack targets will become 'gun-shy' of responding forcefully to an attack,

[13] Rid and Buchanan, "Attributing Cyber Attacks".

which again may be something helpful to the terrorists when they actually launch an attack on that target.

A terrorist organization often runs legitimate (or at least semilegitimate) front organizations. It is certainly possible for the group to select a target known to use hackback with the objective of having them do so and cause 'damages' for which they can demand compensation and threaten litigation and reputational damage. In fact, with good tradecraft in the form of attack obfuscation, perhaps by routing the attack through not only their own front organization systems (but also innocent third parties as well) the terrorists can win either by their attack being successful, or by reacting to hacking back by their intended victim – or both!

There is nothing to prevent a terrorist or terrorist-sympathizer organization from arranging an attack (perhaps by outsourced hackers) against a designated site under their control. Done right, the attack can appear to be – at least to some extent – launched from the terrorist group's intended target. Although that target may have no involvement, evidence can be manipulated to suggest otherwise. The terrorist group then engages in a 'hackback' to defend itself. Depending on jurisdictional issues, a carefully thought-through scenario could use a country's own hackback laws to immunize what is, in fact, an attack against a target by a terrorist group.

A terrorist group can use the fact that a victim hacked back in an argument (that might well work with the terrorist group's sympathizers) that the hackback makes them as much a victim as the original target. Manipulated evidence, falsified testimony and documentation can provide support for such claims. While bogus, these claims can lead to some people believing that the terrorist group is being targeted for unfair attack by the actual victim.

Should Governments Hack Back against Terrorists?

Of course, this consideration of the consequences of hacking back is focused on potential activities of private sector organizations. Do the same factors apply when a governmental entity is considering using hackback techniques as part of an investigation of an incident, or as part of an intelligence gathering operation?

The potential opportunity to use hacking back as a means of attack attribution, or of validating/disproving suspicions regarding who is behind an attack can be of great importance to a government organization. The means of doing hackbacks are well known, and it is expected that resources with such knowledge will be available to the agency involved.

The risks associated with hacking back – like misidentification of the source of an incident, or potential damage (technical, financial) to an innocent third party – are no different for a public sector entity hackback than for a private sector hackback operation. We believe that for any public sector hackback operation, whether operated by law enforcement agencies, military organizations, intelligence agencies or any other government sector, to operate without recognizing these risks and planning how to deal with them is irresponsible.

While governments may be legally able to operate outside of normal criminal statutes, that does not mean that they do not have an obligation to consider potential problems. The concept of collateral damage – defined as “injury inflicted on something other than an intended target”[14] – is directly applicable. The third party whose site was used by an actual perpetrator is not – or should not be - the intended target of hacking back. Causing damage to that third party – particularly with the intention of letting the third party suffer the economic, legal or reputational consequences should not be ignored.

As noted earlier, the third party can incur significant expenses. They can also be required to report the incident – particularly if it appears that certain types of information might be compromised – to government agencies. For example, in the United States, a health care organization that believes that it suffered a compromise involving more than 500 medical records is required to report that to the U.S. Department of Health and Human Services, which publishes the notification on a list available on the Internet.[115]

Should these issues stop a governmental agency involved in an investigation or intelligence collection from carrying it out or cause them to modify their investigative/collection plans to minimize collateral damage to third parties? There is no answer to that question that would apply in all times and in all situations. Could there be situations (perhaps life-and-death situations) where the need for the hackback overrode all other considerations? At the very least, it appears that the process through which governmental hackback operations are developed and approved should have a specific requirement to identify collateral damage issues and require that a specific decision be documented regarding how these issues should be handled.

There is a principle known as the ‘Law of Unintended Consequences’ which basically says that there can be consequences in any project that were not the intention of the project team. For example, there has been a massive global recall of certain automobile airbags because when triggered, those devices may eject metal fragments (like shrapnel) that can injure or kill occupants of the car. Causing those injuries or death were not an intended result by the automobile manufacturer of installing those air bags – they were a result of the design of the bags – design carried out by another company. Nonetheless, the automobile manufacturers had to take responsibility for the airbags they installed.

[14] Merriam-Webster dictionary, “Collateral Damage”, at https://www.merriam-webster.com/dictionary/collateral%20 damage (accessed 2 August 2017).

[15] The publication of this list is mandated by section 13402(e)(4) of the Health Information Technology for Economic and Clinicah Health (HITECH) Act, and the current list can be accessed at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Conclusion

In this article, the potential effects of hackback efforts, including undesired or unintended effects, have been described.

There should be little doubt that governments have the right to conduct cyberoperations including counterattacking those who attack, but the risks of such actions – as with all such plans – must be understood. The actions of NATO and of member states to recognize cyberspace as a valid domain of warfighting underscores the fact that as with operations in any warfighting domain, every operation has potential risks and rewards.

There are potentially significant dangers relating to private sector organizations engaging in hackback operations. There are also ways for terrorist groups to take advantage of private-sector hackback laws in ways that may not have been considered by those drafting such laws.

Our conclusion is that when a governmental entity is planning a hackback operation, there is a moral imperative to identify the potential results and consequences of that operation – intended and unintended, expected and unexpected – and consider each of them in the final design and approval of a project. Undertaking a project without doing should put into question the competence of the project team. Failing to do this analysis may mean that unplanned consequences (like the target detecting the hackback, either to interdict it or collect evidence that can be made public) are not being considered, when doing so is vital. We believe that any hackback planning process which does not include such an analysis is flawed and should be carefully considered by government agencies considering hacking back.

BIBLIOGRAPHY

Doyle, Charles, “Cybercrime: A Sketch of 18 U.S.C 1030 and Related Federal Criminal Law”, *Congressional Research Service Report* 7-5700, (14 October 2014).

Fleishman, Glenn, “Cartoon Captures Spirit of the Internet”, (14 December 2000),*The New York Times.*

Minárik, Tomás, “NATO Recognizes Cyberspace as a ‘Domain of Operations’ at Warsaw Summit”, (21 July 2016), *CCDCOE Incyder*.

Rid, Thomas, and Buchanan, Ben, “Attributing Cyber Attacks,” *Journal of Strategic Studies*, 38 (2015).

Rose, Kevin, “Trump Says that the DNC Hacker Could Be ‘Somebody Sitting on their Bed Who Weighs 400 pounds’”, (26 September 2016), *Fusion*.

Starks, Tim. “Scoop: ‘Hack back’ Bill Gets Version 2.0”, (25 May 2017), *Politico*.

DATR, 2017; 9: 47-59

ISSN 1307 - 9190

The Use of Social Media for Terrorism[1]

Erdal ÖZKAYA[2]

Abstract: *This article goes through the ways in which terrorists have been exploiting social media. It explains how terrorist propaganda litters the internet and how terrorist groups are recruiting new fighters on social media with special interest on Westerners. The article also goes through how the increased encryption of social media platforms has made them ideal for terrorists to use to communicate. Lastly, the article discusses how terrorists have been capitalizing on social media to fulfill their attention-seeking goals. It also brings to light some complementary functions of the dark web to achieve goals that are unattainable on social media. The article ends by suggesting aggressive measures that can be taken by users, governments and social media platforms to bring an end to terrorism on both social media and the dark web.*

Keywords: *Social media, terrorism, cybercrime, cyberterrorism, propaganda*

[1] Received on 25 July 2017. Accepted on 05 October 2017.

[2] *Cybersecurity Architect, Global Cybersecurity Practice, Microsoft Services, e-mail: erozkaya@microsoft.com*

1. Introduction

Over the last decade, there has been a sharp increase in the use of social media by the world. Facebook boasts of a user base of approximately 2 billion people while Twitter and Instagram are heading towards getting half that number of users. The main reason for the establishment of all these social media networks has been to provide social connections. Facebook is now on an ambitious plan to connect the whole world. It aims at doing this through drones that will supply the internet to hard-to-reach places in third world countries. Social media networks provide many advantages to internet users. They have enabled them to stay in touch with loved ones through better and cheaper mean than the traditional telephone. The social media networks have also been used for marketing purposes since they bring together a wide range of consumers. The users have been profiled by the social media platforms and companies can now simply advertise to specific niches of consumers all over the world. Lastly, these platforms have enabled users to get information within the blink of an eye. Traditional media are associated with delays as news moved slowly from one media outlet to another. Today, anything posted on social media gets to other users in near real time.

However, a new set of problems has erupted amidst these positive uses of social media. Terrorist groups have decided to establish themselves and make known their activities through these platforms. They are taking advantage of the interconnectedness of the world right now through such platforms and are using this to further their interests. Attacks have been live streamed to social media users, as they happen, by the terrorists themselves. Recordings of executions and other inhumane acts have been leaked to millions of users on these platforms. Advertisements for recruitment have flooded social media. The blind beliefs of terrorists have been crafted to sound appealing to oblivious social media users. Some users have been wowed by this and have made a dangerous move to join terrorist groups. Social media has also provided a new breeding ground for Muslim extremists through easily accessible materials for radicalization.

In the last few years, the world has witnessed a growing use of social media by terrorists. There have been attacks that were either motivated by social media or their impacts amplified by disseminations on those platforms. In June 2016, former US President Obama acknowledged that an attack done in a gay club in Orlando was caused by online extremism.[3] He said that the attacker, who came to be identified as Omar Mateen, was inspired by so-called jihadist material that was found on Twitter, Facebook and other social media networks. Even more chilling were the messages that Mateen had posted on his Facebook account before committing the attack. He said that his attack was in support of the Islamic State of Iraq and Levant (ISIL/DAESH) terrorist group and that the US had to be prepared for even more attacks.[4] Investigations further revealed that Mateen had multiple Facebook accounts that he used to post comments about ISIL/DAESH. The post before

[3] Alan Blinder, Frances Robles, and Richard Pérez-Peña, "Omar Mateen Posted to Facebook Amid Orlando Attack, Lawmaker Says", (17 June 2016), *New York Times*, available at https://www.nytimes.com/2016/06/17/us/orlando-shooting.html?_r=0 (accessed 05 June 2017).

[4] Ibid.

the attack, which was addressed to the US. told its citizens to taste the vengeance of ISIL/DAESH. It was confirmed that Mateen had searched on his phone about the attack that he had committed during the three-hour standoff with the police.[5] This was most probably to check to what extent the attack had gone viral on the internet.

Shortly after the Orlando attack, there was another social media-influenced terrorist attack in Paris, France. A policemen and his spouse were killed by an extremist called Abballa.[6] Apparently, Abballa live-streamed a twelve-minute video to Facebook while still inside the policeman's home. He revealed that he committed the heinous act in response to a call from senior ISIL/DAESH leaders to followers in Europe and US.[7] The followers of ISIL/DAESH had been informed to unleash terror during Ramadan. Facebook quickly took down the video but did not issue any comments about it, saying just that the video was under active investigation. This was however after it had been accessed by many people during the live stream. There then followed claims that Facebook was struggling to stop such kind of crimes from being shared on its network, especially if they were being live streamed.[8]

There have been many other attacks that have been facilitated significantly by multiple social media platforms. Terrorist groups have been using the same media platforms to significantly magnify the impacts of their terrorist acts. Social media has been used to accelerate and multiply acts of terror. It has also transformed and helped evolve terrorism activities.

2. The reasons why terrorists are using social media

There are many reasons for terrorists to harness the power of social media to support their activities. It all boils down to the fact that social media platforms have a broader audience than any other type of media. Therefore, they can easily reach out to millions if not billions if they use social media platforms effectively. The following are the discussions of some of the reasons why.

2.1 Spreading terrorist propaganda

Many organizations today use social media to advertise their products and to encourage people to remain loyal to their brands. Terror groups have copied this and have been using it to take their propaganda to the masses and to make them support their activities.[9] Groups such as ISIL/DAESH

[5] Ibid.

[6] Lori Hinnant and Elaine Ganley, "Attack that Killed 2 Police Officers in France May Have Been Streamed on Facebook Live", (14 June 2016), *Global News*, available at http://globalnews.ca/news/2760327/frenchman-who-shot-video-of-fatal-paris-police-stabbing-had-terrorist-past/ (accessed 5 June 2017).

[7] Ibid.

[8] Ibid.

[9] Mihaela Marcu and Christina Balteanu, "Social Media - A Real Source of Proliferation of International Terrorism," *Annales Universitatis Apulensis: Series Oeconomica,* 16(1) (2014), pp. 162-169, https://econpapers.repec.org/article/

have consistently used Twitter to spread their propaganda. They make posts that support their ideologies and possibly attract people to either join or support the group. Most times, they will go on to explain how some countries have committed atrocities against other countries. They will also attack poor countries for supporting the ideologies of these nations. They will claim that their aim is to either bring vengeance or ensure equality. They tailor their messages to focus on bringing societal change to countries that have failed. They claim to establish peace by imposing 'peaceful' religious laws that will ensure that there is justice. A person unaware of the grave attacks that these groups commit with complete disregard for human life might be brainwashed to believe in their propaganda.

These terror groups normally have many accounts to spread their messages. In 2016, Twitter had to bring down over 124,000 user accounts that were linked to ISIL/DAESH or were found to be spreading ISIL/DAESH propaganda. Today, the group still has massive influence online and it seems that they bring up new accounts as quickly as the old ones are blocked.[10] They continually make and post professional quality video advertisements and pictures that always try to convince the audience that the so-called 'jihad' is a worthy cause. On social media accounts, the group portrays its caliphate as an Islamic paradise. ISIL/DAESH has however continuously uploaded gruesome videos of bombings and executions. They have used this to spread terror and fear messages to innocent people. This has also been done to normalize and glorify violence for its followers.

2.2 Recruiting foreign fighters

There have been reports of people leaving their home countries, including the United States, to go to Syria and Iraq to join ISIL/DAESH. It is estimated that ISIL/DAESH has received over 30,000 of these people who have traveled from every corner of the world to live in the Islamic paradise promised by the ISIL/DAESH propaganda videos.[11] A lot more have left their homes to join other groups such as Nigeria's Boko Haram. These groups are using social media as a platform to radicalize people and brainwash them with their extremist ideas. The major concern is when these formerly normal people have started going back home. The reason is that most terror groups such as ISIL/DAESH are losing territory and the radicalized fighters are being told to go back home but also assigned other missions. Some are to radicalize more people in their home countries while others are to carry out terrorist attacks. Terror groups are bringing terror to people's doorsteps with their foreign fighters. ISIL/DAESH, in particular, is discouraging people from traveling to Syria, but it is recruiting them on social media platforms.

alujournl/v_3a1_3ay_3a2014_3ai_3a16_3ap_3a14.htm (accessed 5 June 2017).

[10] Ibid.

[11] Ibid.

Recruiters for these terror groups are also hunting for potential followers on social media networks. They are good at determining when a person can easily be brainwashed and radicalized. They have employed a number of tactics to gain as many followers as possible. The initial means of contact involve friend requests, follows and messages on Facebook, Twitter, and WhatsApp. From there, the recruiters are able to slip in their radicalization messages slowly to the minds of their targets. It is therefore not necessarily that all followers of terror groups reached out to the group's social media networks and asked to join. There is an army of recruiters for these groups online that is working towards enlisting more people to their caliphates.

Profiles of young and beautiful women are being used to lure in potential recruits.[10] These accounts are being used to convince a target group of potential members of the 'good' lives that ISIL/DAESH fighters are living in a utopic world located between Syria and Iraq. They are presenting ISIL/DAESH territory in such a positive light that it appears to be the best place to live. It is being showcased as a place where one can live a meaningful and purposeful life in a Islamic state ruled by Islamic laws. They claim that it is a so-called five-star jihad. In 2015, as part of the five-star lifestyle, the group promised its members that it was going to reopen a luxury hotel in Mosul. Other pictures showed ISIL/DAESH girls posing in a fancy BMW while wielding AK-47 rifles.[12]

ISIL/DAESH recruiters are also using messengers to stay in touch with those that want to travel all the way to Syria. There are reports that the recruiters issue brochures detailing the journey to ISIL/DAESH territory, the logistics of getting there, what to carry and where to meet a guide in Turkey. This has prompted the Turkish government to be more vigilant to prevent people from sneaking into Syria through Turkish borders. The New York Times reported in 2015 that half of the members of ISIL/DAESH were foreigners[13]. An estimated 4000 of these were said to be coming from Western countries. The infamous so-called Jihadi John was himself a British Muslim who gained fame when he appeared in execution videos.[14] The group is, therefore, targeting foreigners. It has been said that most of the dangerous radical extremists claiming affiliation with Islam in the group are Western recruits. Most of them join as new Muslim converts searching for adventure and wishing to live in the promised utopia.

The extensive use of social media for recruitment has so far only been witnessed in ISIL/DAESH. Previously, when Al-Qaeda was the most feared terror group, access to information was limited and even recruitment of new members was subject to qualification. Al-Qaeda has more restrictive practices and even turns down new members. The group even has a special rigorous vetting process for foreigners. There are obstacles that it has put in the recruitment process. These are the obstacles

[12] David Sim, "After ISIS: Inside Mosul's Destroyed University and Five-Star Hotel," (20 February 2017), *International Business Times UK*, available at http://www.ibtimes.co.uk/after-isis-inside-mosuls-destroyed-university-five-star-hotel-1604459 (accessed 5 June 2017).

[13] Chris Hughes, "Almost Half of Western ISIS Jihadists Fighting in Syria and Iraq Have Died", (22 March 2016), *Mirror*, available at http://www.mirror.co.uk/news/world-news/half-western-isis-jihadis-been-7609147 (accessed 05 June 2017).

[14] Ibid.

that ISIL/DAESH removed in its more aggressive recruitment strategy that expanded to social media.

2.3 Communicating more effectively

Terrorist groups are also using social media platforms for communication purposes.[15] This is because they are safer than phone calls and text messages. An expose by a former NSA contractor said that the US was actively monitoring phone calls made in multiple countries. The US government was also said to be going through the emails and text messages of its own citizens.[16] This shows that terrorist groups are unlikely to use these types of media because they are actively monitored. It is also easy to locate the senders and receivers of information over such media. Terrorist groups need more secure media. They also need to be able to reach out to many people at a time.

Social media comes as a great solution to all these communication problems. Some platforms promise users end-to-end encryption of messages especially after the US government was found to be snooping into everyone's private messages.[17] Terrorists are using this kind of security assurance to communicate without the fear of being tracked or of having their communications monitored. Several attackers have been found to be in communication with ISIL/DAESH leaders through highly encrypted media such as Telegram. They have used these to get instructions on places to attack and when to do so. Communication about the supply of ammunition and explosives is also done on these platforms.

2.4 Seeking attention

Social media platforms have also played a big role in allowing terror groups to get attention from the world. Before social media, terror groups relied on traditional media to get attention. The problem was that they were not in total control of such media as their stories had to pass through editors before the report aired or was printed. There has however been a long relationship between terrorists and media. Terrorists exploit media to further their messages and goals to a wide audience. Terrorists rely on one thing to gain attention - conducting acts of terrorism and aggression against civilians. For years, they have used this technique.[18] This is because it is significantly difficult for such groups to obtain weapons capable of toppling governments, enabling them to seize power and establish their own rule. They only have enough to spread panic by hurting or killing a few people.

[15] Marcu and Balteanu, "Social Media - A Real Source of Proliferation of International Terrorism".

[16] Micahel Munger, "Review: No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State," *The Independent Review*, 19(4) (2015), pp. 605-609, available at http://www.independent.org/publications/tir/ article.asp?id=1053 (accessed 5 June 2017).

[17] Ibid.

[18] Austin T. Turk, "Sociology of Terrorism," *Annual Review of Sociology* 30 (2004), pp. 271-286, available at http://www.annualreviews.org/doi/abs/10.1146/annurev.soc.30.012703.110510 (accessed 05 June 2017).

After committing such acts, they normally want their intentions to be amplified and spread to a wide audience. Traditionally, these included newspapers, TV and radio stations.

For long, these media have been used by terrorists to convey messages.[19] Even today, if a terrorist attack happens, mass media organizations will scramble to cover it and they will repeat it over and over. This is what terrorists rely on to remain relevant; the trauma that they cause to be broadcasted repeatedly to a global audience. They have been relying on publicity to thrive.[20] Social media has now given terrorist groups control over what the public perceives them to be. They no longer have to rely on getting attention from traditional but scrutinized mass media. With social media, groups like ISIL/DAESH are making periodic releases showing their members training, executing people and even committing terrorist attacks. They are getting their content to the world in an unfiltered way.

The use of social media has however been occasioned with some challenges. Social media is not entirely secure, even for terrorists who want to protect the anonymity of their members, supporters and especially financiers. Several planned attacks have been thwarted after law enforcement agencies gathered intelligence from social media before the execution of attacks. Some wealthy financiers of terrorist groups have been exposed as well. There have been many information 'leaks' from social media thus making it inadequate to fully support terrorist activities. Therefore, terrorists have been looking for a more secure platform that, among many other things, is completely sealed and is very difficult to compromise the anonymity of the parties involved. Therefore, they have adopted the dark web to fill the gaps present in social media platforms.

3. Use of the dark web by terrorists

Governments have been increasing surveillance efforts over telephone systems and social media. Twitter is currently banning hundreds of thousands of accounts that could be linked with terrorist groups. Facebook has been taking down execution videos right after they are posted by terrorists. Security agencies have been trying to get back entries to some social media accounts to identify the owners. This has prompted terrorist groups to seek safer and anonymous alternatives to continue communicating and transacting. Terrorists have evolved with all these new concerns and are now exploiting the power of the dark web. They are using it to complement their activities on other platforms. They are using social media for recruit and spreading their propaganda to the world and the dark web for more secretive communication and transactions. The in-depth discussions below explain more on how the dark web is used by terrorists.

[19] Ibid.

[20] Christopher H. Sterling, "Book Review: Terror Post 9/11 and the Media", *Journalism and Mass Communication Quarterly* 88(3) (2011), pp. 683-684.

3.1 Planning attacks

When terrorists plan to attack, they are cautious to ensure that information does not leak out. If information concerning their planned attacks gets to law enforcement agencies, there is a high likelihood that the attacks will be thwarted. For some reasons, such as ease of identification and tracking on social media, they try to plan on other more secure platforms. Thus, they have turned to the power of anonymity of the dark web. The dark web has highly secure platforms through which terrorists can make their plans. It is riddled with encryptions that make it significantly hard for law enforcement agencies to track down the IP addresses used by its users.

Though it was not originally meant for this purpose, the dark web has seen many other illegal activities being conducted through it. In 2015, after years of tracking, law enforcement agencies were able to crack down and arrest the leader of the largest drug syndicate on the dark web. The leader managed an online shop called The Silkroad where people would buy drugs and have them delivered at their doorstep.[21] In this context, the most important components of this online drug trade are the ordering and delivery mechanisms. They were totally secure and reliable. This means that terrorists are probably using the same type of mechanisms to plan terror attacks. They probably have their own sites on the dark web where members can log in to receive briefings concerning attacks. The French Interior Minister said in 2016 that the masterminds of terrorist attacks in Europe used the deep web to communicate through highly-encrypted messages and using anonymous identities.[22] The delivery system of Silkroad also shows that it is possible that these terrorists have reliable ways of getting armament and explosives to their members in other countries. The Silkroad had an efficient delivery network that even got drugs to children through mailboxes.[23] It is, therefore, possible that terrorists have their own dark web delivery systems.

3.2 Funding and business transactions

Terrorist groups receive funding from many sources. Some of these sources are people that have been tricked into believing the terrorist propaganda. There is a dark web page called "Fund the Islamic Struggle without Leaving a Trace" where people can go and anonymously donate for the so-called *jihad*. There have been rumors that some oil-rich countries in the Middle East and Asia have also been key funders of these extremist terror groups claiming affiliation with Islam.[24] Large terrorist groups also run businesses in order to make money to help them stay solvent. Some terror groups are in control of areas with resources such as oil that they can sell it for cheap to get funds to buy weapons or compensate their fighters.

[21] Zaklina Spalevic and Marija Ilic, "The Use of Dark Web for the Purpose of Illegal Activity Spreading", *Ekonomika* 63(1) (2017), pp. 73-82.

[22] Ibid.

[23] Ibid.

[24] Dimitrious Stergiou, "ISIS Political Economy: Financing a Terror State," *Journal of Money Laundering Control 19*(2) (2016), pp.189-207, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2781384 (access 05 June 2017).

Terrorists also do kidnappings and requests for payment of ransom money. Others are in charge of drug shipping channels and make insanely huge amounts of money to allow the movement of drugs. They are also contracted by wealthy investors for assassinations or to destabilize competitors. Lastly, they sell body organs harvested from captives and antiquities stolen from the cities that they take over.[25] All these activities require money to be moved in a secure and hard-to-trace way. There is an anonymous currency available on the dark web called Bitcoin. It was heavily used for the drug trade on Silkroad and it is still being used for these kinds of terrorist dealings. Transactions made via Bitcoins are hard to trace and thus do not often put the identities of the senders of the money at risk.[26]

3.3 Acquiring weaponry and fake passports

The dark web is a hive of illegal activities. There are dark web stores that specialize in selling and supplying guns, ammunition, and explosives. Investigations into the Paris attacks of 2015 showed that the weapons that were used in the shooting were bought from a dark web store. The supplier was identified as a German citizen operating on the dark web with the username DW Guns. This is only one of the many instances where terrorists have bought guns from the dark web. In 2016, former US President Barrack Obama said that terrorists had bought radioactive isotopes from dark web brokers.[27] He was worried that they could release the radioactive material over populated places using drones. Terrorists are also using the dark web to buy fake passports. There are dark web brokers that readily make and deliver fake passports for people wishing to illegally enter countries such as the US and UK.[28] The transactions are done online, powered by Bitcoin. The brokers also have reliable delivery mechanisms to ensure that the passports get to the terrorists.

4. Conclusion

This article has done an in-depth analysis on the ways that social media is being exploited by terrorists to achieve their goals. It has explained how the world is now interconnected by social media, allowing information to flow faster with less control than it used to through traditional media. The article has also shown how this interconnectedness and fast flow of information could be used by terrorists. It has given a background of two terrorist attacks that caught the attention of the world that were in one way or another facilitated by social media. In one of the attacks, a former US president acknowledged that it was due to the radicalization of the perpetrator on social media. The other attack was even more chilling since the perpetrator streamed a 12-minute video clip on

[25] Ibid.

[26] Spalevic and Ilic, “The use of dark web for the purpose of illegal activity spreading.”

[27] Ibid.

[28] Ibid.

YouTube after the attack. The article has brought to light most of the ways through which social media is being used by terrorists. It has explained how terrorists are using social media to spread their propaganda. They have been using it to spread their ideologies in sugar-coated advertisements aimed at deluding people into believing in their cause.

This article has also detailed how social media is being used extensively to recruit new fighters into terrorist groups. ISIL/DAESH is one of the groups that is capitalizing on Facebook and Twitter to reach out to vulnerable people and enticing them into joining the caliphate. It has repeatedly called on all 'true' believers of Islam to join it and remarkably many people have traveled to Syria to join ISIL/DAESH. Their recruitment strategy is working since reports show that 40% of ISIL/DAESH militants are foreigners. Social media is also being used for communication. This is because phone calls and text messages are easily monitored while, at the same time, social media platforms are becoming harder for law enforcement agencies to keep an eye on due to end-to-end encryption of messages.

This article has also identified that terrorists are using social media to seek attention. It has explained the relationship between terrorism and media, tracing back this relationship to traditional media and explained how social media has given terrorists a new avenue with which to gain attention. Terrorists are using it to show its fighters brandishing weapons, to stream attacks, to showcase the 'paradise' that fighters are living in and to show gruesome executions. Lastly, this article has explained how other online services have been used to complement social media, explaining a few ways that terrorists are using the dark web. It has gone through how it is being used to plan attacks, get funding, conduct transactions and acquire weapons.

This article ends with some recommendations on how the exploitation of social media by terrorists can be controlled. These are:

a) Algorithms to take down terrorist-related materials from social media

The exploitation of social media by terrorists can be stopped through a few collaborative measures done by users, social media platforms, and governments. One of the measures that could be taken is to encourage social media companies to build algorithms to identify terrorist propaganda posts and remove them immediately from all platforms. Social media companies have been spending a lot of resources on developing algorithms to mine data from users. However, they have not been doing the same to come up with algorithms to mine for terrorist related posts and videos. With the right amount of pressure from both users and governments, these platforms can come up with tools that can be used to detect terrorist propaganda, remove the posts and suspend the associated accounts.[29]

[29] Paulina Wu, "Impossible to Regulate? Social Media, Terrorists, and the Role for the U.N.", *Chicago Journal of International Law,* 16(1) (2015), pp. 281-311. http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=690&context=cjil (accessed 05 June 2017).

Three lawsuits have already been filed by some victims of terrorist acts against multiple social networks for allowing terrorist material on their platforms that contained the murder of their friends and family. The suits have had one thing in common – they are asking why social media platforms have not put in a tenth of the efforts that they use for advertising towards barring terrorists from posting some sensitive material.[30] There are emerging fingerprinting technologies that can be used to flag video clips related to terrorism. These technologies could be embedded into the codes for uploading videos so as to prevent the uploading of all terrorism-related material.[30] The advent of artificial intelligence has made it easier for systems to think on their own. AI and machine learning should be incorporated into the sharing, uploading or publishing functionalities of all social media to flag any terrorist-related material.[31]

There have been successful implementations of other technologies that were used to hunt for any child pornography on the internet. A tool called PhotoDNA detected any material that contained child pornography and it was a turning point in the war against the same.[32] This tool was used a decade ago and with the current technologies today, it should be easy to come up with an analysis tool to take down any terrorism-related material. This might prevent terrorists from littering social media with their advertisements and videos of executions or attacks.

b) Encouraging users not to share terrorism-related material

Another measure that can be taken is for users to be encouraged not to share any material that they may come across related to terrorism. When groups such as ISIL/DAESH upload their videos on social media, they go viral because of the users, who share these videos with other users who send the clips to many other people. Governments and social media platforms should warn people against such actions since they give the desired attention and fame to terrorist groups. The platforms could come up with an account suspension rule for all accounts found to have shared terrorist-related material. Governments could come up with regulatory frameworks to hold users accountable for their actions on social media. The government could make it a crime to share videos from terrorists as this is against the good of the public. Users should be encouraged to report such videos so that the social media platforms can take them down easily. This will greatly reduce the number of people who get access to material from terrorist groups and in turn, this will take attention and relevance from the terrorists.

[30] Gabriel Weimann, "Terrorist Migration to the Dark Web", *Perspectives on Terrorism*, 10 (3) (2016), at http://www.terrorismanalysts.com/pt/index.php/pot/issue/view/58 (accessed 05 June 2017).
at http://www.terrorismanalysts.com/pt/index.php/pot/article/view/513/html (accessed 05 June 2017).

[31] Wu, "Impossible to regulate? Social media, terrorists, and the role for the U.N.*"*.

[32] Weimann, *Terrorist Migration to the Dark Web*.

c) Indexing the dark web

Lastly, since this article highlighted the use of the dark web by terrorists, there is one sure way that this can be prevented. The dark web should be indexed, at the very least, to identify the sites that operate in it. Most of these sites have been promoting terrorism either by selling weapons and fake passports or by providing very secure platforms for terrorists to communicate. Indexing of the dark web will help authorities know these sites and effectively shut them. DARPA, an American defense research agency, claims that it has a tool that can be used to kill terrorism activity on the dark web. The agency developed a tool called MEMEX that was used to monitor human trafficking on the dark web. It was effective against hunting down all human trafficking dark sites and can be used again to bring down terrorism-related sites as well.

BIBLIOGRAPHY

Binder, Alan, Robles, Frances, and Pérez-Peña, Richard, "Omar Mateen Posted to Facebook Amid Orlando Attack, Lawmaker Says", (17 June 2016), *New York Times*.

Hinnant, Lori, & Ganley, Elaine, "Attack that Killed 2 Police Officers in France May Have Been Streamed on Facebook Live", (14 June 2016), *Global News*.

Hughes, Chris, "Almost Half of Western ISIS Jihadists Fighting in Syria and Iraq Have Died", (22 March 2016), *Mirror*.

Marcu, Michaela, and Balteanu, Christina, "Social Media - A Real Source of Proliferation of International Terrorism", *Annales Universitatis Apulensis: Series Oeconomica,* 16(1) (2014).

Munger, Michael, "Review: No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State", *The Independent Review* 19(4) (2015).

Sim, David, "After ISIS: Inside Mosul's Destroyed University and Five-Star Hotel", (20 February 2017), *International Business Times UK*.

Spalevic, Zaklina, & Ilic, Marija, "The Use of Dark Web for the Purpose of Illegal Activity Spreading", *Ekonomika* 63(1) (2017).

Stergiou, Dimitrious, "ISIS Political Economy: Financing a Terror State", *Journal of Money Laundering Control* 19(2) (2016).

Sterling, Christopher H., "Book Review: Terror Post 9/11 and the Media", *Journalism and Mass Communication Quarterly*, 88(3) (2011).

Turk, Austin T., "Sociology of Terrorism", *Annual Review of Sociology* 30 (2004).

Weimann, Gabriel, "Terrorist Migration to the Dark Web", *Perspectives on Terrorism*, 10 (3) (2016).

Wu, Paulina, "Impossible to Regulate? Social Media, Terrorists, and the Role for the U.N.", *Chicago Journal of International Law* 16(1) (2015).

This Page Intentionally Left Blank

DATR, 2017; 9: 61-76

ISSN 1307 - 9190

Islamic State of Iraq and Syria’s Terrorism: A Universal Instrument of Asymmetric Warfare and the New Battlefield in Europe[1]

Thomas MAURER[2]

Abstract: *Since its inception, ISIS has been responsible for more than 5,000 terrorist attacks worldwide. This paper assesses ISIS terrorism to be a particularly effective and universal instrument to generate effects on different levels. ISIS conducts terrorist attacks for several purposes: to demoralize opposing forces, to destabilize adjacent regions and adversary states; and also to retaliate against superior alliances. As yet, neither the organization’s ability to commit terrorist attacks nor its global reach have been substantially degraded. Through targeted strategic attacks in Europe, ISIS has succeeded in instilling fear and horror in Western societies and has been able to underpin the legitimacy of its self-proclaimed ‘Islamic Caliphate‘ in order to assert itself as the foremost representative of the so-called ‘global jihadist’ cause. The most dangerous scenario is that ISIS will transform into a transnational, non-state terrorist threat network without any protostate features and it will seek its new battlefield in Europe.*

Keywords: *ISIS, terrorism, Turkey, Europe, Urban Guerrilla, Lone Wolf Strategy*

[1] Submitted on 29 May 2017. Accepted on 23 June 2017.

[2] M.A. mult., Studies on Military Leadership and International Security, Helmut-Schmidt-University/ University of the Armed Forces, Germany, e-mail: t.maurer@hsu-hh.de

Introduction

As an essentially offensive strategy, terrorism expands upon guerrilla warfare tactics and, in doing so, revolutionizes the concept of asymmetric warfare, thus introducing a new form and era of warfare.[3] Over the last fifteen years, the number of victims of terrorist attacks has increased tenfold. In recent times, terrorist attacks have been committed in more than 100 countries worldwide.[4] Terrorism has not only developed into a weak actor's strategy of using force but also into a manifestation of current extremist ideologies, often claiming an affiliation with Islam. Terrorist warfare is one of the new modes of war, which – in all likelihood – could determine future war scenarios.[5]

Terrorism seems to be a key pillar of belligerent actions performed by the Islamic State of Iraq and Syria (ISIS[6]). Some commentators say that the organization is acting like a wounded beast that is wildly thrashing around, while others claim that ISIS employs terrorist attacks very deliberately.[7] To ease these tensions, this article poses the question for which specific purposes does ISIS employ terrorism? Regarding this, the organization's conduct of terrorism – the patterns[8] of their different terrorist attacks and engagements worldwide between early 2014 and now – will be analyzed in detail, using the three levels of classic military theory: tactical, operational and strategic. With this method, this article can clarify whether the organization is acting systematically or just like a wounded beast.

Terrorism as a Tactical Instrument

Focusing on the tactical level, ISIS has very skillfully employed terrorism in its activities in Iraq and Syria. Weeks before actually launching its Iraqi offensive in January 2014, ISIS had already

[3] Sean N. Kalic, "Terrorism in the twenty-first century", in An International History of Terrorism: Western and non-western Experiences (Hanhimäki, Jussi M. and Bernhard Blumenau, eds., Routledge, 2013). p. 271.

[4] Institute for Economics and Peace (IEP), *Global Terrorism Index 2015 – Measuring and Understanding the Impact of Terrorism* (Institute for Economics and Peace, 2015), p. 2.

[5] Herfried Münkler, "Terrorismus heute: Die Asymmetrierung des Krieges", *Internationale Politik* 2 (2004), p. 1.

[6] The Islamic State of Iraq and Syria refers to itself as a state. This claim is considered highly controversial both morally and politically, as well as with regard to international law. Therefore, the organization has been given different names in different countries. In relevant literature, the organization is formally entitled the *Islamic State of Iraq and the Levant* (ISIL) or *Islamic State of Iraq and al-Sham (Greater Syria)* (ISIS). Referring to its origins, it is also called a Sunni extremist militia, a terrorist militia or terrorist organization. And it is also referred to its protostates features as *the so-called Islamic State* (IS) or as *Da'ish/Daesh*, the abbreviation of *daula al-islamiya fil-Iraq qa al-Sham* – the *Islamic State of Iraq and Greater Syria*. This article will explicitly refrain from taking part in this discussion and will only use the designation 'ISIS'.

[7] Patrick Cockburn, *ISIS: Battling the Menace* (Independent Print Limited, 2016), pp. 62-64; See also Florian Flade and Alfred Hackensberger, "Wie eine Verwundete Bestie", (27 March 2016), *Die Welt*, available at http://www.welt.de/print/wams/politik/article153708574/Wie-eine-verwundete-Bestie.html (last visited 01 December 2017).

[8] Due to the lack of primary sources, the following assessment is mainly based on reliable studies on ISIS's modes of warfare published by the Combating Terrorism Center (CTC) at West Point, the Institute for the Study of War (ISW) in Washington D.C., the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland, the International Institute for Strategic Studies (IISS) in London, the International Centre for Counter-Terrorism (ICCT) in The Hague and on open source reports by the European Union Agency for Law Enforcement Cooperation (EUROPOL). The final assessment merely represents the author's personal evaluation and opinion.

started to announce its upcoming assaults on cities. Both the Iraqi Security Forces (ISF) and the Shiite population were systematically intimidated and warned that anyone standing up to ISIS would be killed. These threats were reinforced by numerous mass executions during which Iraqi soldiers were beheaded, crucified or impaled.[9] To make optimum use of the effects of these terrorist methods, ISIS employed modern media, particularly social networks, as platforms to exhibit these atrocities and was thus able to incite fear, panic and hysteria among the population - terrorism. ISIS understands that the impact of terrorist acts is intensified by media coverage and the resulting war of images.[10] In Tikrit, for example, approximately 100 Iraqi soldiers were brutally executed, their bodies paraded in public and videos of the executions deliberately distributed through social media networks.[11] With these threats and demonstrative executions, ISIS succeeded in generating fear and horror. As a result, the ISF lost most of their morale so their combat effectiveness was diminished considerably.[12] Numerous terrorist attacks against the Shiite population increased the fear and panic among the people in the cities under attack, contributing to the demoralization of the defending forces, whose members, intimidated by the *black banner* and fearing the merciless brutality of ISIS, deserted in their hundreds.[13]

As far as its current defensive campaign is concerned, the terrorist organization continues to rely on public executions to demonstrate its control over the local population and to demoralize its opponents.[14] By using these terrorist methods, ISIS achieves a direct shock effect – also referred to as 'terror shock value' – at the tactical level even before launching combat operations. Consequently, this use of terrorist methods to directly influence opposing forces on the battlefield could be called psychological warfare in the form of terrorism.[15]

A Tool for Operational/Mid-Term Goals

Since July 2013, ISIS has also been deliberately using the tool of terrorism to achieve its mid-term goals. Terrorist activities have been focused on civilian Shiite targets located in the Iraqi capital

[9] Guido Steinberg, *Kalifat des Schreckens: IS und die Bedrohung durch den islamistischen Terror (Knaur TB, 2015)*, pp. 98-100.

[10] Michael Lüders, *Wer den Wind Sät: Was Westliche Politik im Orient Anrichtet,* (C.H. Beck, 2016), p. 94.

[11] Michael Knights, "ISIL's Political-Military Power in Iraq", *Combating Terrorism Center (CTC) Sentinel* 8 (2014), p. 4.

[12] Rainer Hermann, *Endstation Islamischer Staat? – Staatsversagen und Religionskrieg in der arabischen Welt* (dtv Verlagsgesellschaft, 2015), p. 63; See also Guido Steinberg, *Kalifat des Schreckens: IS und die Bedrohung durch den islamistischen Terror*, p. 98; Charles Lister, "Assessing Syria's Jihad", *Middle Eastern Security: The US Pivot and the Rise of ISIS* (Dodge, Toby and Emile Hokayem, eds., Routledge, 2014), p. 78.

[13] Daniel Milton et al., "The Islamic State in Iraq and the Levant: More than Just a June Surprise", *Combating Terrorism Center (CTC) Sentinel* 6 (2014), p. 3; See also Guido Steinberg, *Kalifat des Schreckens: IS und die Bedrohung durch den islamistischen Terror*, p. 112.

[14] Kevin Cooper and Emily Anagnostos, "Iraq Situation Report – November 9-17, 2016", *Institute for the Study of War (ISW)*, (17 November 2016), available at http://www.understandingwar.org/backgrounder/iraq-situation-report-november-9-17-2016 (last visited 01 December 2017).

[15] Malcom W. Nance, *Defeating ISIS: Who They are, How They Fight, What They Believe*, (Skyhorse Publishing, 2016), p. 315.

city of Baghdad. From the second half of 2013 until the end of 2014, ISIS was responsible for more than a hundred attacks in the ISF-controlled areas, claiming over a thousand lives per month.[16] ISIS's primary objective was to further aggravate existing religious and ethnic tensions so as to unleash a sectarian civil war between Shiites and Sunnis in order to be able to assume leadership of the Sunni part of the population.[17] Although ISIS failed to provoke a Sunni uprising or a major civil war, it nevertheless managed to take control of parts of the Sunni population by proclaiming a so-called 'caliphate,' which found acceptance among these people. Since the end of 2014, ISIS has been forced into a more defensive posture, yet it is still using terrorism as an operational means to destabilize adjacent regions. The terrorist campaigns employed by ISIS have been focused on the city of Baghdad and were aimed at further destabilizing the Iraqi state, especially its armed forces, in order to provoke their collapse. At the same time, this approach served to tie down the ISF and fix both their assets and attention on the provinces of Baghdad and Al-Anbar.[18] This was evident during the unsuccessful, large-scale ISF offensive to liberate the ISIS stronghold of Mosul at the end of March 2016. Just one day after the ISF and the Iraqi-Kurdish *Peshmerga* had begun their offensive, ISIS carried out a series of suicide attacks against the civilian population, which killed dozens of Shiites.[19] Kurdish soldiers captured near Mosul were publicly executed and video footage was published to attract media attention and to undermine the morale of the *Peshmerga*, with the aim of weakening cohesion and solidarity among the Iraqi-Kurdish coalition forces. When ISIS lost the strategically important Iraqi city of Fallujah, it likewise responded with a demonstration of its capability to conduct terrorism, carrying out a major suicide bombing in Baghdad at the beginning of July 2016 – the most devastating suicide attack since 2003 – killing more than 250 Shiites.[20] Since September 2016, ISIS has been extending the range of its terrorist attacks to areas outside the Baghdad and Al-Anbar provinces to achieve medium-term objectives. This strategy deliberately fixes the ISF in comparatively unimportant Iraqi provinces in order to restrict their availability and consequently prevent the recapture of ISIS's remaining stronghold.[21]

[16] Guido Steinberg, *Kalifat des Schreckens: IS und die Bedrohung durch den Islamistischen Terror*, p. 103.

[17] Christoph Reuther, *Die Schwarze Macht: Der Islamische Staat und die Strategen des Terrors*, (Deutsche Verlags-Anstalt, 2015), p. 241.

[18] Patrick Martin et al., "Iraq Situation Report – May 11-24, 2016", *Institute for the Study of War (ISW)*, (25 May 2016), available at http://understandingwar.org/backgrounder/iraq-situation-report-may-11-24-2016 (last visited 05 September 2017); See also Uri Friedman, "Is Terrorism Getting Worse? It Depends Where You Look", (14 July 2016), *The Atlantic*, , available at http://www.theatlantic.com/international/archive/2016/07/terrorism-isis-global-america/490352/ (last visited 01 December 2017).

[19] Patrick Martin, "Iraq Situation Report – March 29-April 4, 2016", *Institute for the Study of War (ISW)*, (04 April 2016), available at http://understandingwar.org/backgrounder/iraq-situation-report-march-29-april-4-2016 (last visited 01 December 2017).

[20] Emily Anagnostos, "Iraq Situation Report – June 29-July 6", *Institute for the Study of War (ISW)*, (05 July 2016), available at http://www.understandingwar.org/backgrounder/iraq-situation-report-june-29-july-6-2016 (last visited 01 December 2017).

[21] Jessica D. Lewis McFate and Alexandra Gutowsko, "ISIS's Capable Defense of Mosul – Counteroffensives in Kirkuk, Rutbah, and Sinjar", *Institute for the Study of War (ISW)*, (06 July 2016), available at http://iswresearch.blogspot.de/2016/10/isis-capable-defense-of-mosul.html (last visited 01 December 2017); See also Emily Anagnostos, "Iraq Situation Report – September 7-19, 2016", *Institute for the Study of War (ISW)*, (19 September 2016), available at http://www.understandingwar.org/backgrounder/iraq-situation-report-september-7-19-2016 (last visited 01 December 2017).

ISIS terrorist attacks are also directed against Turkey, the country neighboring the caliphate. The border region is very important to ISIS; it is the alleged transit route for foreign fighters joining ISIS and serves as a smuggling route for weapons, supplies and crude oil. In view of this situation, Turkey started air raids against positions of ISIS combat units in 2015 and introduced additional measures to limit the caliphate's transit and trafficking activities.[22] In Turkey, however, ISIS can draw on capable logistic networks, terrorist sleeper cells and probably also alliances with Turkish extremists.[23] With these assets, ISIS has been able to repeatedly launch rapid offensives with suicide attacks, occasionally even 'Mumbai-style attacks',[24] against Turkey, for example in Ankara, Gaziantep and at the international Ataturk Airport in Istanbul. The attack on an Istanbul nightclub on New Year's Eve 2017 – during which 39 people were killed by a single perpetrator – has been termed the most dramatic terrorist attack that has taken place in Turkey to date.[25] By killing numerous civilians, including foreign tourists, ISIS is deliberately targeting minorities such as Kurds, Alevis and left-wing groups in order to fuel domestic conflicts in Turkey and to destabilize the Turkish government. With this form of terrorism, ISIS has been able to partly regain its freedom of movement and action along trafficking and transit routes in the border region between Turkey and the caliphate.[26]

Further afield, even Iran is trying to gain political influence in the Levant by training and mentoring Shia militias from *Hash'd al Shaabi*, the so-called Popular Mobilization Units (PMU), in Iraq. It is also assisting the Syrian regime with troops from the Islamic Revolutionary Guard Corps embedded with militias from the Lebanese radical group *Hezbollah.* [27] On 7 June 2017, teams of gunmen assaulted the parliament and the revered tomb of the spiritual leader of the Iranian Revo-

[22] International Institute for Strategic Studies (IISS), "Turkey's diminishing policy options in Syria", *IISS Strategic Comments* 7 (2016), p. 2.

[23] Jennifer Cafarella, "How Turkey Could Become the Next Pakistan", *Institute for the Study of War (ISW)*, (19 July 2016), available at http://www.understandingwar.org/backgrounder/how-turkey-could-become-next-pakistan (last visited 01 December 2017).

[24] On 26 November 2008, a well-trained squad of terrorists from *Lashkr-i-Tayyiba* assaulted several soft targets – public buildings and facilities – in India's metropolis of Mumbai. Heavily armed and equipped, they succeeded in taking hostages without a demand for ransom and killed 145 civilians. Knowing that they would certainly die as martyrs, the perpetrators were able to project an extreme potential of violence and destruction on public life in Mumbai. These kinds of complex terrorist attacks and intensively pre-planned martyr operations against multiple soft targets are the latest tactical innovation of modern terrorism and are often called urban siege or barricade hostage siege, frequently also named after their first appearance as 'Mumbai-style attacks.' See also Stephen Tankel, "Laskhar-i-Tayyiba – One Year After Mumbai", *Combating Terrorism Center (CTC) Sentinel* 11 (2009), pp. 1-5; John P. Sullivan and Adam Elkus, "Postcard from Mumbai, Modern Urban Siege" (16 February 2009), available at http://smallwarsjournal.com/mag/docs-temp/181-sullivan.pdf (last visited 01 December 2017); See Adam Dolnik, "From Sydney to Paris, The Return of Terrorist Barricade Hostage Incidents", *Combating Terrorism Center (CTC) Sentinel* 1 (2015), p. 5; see also Edwin Bakker and Liesbeth van der Heiden, *Mumbai-Style Attacks in Paris*, pp. 1-2.

[25] Marielle Ness, *Beyond the Caliphate: Islamic State Activity outside the Group's defined Wilayat – The Islamic State's Two-Pronged Assault on Turkey*, (Combating Terrorism Center, 2017), p. 3.

[26] Caitlin Forrest and Chris Kozak, "ISIS's Campaign in Turkey", *Institute for the Study of War (ISW)*, (30 June 2016), available at http://understandingwar.org/backgrounder/isiss-campaign-turkey (last visited 01 December 2017); See also Bunde et al., *Munich Security Report 2016: Boundless Crises, Reckless Spoilers, Helpless Guardians*, (Munich Security Conference Foundation, 2017), p. 18.

[27] Jack Watling, "The Shia Militias of Iraq", *The Atlantic*, (22 December 2016), available at https://www.theatlantic.com/international/archive/2016/12/shia-militias-iraq-isis/510938/ (last visited 01 December 2017); Anastasia Voronkova, *The IISS Armed Conflict Survey 2015*, pp. 95-97; Erik Holmquist, *ISIS and Hezbollah: Conduits of Instability*, pp. 32-34.

lution, Ayatollah Khomeini; two highly symbolic sites in Tehran. The hit team killed at least 12 people and injured more than 30, using automatic weapons and suicide vests. It was ISIS's most ambitious operation against Iran. ISIS has recently stepped up its propaganda against Iran as well – calling on Iran's Sunni minority to rise up against the regime in order to weaken Iran's Shia leadership by expanding Iraq's sectarian tension into Iran. [28]

The Strategic Dimension of ISIS's Terrorism

ISIS uses terrorism in a strategic dimension as a global-power instrument of retaliation. Europe is now regarded as a hostile alliance waging war against ISIS.[29] The organization has been continually extending the range of its attacks. In 2013, ISIS mainly carried out attacks in the Levant and adjacent countries; in the following year, as many as 19 different countries were affected by ISIS's terrorism and 2015 saw terrorist attacks in 33 different countries.[30] ISIS seeks retribution for the so-called 'crusaders' military action in Syria and Iraq. With this objective in mind, ISIS managed to carry out terrorist attacks in France and Belgium, both of which had joined the US-led coalition in September 2014. On 13 November 2015, a well-trained and heavily-armed group of ISIS *Inghimasi*[31] attacked in Paris, in a terrorist urban siege, resulting in the declaration of a state of emergency for the city. On that night, in the Paris neighborhood near the Saint-Martin canal, over a hundred people fell victim to professionally planned and brutally executed shooting attacks and multiple person-borne improvised explosive device (PBIED) explosions. In the Bataclan concert hall, dozens of civilian hostages were executed. At the time, it was the most devastating terrorist attack in Europe in decades.[32] With further attacks on an airport terminal and a subway station in Brussels near the seats of the European Parliament and NATO in March 2016, which left many people dead and hundreds injured, ISIS once again confirmed that the organization is able to carry out targeted large-scale attacks in Europe.[33] The planning and effective execution of these attacks demonstrated how professional ISIS underground cells operate. Firstly, they have shown that they have the necessary tactical knowledge to carry out terrorist attacks and bombings. Secondly, they have shown that they have secure hideouts from which to plan and prepare the attacks, as well as to store weapons and stolen cars. Finally, they have shown that they can prepare ways to go underground afterwards. During the lead-up to the attack,

[28] Chris Zambelis, "Terror in Teheran: The Islamic State Goes to War with the Islamic Republic", *Combating Terrorism Center (CTC) Sentinel* 6 (2017), pp. 16-20.

[29] Peter R. Neumann, *Die Neuen Dschihadisten: IS, Europa und die Nächste Welle des Terrorismus*, (Econ, 2015), p. 184.

[30] Erin Miller et al., *Patterns of Islamic State-Related Terrorism 2002-2015,* (National Consortium for the Study of Terrorism and Responses to Terrorism, 2016), p. 4.

[31] Terrorists prepared to die as martyrs.

[32] Jean-Charles Brisard, "The Paris Attacks and the Evolving Islamic State Threat to France", *Combating Terrorism Center (CTC) Sentinel* 11 (2015), p. 5; See Erin Miller, *Mass-Fatality, Coordinated Attacks Worldwide, and Terrorism in France*, p. 1; See also Edwin Bakker and Liesbeth van der Heiden, *Mumbai-Style Attacks in Paris*, pp. 1-2.

[33] Harleen Gambhir and Claire Coyne, "ISIS's Campaign in Europe", *Institute for the Study of War (ISW),* (25 March 2016), available at http://www.understandingwar.org/backgrounder/isiss-campaign-europe-march-2016 (last visited 01 December 2017).

they were able to travel back and forth undetected between Europe and the Caliphate territory.[34] The professional approach pursued by ISIS cells is a prime example of the 'urban guerrilla' concept developed by the Brazilian revolutionary Carlos Marighella (1911-1969). In Europe, only terrorist organizations such as the Irish Republican Army, the Red Brigades in Italy and the Red Army Faction in Germany were able to implement this concept to a similar degree. [35] At the beginning of 2013, military expert David John Kilcullen spoke about "the coming age of the urban guerrilla", which in his opinion would become the dominating method of terrorist attack against Europe.[36]

Apart from employing these professional groups of fighters, ISIS also made successful use of the 'lone wolf' strategy to attack Europe. As military pressure on ISIS increased and measures to prevent potential recruits from reaching the caliphate territory became more effective, ISIS adapted its recruitment tactics. It now declares that perpetrating a terrorist attack as a lone actor in the West is preferable to travelling to join the caliphate.[37] With this strategy, the organization has inspired several local, isolated perpetrators to commit targeted attacks, such as those against police officers and Christian clerics in France and Belgium.[38] During the French national holiday celebrations of 14 July 2016, a lone actor inspired by ISIS committed a particularly devastating act of terrorist mass murder in Nice in southern France by driving a cargo truck through a crowd of people.[39] In May 2016, former ISIS spokesman and propaganda chief Abu Muhammad al-Adnani (1977-2016)[40] called upon ISIS followers all over the world to carry out such simply structured attacks in the Western world, using simple means and makeshift weapons if necessary.[41] Many attacks over the last year have been carried out by individuals with no direct connection to ISIS; their only inspiration was the ideology.[42] In Germany, radicalized lone perpetrators were inspired to commit similar low-tech terrorist attacks using cut and thrust weapons, leaving several people injured. On 26 February 2016, a German-Moroccan girl attacked a federal police officer with a kitchen knife at Hannover central station, inflicting life-threatening injuries. In July 2016, an Afghan migrant attacked passengers in a local train with an axe and a knife. He injured five passengers. The assailant was shot by the police while fleeing. Subsequently, on 24 July 2016, a Syrian refugee blew himself up with a PBIED during a music festival in a Bavarian city, injuring 12 people. According to intelli-

[34] Daniel Benjamin and Steven Simon, "The Global Terror Threat in 2016: A Forecast", *Combating Terrorism Center (CTC) Sentinel* 9 (2016), p. 2; See Peter van Ostaeyen, "Belgian Radical Networks and the Road to the Brussels Attacks", p. 10.

[35] Jean-Charles Brisard, "The Paris Attacks and the Evolving Islamic State Threat to France", p. 5.

[36] David J. Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerilla*, (Oxford University Press, 2013), p. 52.

[37] European Police Office (EUROPOL), *European Union Terrorism Situation and Trend Report 2017 (TE-SAT)*, p. 25.

[38] Cato Hemmingby, '*Exploring the Continuum of Lethality: Militant Islamists' Targeting Preferences in Europe*, *Perspectives on Terrorism* 5 (2017), pp. 30-33.

[39] Rohan Gunaratna, *After Nice: The Threat Within Europe*, p. 1.

[40] According to US Department of Defense (DoD) information, Abu Muhammad Al-Adnani was killed by a US air strike on 30 August 2016 during an operation near the Syrian city of Aleppo. His death was confirmed by IS. See Thomas Joscelyn, "Islamic State Says Senior Official Killed in Aleppo Province", *The Long War Journal*, (30 August 2016), available at http://www.longwarjournal.org/archives/2016/08/islamic-state-says-senior-official-killed-in-aleppo-syria.php (last visited 01 December 2017).

[41] Peter Nesser et al., "Jihadi Terrorism in Europe: The IS-Effect", *Perspectives on Terrorism* 6 (2016), p. 12.

[42] Lorenzo Vidino et al., *Fear Thy Neighbor*, (LediPublishing, 2017), p. 65.

gence gathered by the German security authorities, this was the long-feared first ISIS suicide attack to take place in Germany.

In all these cases, the responsible law enforcement authorities were able to prove that the perpetrators had either communicated with ISIS beforehand or that they had been ideologically influenced by them. Although these were comparatively minor incidents, they nonetheless are significant incidents because they have had a highly polarizing and shocking effect on the post-heroic German society.[43] The deadliest terrorist attack in Germany took place on 21 December 2016. The attacker, again a lone perpetrator motivated by ISIS, hijacked a Polish truck, killed the driver and raced the vehicle through a crowded Christmas market in Berlin, killing 12 people.[44] It can probably be assumed that Europe's latest lone actor incidents in Stockholm, London, Manchester and Barcelona were inspired by ISIS's ideological propaganda.[45] Since the proclamation of their caliphate three years ago, ISIS has been responsible for more than 51 attacks in Europe, causing 395 deaths and no less than 1,549 injuries.[46]

The Russian Federation started to support the Syrian army with weapon supplies, training assistance and air force support on 30 September 2015, so it is therefore now also regarded as a strategic adversary by ISIS. Consequently, Russia has had to contend with retaliatory terrorist attacks. In October 2015, the detonation of a hidden improvised explosive device (IED) caused an A321 aircraft of a Russian airline to crash in Egypt. Shortly afterwards, ISIS claimed responsibility for the attack, stating that this act of terrorism had been committed in retaliation for the Russian Federation's entry into the war.[47] A similar pattern could be observed after the recapture of the Syrian city of Palmyra in March 2016. During the fighting, Russian armed forces had provided significant support to the regular Syrian army. Only a few days afterwards, ISIS retaliated for this continuation of direct military assistance with a vehicle-borne improvised explosive device (VBIED) attack against Russian police officers in Dagestan in the North Caucasus.[48] Additionally, on 3 April 2017, a PBIED-blast in Russia's old imperial metropolis of St. Petersburg killed at least 13 people and injured dozens more. The Chechen Mujahedeen group, the 'Imam Schamil Bataillon*'*, claimed responsibility for the bombing. The suicide bomber, a Kyrgyz-born Russian citizen, was most likely

[43] Robin Simcox, "The Islamic State's Western Teenage Plotters", *Combating Terrorism Center (CTC) Sentinel* 2 (2017), p. 21. See Florian Flade, "The Islamic State Threat to Germany: Evidence from the Investigations", *Combating Terrorism Center (CTC) Sentinel* 7 (2016), p. 13. See also European Police Office (EUROPOL), *European Union Terrorism Situation and Trend Report 2017 (TE-SAT)*, pp. 23-24.

[44] Georg Heil, "The Berlin Attack and the 'Abu Walaa' Islamic State Recruitment Network", *Combating Terrorism Center (CTC) Sentinel* 2 (2017), pp. 1-9.

[45] Joris van Wijk and Maarten P. Bolhuis, "Awareness Trainings and Detecting Jihadists among Asylum Seekers", *Perspectives on Terrorism* 4 (2017), p. 39; Raffaello Pantucci, "Britain on Alert: The Attacks in London and Manchester and the Evolving Threat", pp. 1-4; International Institute for Strategic Studies (IISS), "The Barcelona terrorist attack", pp. 1-3.

[46] Lorenzo Vidino et al., *Fear Thy Neighbor*, pp. 16-17.

[47] Fawaz A. Gerges, *ISIS: A History*, (Princeton University Press, 2016), p. 3. See also Robert Liscouski and William McGann, "The Evolving Challenges for Explosive Detection in the Aviation Sector and Beyond", *Combating Terrorism Center (CTC) Sentinel* 5 (2016), p. 1.

[48] Christian Lowe et al., "Russia police say blast kills officer, Islamic State claims responsibility", (30 March 2016), *Reuters*, available at http://www.reuters.com/article/us-russia-car-blast-idUSKCN0WW0M6 (last visited 01 December 2017).

supported by ISIS's transregional network. Due to this, Russian officials termed the incident to be a hybrid Chechen rebel-ISIS attack.[49]

The ISIS caliphate has even managed to reach US soil with its terrorist attacks. In San Bernardino, California, several people were killed in December 2015 by two ISIS-inspired assailants armed with automatic rifles. In June 2016, another ISIS-inspired attacker conducted a shooting rampage in an Orlando nightclub, killing 49 civilians. It was the most devastating terrorist act of violence committed in the US since 11 September 2001.[50] And on 31 October 2017 a lone perpetrator, who had pledged allegiance to ISIS, killed 8 people and badly injured 12 pedestrians in Manhattan, New York by vehicular attack.[51] With this Halloween truck attack, ISIS once again managed to attack the US to prove its global strategic reach.

Terrorism as ISIS's Universal Instrument

Despite what is often said, the fact that ISIS commits terrorist attacks against its opponents does not signify that they are acting like a wounded beast. On the contrary, the organization is acting rationally to deliberately employ terrorism against its strategic adversaries. Spectacular terrorist actions capture the public's attention, designed to create the image of ISIS as a powerful and fearsome caliphate and as the leading terrorist organization worldwide. Moreover, these terrorist attacks enable ISIS to constantly demonstrate its clout and global power.[52] All in all, it is apparent that the extremist organization can systematically employ terrorist attacks for several purposes: to demoralize opposing forces, to destabilize adjacent regions and adversary states and also to retaliate against superior alliances. ISIS's terrorism is a particularly effective and universal instrument to generate effects on different levels. Since it came into being, ISIS has been responsible for more than 5,000 terrorist attacks worldwide.[53] In 2016, ISIS remained the deadliest terrorist organization, carrying out more than 1,400 attacks that resulted in more than 7,300 deaths.[54]

Although international coalitions have made significant progress in the fight against ISIS, the organization's ability to commit terrorist attacks and its global reach have not yet been diminished.

[49] Damien Sharkov, "Four Questions about the St. Petersburg Attack Answered", (04 April 2017), *Newsweek*, available at http://www.newsweek.com/four-questions-about-st-petersburg-attack-answered-578818 (last visited 01 December 2017).

[50] Jessica D. Lewis McFate and Melissa Pavlik, "ISIS's Global Attack Network: November 13, 2015-November 9, 2016", *Institute for the Study of War (ISW),* (13 November 2016), available at http://iswresearch.blogspot.de/2016/11/isiss-global-attack-network-november-13.html (last visited 01 December 2017).

[51] Renae Merle, Devlin Barrett and Mark Berman, "New York Truck Attacker Planned for Weeks and Carried out Rampage in the Name of ISIS, Officials say", *The Washington Post*, (01 November 2017), available at https://www.washingtonpost.com/news/post-nation/wp/2017/11/01/new-york-attack-probe-expands-to-uzbekistan-as-possible-militant-links-explored/?utm_term=.42f23763d165 (last visited 01 December 2017).

[52] Florian Flade and Alfred Hackensberger, "Wie eine Verwundete Bestie", *Die Welt*, (27 March 2016), available at http://www.welt.de/print/wams/politik/article153708574/Wie-eine-verwundete-Bestie.html (last visited 01 December 2017).

[53] This number includes attacks committed by regional insurgent groups who have sworn religious and political allegiance, the Bay'a, to the IS. See Erin Miller et al., *Patterns of Islamic State-Related Terrorism 2002-2015,* p. 4.

[54] Erin Miller et al., *Overview: Terrorism in 2016,* p. 2.

With the targeted strategic attacks of Paris, Brussels, Nice, Berlin, Stockholm, London, Manchester and Barcelona, ISIS has succeeded in inspiring fear and horror in Europe and in threatening Western societies. The organization has been able to prove its power and to thus underpin the legitimacy of its self-declared caliphate. Power projections achieved by means of strategic terrorist attacks are an excellent opportunity for ISIS to assert itself as the outstanding global representative of extremists claiming affiliation with Islam.[55] In particular, the roughly 30 to 40 percent[56] of the 5,000 Europeans who have fought for ISIS abroad and presumably returned to their home countries enable ISIS to commit further attacks in Europe.[57] Some of these returning foreign ISIS fighters are disillusioned; others, however, remain loyal to ISIS and its cause; they could form more groups of urban guerrillas in European cities.[58] According to estimates by European police authorities, hundreds of these returnees, among them women, are prepared to carry out terrorist attacks in Europe. Therefore ISIS may be able to turn out masses of well-trained *Inghimasi*s who are prepared to die as martyrs. These fighters would then only have to be smuggled into the countries to carry out their mission. In this respect, the continuing migration and refugee crisis facilitates a quick, cost-effective and targeted transfer of prepared fighters to Europe.[59] At the same time, the huge amount of violent propaganda continuously disseminated by ISIS leads to a radicalization of disoriented Muslims, turning them into ideologically motivated insurgent fighters. These lone actors would then commit terrorist attacks against Western societies to obey the call to arms of their caliph Abu Bakr al-Baghdad: “Never allow the crusaders and apostates to enjoy a life of peace and security in their homes at the same time your brothers taste the bitterness of strikes and destruction.”[60]

Conclusion

Because ISIS claims global influence, it is highly probable that the organization has already prepared and planned for an imminent fall of their strongholds and safe havens in the Levant. While constantly conducting delaying actions to wear down its opponents in Iraq and Syria, ISIS will presumably reorganize their caliphate’s leadership and its ideology in order to transfer it to new

[55] Daniel Benjamin and Steven Simon, “The Global Terror Threat in 2016: A Forecast”, pp. 1.

[56] The Organization for Security and Co-operation in Europe (OSCE) assessed that between 40 and 50 percent of the foreign fighters are still fighting for ISIS in Syria and Iraq. Approximately 25 percent were killed. It can be estimated that nearly 40 percent have returned already to Europe. Peter R. Neumann, *Countering Violent Extremism and Radicalisation that Lead to Terrorism: Ideas, Recommendations, and Good Practices from the OSCE Region*, p. 74.

[57] Bibi van Ginke and Eva Entenmann, *The Foreign Fighters Phenomenon in the European Union: Profiles, Threats and Policies*, (International Center for Counter-Terrorism, 2016), p. 13.

[58] Tobias Bunde et al., *Munich Security Report 2016: Boundless Crises, Reckless Spoilers, Helpless Guardians*, p. 18.

[59] European Police Office (EUROPOL), *European Union Terrorism Situation and Trend Report (TE-SAT) 2016*, p. 22; European Police Office (EUROPOL), *Changes in Modus Operandi of Islamic State terrorist attacks: Review held by experts from Member States and Europol*, p. 3.

[60] Sam Mullins, “The Road to Orlando: Jihadist-Inspired Violence in the West, 2012-2016”, *Combating Terrorism Center (CTC) Sentinel* 6 (2016), p. 29; see Jessica Stern and J.M. Berger, *ISIS: The State of Terror*, p. 195; Frederick W. Kagan et al., *Al Qaeda and ISIS: Existential Threats to the U.S. and Europe*, p. 24; Louisa Loveluck, “ISIS releases audio it claims to be of leader Abu Bakr al-Baghdadi”, *The Washington Post*, (28 September 2017), available at https://www.washingtonpost.com/world/isis-releases-recorded-message-purportedly-from-baghdadi/2017/09/28/c749a14a-a470-11e7-ade1-76d061d56efa_story.html?utm_term=.ffb189d60f38 (last visited 01 December 2017).

provinces (*Wilayats*). The branches in North Africa – especially the Egypt-based ISIS affiliate *Wilayat Sinai*, where the terrorist organization was able to conduct its most devastating attack, killing at least 305 people at the Al Rawda in the city of Bir al-Abed – are particularly well set up and would thus probably be most suitable for this purpose.[61] While shifting and reorganizing its efforts in this way, ISIS will noticeably increase its strategic terrorist activities against Europe, and maybe even against Russia and the US, to retaliate for and deter further military involvement on the part of these countries. This approach will also enable ISIS to secure a power base, to demonstrate strength and to protect its new headquarters.[62] In this context, the lone wolf strategy will presumably be the preferred method to carry out future terrorist attacks in Europe.[63] It may well turn out that these attacks are merely intended to overburden the security agencies, and that other professional attacks on a much larger scale are already being planned to further paralyze Western societies. The latest low technology attack in Barcelona, for instance, is approved to be the hasty contingency plan of a sophisticated terrorist cell. Their accidently destroyed IED facility was most likely built for a larger plot – to destructively strike the famous Spanish basilica *Sagrada Familia* and to create Europe's 9/11.[64]

Thus, ISIS will evolve from a protostate with fixed safe havens into a clandestine movement, a transnational terrorist threat network with no protostate features dispersed throughout the region and the global, which will seek its new battlefield in Europe. This is eminently possible and poses the most dangerous scenario. Broader intranational intelligence and law enforcement cooperation will remain operational priority for Europe's security agencies. However, despite their best attempts, it is inevitable that a few terrorist attacks will succeed, so European societies will also have to work on their resilience.[65] The longer ISIS prevails in Iraq and Syria, and the more support it gets from people in other countries, the more difficult it will be to defeat.[66] While finally destroying their caliphate may be a significant victory, it will not be a decisive one. ISIS after the caliphate may inspire more and increasing violence. It can be anticipated that the fight against ISIS will be a difficult and lengthy war against terrorism, its ideology and roots. The worldwide insurgency will go on. [67]

[61] Geoff D. Porter, "What to Make of the Bay'a in North Africa?", pp. 14-17; Nelly Lahoud, "The Province of Sinai: Why Bother with Palestine if You Can Be Part of the 'Islamic State'?", pp. 12-14; Michael Horton, "Crossing the Canal: Why Egypt Faces a Creeping Insurgency", p. 22; Jacob Zenn, "A Biography of Boko Haram and the Bay'a to al-Baghdadi", pp. 19-21.

[62] Paul Cruickshank and Brian Dodwell, "A View from the CT Foxhole: An Interview with John Brennan, Director CIA", p. 3; Caitlin Forrest, *ISIS's Global Strategy: Ramadan 2016*, p. 1; Andres Watkins, "Losing Territory and Lashing Out: The Islamic State and International Terror", p. 17.

[63] European Police Office (EUROPOL), *European Union Terrorism Situation and Trend Report (TE-SAT) 2016*, p. 26.

[64] International Institute for Strategic Studies (IISS), "The Barcelona terrorist attack", pp. 2-3.

[65] Phil Gurski, "An Era of Near Unstoppable Terrorism?", *International Centre for Counter-Terrorism* (29 August 2017), available at https://icct.nl/publication/an-era-of-near-unstoppable-terrorism/ (last visited 01 December 2017).

[66] Bryan Price, "A View from the CT Foxhole: The Honorable Juan C. Zarate, former Deputy National Security Advisor for Combating Terrorism", p. 12; Jessica D. Lewis McFate, "The Islamic State Digs In", p. 7.

[67] Nelly Lahoud, *How will the Islamic State endure?*, *The International Institute for Strategic Studies* (31 October 2017), available at https://www.iiss.org/en/politics and strategy/blogsections/2017-6dda/october-f3ac/how-will-the-islamic-state-endure-b482 (last visited 01 December 2017); See Thomas R. McCabe, "The Islamic State After the Caliphate - Can IS Go Underground?", p. 99; See also Muhammad Al-'Ubaydi et al., *The Group That Calls Itself a State: Understanding the Evolution and Challenges of the Islamic State*, p. 7.

BIBLIOGRAPHY

Al-'Ubaydi, Muhammad Nelly Lahoud, Daniel Milton and Bryan Price, *The Group That Calls Itself a State: Understanding the Evolution and Challenges of the Islamic State* (Combating Terrorism Center, 2014).

Anagnostos, Emily, "Iraq Situation Report – September 7-19, 2016", *Institute for the Study of War (ISW)*, (19 September 2016).

Anagnostos, Emily, "Iraq Situation Report – June 29-July 6", *Institute for the Study of War (ISW)*, (05 July 2016).

Bakker, Edwin and Liesbeth van der Heiden, *Mumbai-Style Attacks in Paris* (International Center for Counter-Terrorism, 2015).

Benjamin, Daniel and Steven Simon, "The Global Terror Threat in 2016: A Forecast", *Combating Terrorism Center (CTC) Sentinel* 9 (2016).

Brisard, Jean-Charles, "The Paris Attacks and the Evolving Islamic State Threat to France", *Combating Terrorism Center (CTC) Sentinel* 11 (2015).

Bunde, Tobias, Benedikt Franke, Vera Lamprecht, Adrian Oroz, Lisa Marie Ullrich and Kai Wittek, *Munich Security Report 2016: Boundless Crises, Reckless Spoilers, Helpless Guardians* (Munich Security Conference Foundation, 2017).

Cafarella, Jennifer, "How Turkey Could Become the Next Pakistan", *Institute for the Study of War (ISW)*, (19 July 2016).

Cockburn, Patrick, *ISIS: Battling the Menace* (Independent Print Limited, 2016)

Cooper, Kevin and Emily Anagnostos, "Iraq Situation Report – November 9-17, 2016", *Institute for the Study of War (ISW)*, (17 November 2016).

Cruickshank, Paul and Brian Dodwell, "A View from the CT Foxhole: An Interview with John Brennan, Director CIA", *Combating Terrorism Center (CTC) Sentinel* 9 (2016).

Dolnik, Adam, "From Sydney to Paris, The Return of Terrorist Barricade Hostage Incidents", *Combating Terrorism Center (CTC) Sentinel* 1 (2015).

European Police Office (EUROPOL), *European Union Terrorism Situation and Trend Report (TE-SAT) 2017* (EUROPOL, 2017).

European Police Office (EUROPOL), *European Union Terrorism Situation and Trend Report (TE-SAT) 2016* (EUROPOL, 2016).

European Police Office (EUROPOL), *Changes in modus operandi of Islamic State terrorist attacks: Review held by experts from Member States and Europol* (EUROPOL, 2016).

Flade, Florian, "The Islamic State Threat to Germany: Evidence from the Investigations", *Combating Terrorism Center (CTC) Sentinel* 7 (2016).

Flade, Florian and Alfred Hackensberger, "Wie eine verwundete Bestie", *Die Welt* (27 March 27, 2016).

Forrest, Caitlin and Chris Kozak, "ISIS's Campaign in Turkey", *Institute for the Study of War (ISW)*, (30 June 2016).

Forrest, Caitlin, *ISIS's Global Strategy: Ramadan 2016* (Institute for the Study of War, 2016).

Friedman, Uri, "Is Terrorism Getting Worse? It depends where you look", *The Atlantic*, (14 July 2016).

Fulton, Will, Joseph Holliday and Sam Wyer, "Iran's Strategy in Syria", *Institute for the Study of War (ISW),* (25 March 2016).

Gambhir, Harleen and Claire Coyne, "ISIS's Campaign in Europe", *Institute for the Study of War (ISW),* (25 March 2016).

Gerges, Fawaz A., *ISIS: A History* (Princeton University Press, 2016).

Ginke, Bibi van and Eva Entenmann, *The Foreign Fighters Phenomenon in the European Union: Profiles, Threats and Policies* (International Center for Counter-Terrorism, 2016).

Gunaratna, Rohan, *After Nice: The Threat Within Europe* (S. Rajaratnam School of International Studies, 2016).

Gurski, Phil, "An Era of Near Unstoppable Terrorism?", *International Centre for Counter-Terrorism*, (29 August 2017).

Heil, Georg, "The Berlin Attack and the 'Abu Walaa' Islamic State Recruitment Network", *Combating Terrorism Center (CTC) Sentinel* 2 (2017).

Hemmingby, Cato, "Exploring the Continuum of Lethality: Militant Islamists' Targeting Preferences in Europe", *Perspectives on Terrorism* 5 (2017).

Hermann, Rainer, *Endstation Islamischer Staat? – Staatsversagen und Religionskrieg in der arabischen Welt* (dtv Verlagsgesellschaft, 2015).

Holmquist, Erik, *ISIS and Hezbollah: Conduits of Instability* (Swedish Defence Research Agency, 2015).

Horton, Michael, "Crossing the Canal: Why Egypt Faces a Creeping Insurgency", *Combating Terrorism Center (CTC) Sentinel* 6 (2017).

Institute for Economics and Peace (IEP), *Global Terrorism Index 2015 – Measuring and Understanding the Impact of Terrorism* (Institute for Economics and Peace, 2015).

International Institute for Strategic Studies (IISS), "The Barcelona terrorist attack", *IISS Strategic Comments* 30 (2017).

International Institute for Strategic Studies (IISS), "Turkey's diminishing policy options in Syria", *IISS Strategic Comments* 7 (2016).

Joscelyn, Thomas, "Islamic State says senior official killed in Aleppo province", *The Long War Journal*, (30 August 2016).

Kagan, Frederick W., Kimberly Kagan, Jennifer Cafarella, Harleen Gambhir and Katherine Zimmerman, *Al Qaeda and ISIS: Existential Threats to the U.S. and Europe* (Institute for the Study of War, 2016).

Kalic, Sean N., "Terrorism in the twenty-first century", *An International History of Terrorism: Western and non-western Experiences* (Hanhimäki, Jussi M. and Bernhard Blumenau, eds., Routledge, 2013).

Kilcullen, David J., *Out of the Mountains: The Coming Age of the Urban Guerilla* (Oxford University Press, 2013).

Knights, Michael, "ISIL's Political-Military Power in Iraq", *Combating Terrorism Center (CTC) Sentinel* 8 (2014).

Lahoud, Nelly, "How will the Islamic State endure?", *The International Institute for Strategic Studies*, (31 October 2017).

Lahoud, Nelly, "The Province of Sinai: Why Bother with Palestine if You Can Be Part of the 'Islamic State'?", *Combating Terrorism Center (CTC) Sentinel* 3 (2015).

Lewis McFate Jessica D. and Melissa Pavlik, "ISIS's Global Attack Network: November 13, 2015-November 9, 2016", *Institute for the Study of War (ISW),* (13 November 2016).

Lewis McFate, Jessica D. and Alexandra Gutowsko, "ISIS's Capable Defense of Mosul – Counteroffensives in Kirkuk, Rutbah, and Sinjar", *Institute for the Study of War (ISW)*, (06 July 2016).

Lewis McFate, Jessica D., "The Islamic State Digs In", *Combating Terrorism Center (CTC) Sentinel* 10 (2015).

Liscouski, Robert and William McGann", The Evolving Challenges for Explosive Detection in the Aviation Sector and Beyond", *Combating Terrorism Center (CTC) Sentinel* 5 (2016).

Lister, Charles, "Assessing Syria's Jihad", *Middle Eastern Security: The US Pivot and the Rise of ISIS* (Dodge, Toby and Emile Hokayem, eds., Routledge, 2014).

Loveluck, Louisa, "ISIS releases audio it claims to be of leader Abu Bakr al-Baghdadi", *The Washington Post*, (28 September 2017).

Lowe, Christian, Vladimir Soldatkin and Maria Tsvektova, "Russia police say blast kills officer, Islamic State claims responsibility", (30 March 2016), *Reuters*.

Lüders, Michael, *Wer den Wind sät: Was westliche Politik im Orient anrichtet,* (C.H. Beck, 2016).

Martin, Patrick, Hannah Werman and Emily Anagnostos, "Iraq Situation Report – May 11-24, 2016", *Institute for the Study of War (ISW)* (25 May 2016).

Martin, Patrick "Iraq Situation Report, March 29-April 4, 2016", *Institute for the Study of War (ISW)*, (04 April 2016).

McCabe, Thomas R. "The Islamic State After the Caliphate - Can IS Go Underground?", *Perspectives on Terrorism* 4 (2017).

Merle, Renae, Devlin Barrett and Mark Berman, "New York truck attacker planned for weeks and carried out rampage in the name of ISIS, officials say", *The Washington Post*, (01 November 2017).

Miller, Erin, *Background Report*, *Overview: Terrorism in 2016* (National Consortium for the Study of Terrorism and Responses to Terrorism, 2017).

Miller, Erin, *Mass-Fatality, Coordinated Attacks Worldwide, and Terrorism in France* (National Consortium for the Study of Terrorism and Responses to Terrorism, 2015).

Miller, Erin, Sheehan Kane, William Kammerer and Brian Wingenroth, *Patterns of Islamic State-Related Terrorism 2002-2015* (National Consortium for the Study of Terrorism and Responses to Terrorism, 2016).

Milton, Daniel, Price, Bryan; and Al-'Ubaydi, Muahammad, "The Islamic State in Iraq and the Levant: More than Just a June Surprise", *Combating Terrorism Center (CTC) Sentinel* 6 (2014).

Mullins, Sam, "The Road to Orlando: Jihadist-Inspired Violence in the West, 2012-2016", *Combating Terrorism Center (CTC) Sentinel* 6 (2016).

Münkler, Herfried, "Terrorismus heute: Die Asymmetrierung des Krieges", *Internationale Politik* 2 (2004).

Nance, Malcom W., *Defeating ISIS: Who They are, How They Fight, What They Believe* (Skyhorse Publishing, 2016).

Ness, Marielle, *Beyond the Caliphate: Islamic State Activity outside the Group's defined Wilayat – The Islamic State's Two-Pronged Assault on Turkey* (Combating Terrorism Center, 2017).

Nesser, Peter, Anne Stenersen and Emilie Oftedal, "Jihadi Terrorism in Europe: The IS-Effect", *Perspectives on Terrorism* 6 (2016).

Neumann, Peter R., *Countering Violent Extremism and Radicalisation that Lead to Terrorism: Ideas, Recommendations, and Good Practices from the OSCE Region* (Organisation for Security and Co-operation in Europe, 2017*).*

Neumann, Peter R., *Die neuen Dschihadisten: IS, Europa und die nächste Welle des Terrorismus* (Econ, 2015).

Ostaeyen, Peter van, "Belgian Radical Networks and the Road to the Brussels Attacks", *Combating Terrorism Center (CTC) Sentinel* 9 (2016).

Pantucci, Raffaello, "Britain on Alert: The Attacks in London and Manchester and the Evolving Threat", *Combating Terrorism Center (CTC) Sentinel* 7 (2017).

Porter, Geoff D., "What to Make of the Bay'a in North Africa?", *Combating Terrorism Center (CTC) Sentinel* 3 (2015).

Price, Bryan, "A View from the CT Foxhole: The Honorable Juan C. Zarate, former Deputy National Security Advisor for Combating Terrorism", *Combating Terrorism Center (CTC) Sentinel* 4 (2016).

Reuther, Christoph, *Die Schwarze Macht: Der Islamische Staat und die Strategen des Terrors* (Deutsche Verlags-Anstalt, 2015).

Sharkov, Damien, "Four Questions About The St. Petersburg Attack Answered", *Newsweek*, (04 April 2017).

Simcox, Robin, "The Islamic State's Western Teenage Plotters", *Combating Terrorism Center (CTC) Sentinel* 2 (2017).

Steinberg, Guido, *Kalifat des Schreckens: IS und die Bedrohung durch den islamistischen Terror* (Knaur TB, 2015).

Stern, Jessica and J.M. Berger, *ISIS: The State of Terror* (Ecco, 2015).

Sullivan, John P. and Adam Elkus, "Postcard from Mumbai, Modern Urban Siege", *Small Wars Journal,* (16 February 2009).

Tankel, Stephen, "Laskhar-i-Tayyiba – One Year After Mumbai", *Combating Terrorism Center (CTC) Sentinel* 11 (2009).

Vidino, Lorenzo; Marone, Francesco and Entenmann, Eva, *Fear Thy Neighbor: Radicalization and Jihadist Attacks in the West* (LediPublishing, 2017).

Voronkova, Anastasia, *The IISS Armed Conflict Survey 2015* (The International Institute for Strategic Studies, 2017).

Watkins, Andres, “Losing Territory and Lashing Out: The Islamic State and International Terror”, *Combating Terrorism Center (CTC) Sentinel* 3 (2016).

Watling, Jack, “The Shia Militias of Iraq”, *The Atlantic*, (22 December 2016).

Van Wijk, Joris and Maarten P. Bolhuis, “Awareness Trainings and Detecting Jihadists among Asylum Seekers - A Case Study from The Netherlands”, *Perspectives on Terrorism* 4 (2017).

Zambelis, Chris, “Terror in Tehran: The Islamic State Goes to War with Islamic Republic”, *Combating Terrorism Center (CTC) Sentinel* 6 (2017).

Zenn, Jacob, “A Biography of Boko Haram and the Bay’a to al-Baghdadi”, *Combating Terrorism Center (CTC) Sentinel* 3 (2015).

PUBLISHING PRINCIPLES

Articles sent to the ***Defence Against Terrorism Review*** must not be published elsewhere or must not have been sent to another publication in order to be published. Once the articles are submitted to DATR, the authors must acknowledge that they cannot submit their articles to other publications unless the total rejection of concerned articles by the Editor or the Endorsement Committee (EC).

A. GENERAL PRINCIPLES

1. Language of publication is English. The texts submitted must be clear and understandable, and be in line with scientific/academic criteria in terms of language, expression and citation.
2. The texts submitted to be published should be between 4000 and 12000 words (approximately 10-30 pages), including the abstract and bibliography.
3. The texts must be submitted together with an abstract no longer than 300 words at the beginning of the paper and with five keywords after the abstract.
4. The name of the author must be placed in the first footnote, with his/her title, place of duty and e-mail address. Footnotes for other explanations must be provided both in the text and down the page in numbers.
5. The type character must be Arial, "11 type size", line spacing "1,5 nk", footnotes in "9 type size" and with "single" line spacing.

General Contents

The following are general stylistic conventions used by COE-DAT:

1. Writing should be scholarly in nature and not overly conversational. Do not use "I" or "we" but "the author" or the "authors."
2. Do not use contractions except in quotes.
3. Except in quotes, do not underline or bold text to emphasize it but instead use word order for emphasis. To highlight a term, show the key words in single mark ('aerospace').
4. Use italic font for foreign phrases and names of court cases.
5. For dates, use – date month year format (10 March 2011) – not numbers (10/03/11). In footnotes, dates of the sources may follow the format used in the source.
6. There should be only one space between the period at the end of a sentence and the beginning of the next sentence.
7. Acronyms should be defined when first used with the full name in parentheses after the acronym; acronyms in foreign languages should have the name in the foreign first in parentheses, followed by the English translation. If an acronym has been defined once in the text of the article, it is unnecessary to spell it out again either in text or footnotes.
8. Numbers less than twenty or less should be spelled out; numbers 21 and above should be left in numbers.
9. Values in currency should be quoted in the actual currency followed by the amount in dollars (USD) or euros (€) in parentheses.
10. While making quotations;

a. If the part taken from the source is 4 lines and less than 4 lines, quotation marks ("...sentence...") can be used.

b. If the part taken from the source is more than 4 lines, it must be given with extra indentations.

- In addition, the writer of the article must avoid excessive use of each source, in particular from their own previous writings.

B. PRINCIPLES AS TO PAGE LAYOUT

Formatting: Double-spaced with standard page margins. The text and all headings should be left justified. Set language as American English. The publisher employed by COE-DAT uses a particular document formatting that will be applied by the editors.

C. PRINCIPLES AS TO REFERENCES AND CITATIONS

Citations shall be given down the pages in numbers in ***Defence Against Terrorism Review*** and references shall not be presented in the text (e.g. Waltz, 2009: 101.).

Full identity of the resources cited shall be given; any resource not actually cite shall not be presented in the bibliography.

Format for footnote citations;

1. For Books

a. Books with Single Author:

Name and surname of the author, *name of work* ("volume no" if applicable, translator if any, publisher and date of publication), page number(s).

Joseph Needham, *Science and Civilization in China*, (Vol. 5, Cambridge Univ. Pres, 1954), p. 7.

Joseph Needham, Science in Traditional China (Harvard Univ. Pres, 1981), p. 37.

b. Books with Two or Three Authors:

Name and surname of the first author, name and surname of the second author, name and surname of the third author, *name of work* ("volume no" if applicable, translator if any, publisher and date of publication), page number(s).

Joseph S. Nye Jr. and David A. Welch, *Understanding Global Conflict and Cooperation,* (Pearson Publication, 2011), p. 280.

c. Books with More Than Three Authors:

Name and surname of the first author et. al., *name of work* ("volume no" if applicable, translator if any, publisher and date of publication), page number(s).

Luis Benton et. al., *Informal Economy,* (The John Hopkins University Press, 1989), pp. 47-59.

d. Books with Name of Author or Editor Non-Specified:

Redefining Security (Praeger Publication, 1998), p. 81.

2. For Articles

Name and surname of the author (for all authors if two or three, if more than three authors just for the first author and et. al.), "name of the article" (translator if any), *name of periodical in which it is published,* volume number (issue) (publication year), pages in journal, cited page number.

a. Articles with One Author:

Barry Buzan, "New Patterns of Global Security in the Twenty-First Century," *International Affairs* 67(3) (1991), pp. 431-451, p. 442.

b. Articles in Compilation Books:

Barry Buzan, “Is International Security Possible?”, in *New Thinking About Strategy and International Security* (Ken Botth and Don Kaufman, eds, Harper Collins, 1991), pp. 31-55, p. 42.

c. Articles from Daily Newspapers:

Yossi Melman, “Computer Virus in Iran Actually Targeted Larger Nuclear Facility”, *Haaretz* (22 September 2011), p. 7.

“Tehran’s nuclear ambitions”, *The Washington Post* (26 September 2009), p. 5.

3. For Theses

No italics shall be used for the titles of non-published theses. Name and surname of the author, “title of the thesis” (whether it has been published and academic degree of the thesis, institution and institute of the thesis, date of the thesis), page number.

Atasay Özdemir, “Approaches of the Effective Actors of the International System to Iran’s Nuclear Programme” (Unpublished Doctoral Thesis, War College Strategic Researchs Institute, Istanbul, 2013), p. 22.

4. For Reports

a. Report with Author Specified

Tariq Khaitous, “Arab Reactions to a Nuclear Armed Iran” (Washington Institute for Near East Policy, Policy Focus 94, June 2009), p. 14.

b. Report with Author Non-Specified

Albania Country Report (TİKA Publishing, 1995), p. 7.

c. Report prepared by an Institution, Firm or Institute

American Petroleum Institute, “Drilling and Production Practice Proceedings of the Spring Meeting” (Shell Development Company, 1956), p. 42.

d. For Internet Resources

If any of the above resources are available on the Internet, follow the citation above with “available at” with the full http address and the date accessed in paratheses

e. Web Pages

“The World Factbook-Turkey,” Central Intelligence Agency, at https://www.cia.gov/library/publications/the-world-factbook/geos/tr.htm (accessed 25 February 2013).

“Dimona: Negev Nuclear Research Center,” Global Security, at http://www.globalsecurity.org/wmd/world/israel/dimona.htm (accessed 11 January 2010).

“Russia’s National Security Strategy to 2020” (12 May 2009), Rustrans, at http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020 (accessed 02 May 2011).

5. Subsequent citations of the same source:

a. If the citation is to the footnote directly before, use “Ibid” – if the page or paragraph changes, you can add the new informatıın, as in “Ibid, p. 48” or Ibid, para. 68).

b. If the source is earlier than the previous one, use the author’s last name (if there is one), followed by the name of the article, followed by the new page or paragraphe number.

Buzan, “Is International Security Possible?”, p. 48.

D. PRINCIPLES TO ABIDE BY IN USING OF DOCUMENTS, TABLES, FIGURES AND GRAPHICS

1. Attachments (documents), shall be presented at the end of the text and down below shall be a brief information as to the content of the document and proper citation in line with the relevant criteria.

2. Other attachments (Table, Figure and Graphics) shall be presented as Additional Table: 1, Additional Graphic: 3 and Additional Figure: 7. If indicators other than the text are too many in number; attachments shall be presented after the References.

a. References to these attachments in the text shall absolutely be made as Additional Table: 1, Additional Graphic: 3 or Additional Figure: 7.

b. If citation has been made for table, figure, graphic or picture, the source shall absolutely be indicated.

3. The names of the tables within the text shall be written on the top of the table and these tables shall be cited in the footnote according the publication type from which it was cited.

4. The names of the figures, graphics and maps within the text shall be written at the bottom of the figures, graphics and maps and these figures, graphics and maps shall be citied in the footnote according the publication type from which it was cited.

E. PRINCIPLES TO ABIDE BY IN BIBLIOGRAPHY

1. Just like giving citations but this time surname of the fauthor shall be at the beginning.
2. Resources shall be sorted alphabetically from A to Z.
3. Page numbers shall not be indicated.