

Katarzyna MANISZEWSKA, Paulina PIASECKA Editors

SECURITY AND SOCIETY




IN THE INFORMATION AGE



Collegium
Civitas

Katarzyna MANISZEWSKA, Paulina PIASECKA Editors

SECURITY
AND
SOCIETY
IN THE INFORMATION AGE



SRAS

Collegium
Civitas

COLLEGIUM CIVITAS

„Security and Society in the Information Age” publication is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License under the following terms – you must keep this information and credit Collegium Civitas as the holder of the copyrights to this publication.



To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/4.0/>

Reviews:

Dobrosław Mąka, PhD (Wyższa Szkoła Biznesu i Przedsiębiorczości
w Ostrowcu Świętokrzyskim, Collegium Civitas)
Tomasz Serafin, PhD (Collegium Civitas)

Editors: Katarzyna Maniszewska, PhD and Paulina Piasecka, PhD
Proofreader: Victoria Prince

ISBN print 978-83-61067-87-0
e-ISBN 978-83-61067-90-0

DOI 10.6084/m9.figshare.7454207

Publisher: Collegium Civitas Press
Palace of Culture and Science, XI floor
00-901 Warsaw, 1 Defilad Square
tel. +48 22 656 71 96
e-mail: wydawnictwo@civitas.edu.pl
<http://www.civitas.edu.pl>

Cover design, typesetting and text makeup:
Ważka Łukasz Piotrowski
03-138 Warszawa, Strumykowa 6b/73

Contents

Opening Remarks	5
CHAPTER 1 A Different Way to Approach Disinformation: Collective Impact Quinn Harty	7
CHAPTER 2 A Violent Psyche Bianca Canal	16
CHAPTER 3 Retweeting Radicalization: Radicalization and Recruitment to Terrorist Organizations in the Information Age Nicole Wojtkiewicz	25
CHAPTER 4 Can We Identify the Next Shooter? Preventing Mass Shootings and Active Shooters by Identifying Concerning Behaviors of the Shooter Prior to the Attack Casey Guthrie	35
CHAPTER 5 Framing Grey Area Violence in Media and Politics: A Framework for Decision Making Abigail Kuchek	44

CHAPTER 6 "If it Bleeds it Leads": How Mainstream Media Shapes Public Opinion on Terrorism Hazal Bulut	54
CHAPTER 7 United States Mass Shootings Placed in Context with Media and Public Discussion Charles Schmidt	61
CHAPTER 8 Defend and Collaborate: Information Security Considerations for Every Business Organization Jacob M. Schmitt	82
CHAPTER 9 Hybrid threats – how is the security environment in Central and Eastern Europe changing? Krzysztof Liedel	92
CHAPTER 10 The narrative of terrorism: evolution of the message of violence Paulina Piasecka	101
CHAPTER 11 Digital technologies for the protection of cultural heritage in the 21st century Katarzyna Góralczyk and Katarzyna Zielińska	112
CHAPTER 12 Success Factors of Islamic State Propaganda Wojciech Szewko	120
Bibliography	131
Authors' notes	145

Dear Reader

It is our pleasure to present this unique publication – composed of papers written by talented young American students – participants in the Summer School Program “Security and Society in the Information Age” and by experts cooperating with the Terrorism Research Center at Collegium Civitas University in Warsaw, Poland.

The Summer School Program “Security and Society in the Information Age” is organized in Warsaw jointly by Collegium Civitas and SRAS (USA). The Program aims to present global topics from the unique perspective of Central and Eastern Europe. Courses devoted to a wide range of history and security issues are designed with the region serving as a case study. They are taught in English and are aimed at ambitious students who are eager to really engage in and out of the classroom.

The participants are also given the opportunity to embark on a research internship in Warsaw. During the internship the students are invited to work on their own research project, supervised by an academic mentor. The interns conduct research, interviews, analysis, attend events and meetings with experts and professionals.

This book is the result of the internship program held in summer 2018 at the Terrorism Research Center which is one of the leading think-tanks in Poland with renowned experts participating in projects conducted by the Center. The main thematic focus of the internship was the changing paradigm in security. The interns looked at such important issues as cybersecurity, the prevention of mass shootings and active shooter situations through education and awareness programs, radicalization and recruitment to terrorist organizations, the role of the mass media in shaping public opinion on terrorism, the condition of democracy in the age of fake news, the evolution of modern terrorism and many more.

The authors paint in this book a complex picture of security issues facing modern societies. However, it is not only an analysis of the serious security problems in today’s interconnected world. The contributors look for solutions and the papers are accompanied by recommendations for administration, policy makers and for each of us – living in modern societies confronted with various security threats.

We hope you will find the book interesting and valuable and we cordially invite you to learn more about “Security and Society in the Information Age” programming at www.securityandsociety.org.

Dr. Katarzyna Maniszewska
Vice-Rector for International
Relations
Collegium Civitas

Renee Stillings
Director
SRAS

Chapter 1

A Different Way to Approach Disinformation: Collective Impact

Quinn Harty

“He will win whose army is animated
by the same spirit throughout all its ranks.”

Sun Tzu

Abstract

How can North Atlantic Treaty Organization (NATO) members combat disinformation campaigns more effectively using strategic communication and control their strategic narrative? This article aims to answer this question by proposing a framework for NATO members to fight disinformation campaigns using the principles of collective impact and strategic narrative. This article will first present a literature review of the current thoughts on hybrid warfare, specifically as it relates to disinformation and will then explain the definition of strategic communication and strategic narratives. It will then give examples of common solutions that different governments and non-governmental organizations (NGOs) are pursuing to combat disinformation campaigns and how they are inadequate attempts to control the narrative because of their isolated effort. Third, this article will explain the concept of collective impact and show successful examples. Collective impact is successful only if these five conditions are met: a common agenda, shared measurement systems, mutually reinforcing activities, continuous communication, and a backbone organization. Fourth, this article will lay out a way for NATO countries and possibly NGOs to potentially cooperate to combat disinformation campaigns using StratCom as a backbone organization to coordinate strategic communications and regain control of a desired strategic narrative. Finally, this article will discuss possible shortcomings of this approach, pitfalls to be avoided, and address the importance of this solution.

Warfare and Disinformation

A primary goal in warfare is to obstruct the decision making and command of an enemy leader. This principle is an old one. This same thinking about warfare in the 21st century must be applied to NATO about hybrid warfare. According to this definition, hybrid warfare is to accomplish strategic goals that undermine the norms of conventional warfighting (Johnson, 2018). Conventional warfighting has always included unconventional or asymmetrical attempts to achieve strategic objectives. Sun Tzu recognized the power of using spies to gather information because that would maximize potential to achieve a strategic objective without engaging in conventional conflict. Even though there was no concept like hybrid warfare back then, classical theories of war provide insights into how to achieve strategic objectives. What is new to NATO powers is the ability to achieve strategic objectives without crossing a threshold that would justify a conventional war being launched (Johnson, 2018). But this does not just include Russia using special operations forces to support pro-Russian rebels in Ukraine or China creating artificial islands to expand its territory. What is new to the concept of warfare is the use of disinformation campaigns to accomplish strategic goals without crossing a threshold that could provoke a conventional response. The most difficult of which to deal with and the most important to address is how Russia uses disinformation to influence citizens in other countries through social media and controls the strategic narrative.

Disinformation is “a carefully constructed false message leaked to an opponent’s communication system in order to deceive the decision-making elite or the public” (Arenstein, 1986). Disinformation campaigns use this principle on a larger scale and for a long period of time to achieve their intended result. This principle of disinformation was originally developed by Russia and is called reflexive control. Reflexive control is defined as “... a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action” (Thomas, 2004). Reflexive control’s main principles are to divide, distract, distort and to dismay an intended target with disinformation. This affects the decision-making cycle often referred to as the Observe, Orient, Decide, and Act (OODA) loop of the intended target. The main target of reflexive control is the orientation stage of the OODA loop because the disinformation has a chance to influence the decision of a target towards one that is favorable to Russia. The guiding principles behind reflexive control pair well with disinformation campaigns waged by Russian media like Russia

Today (RT), ideological posters on social media, and social media bots which disseminate ideological content on a large scale. Reflexive control is far more useful as a principle today than it ever was during the cold war. By targeting the voting population of a country, Russia can affect the largest decision-making actors in a state and potentially influence the outcome of elections to produce a favorable outcome for Russia. This is not to say, however, that there is a central coordinating node for all the activity on social and traditional media. The Kremlin does seek to influence non-state level actors to seize initiative and take opportunities to promote Russia's narrative despite not being able to coordinate content creation and distribution (Galeotti, 2017).

Examples of disinformation distribution networks include the pro-Russian ideological postings on social media by users in the Baltic States to influence dialogue and divide populations based on opinion. There are large networks of users there who are not part of troll factories or bots who write, share and spread ideological content related to World War II, communism, the West and other areas of debate with stark divisions of opinion all on social media platforms (Teperik et al., 2018). In the United States, bots and trolls are the primary disseminators of content and discussion. The height of the Russian disinformation campaign against the U.S. was predominantly during the 2016 presidential election. Facebook reported having taken down hundreds of accounts that spread disinformation about both Hillary Clinton and Donald Trump, as well as posted content intended to promote harmful discussion. Facebook also recently removed 270 accounts controlled by the Internet Research Agency which posted content aimed at Russian-speakers in nearby countries (Shane, 2018). These ideological users, trolls, and bots all end up with the same goal: to change voters' perception about what is true. That is how they change the strategic narrative and try to change how people vote.

The Importance of Narrative and Communication

Strategic narratives are critical to control because they order the world so that citizens see their position in relation to an 'other' (Roselle et al., 2014). Strategic narratives are also important because they are like a company's brand: they try to explain what the company is, its history, desired future and its values (Bonchek, 2016). Controlling the strategic narrative is a way to create an order out of chaos (Roselle et al., 2014). Applying those concepts to NATO and other countries is quite simple. NATO must address the concerns of its member states and try to convince them to allocate more financial resources

to the defense budgets. NATO also has the difficult task of trying to increase cooperation among member states. Like all states, NATO members try to improve their own security before the safety of others and hold information they perceive as sensitive close to their chests. Each state has their own strategic narrative of the security situation in Europe. NATO as an institution, however, has its own strategic narrative for how it would like to be seen in the world after the invasion of Crimea. In essence, NATO wants to show its member states that it is re-committed to ensuring security and is prepared to help states defend themselves from a wider variety of security threats, be they cyber or physical (Lindley-French, 2014). This strategic narrative requires cooperation on a large scale, which will be addressed later. Russia's general strategic narrative is that the West and NATO are corrupt and decadent. Russia also has the advantage of not having to cooperate with other states to cultivate a larger strategic narrative. Russia would also like to position itself as the only country capable of ensuring defense for its allies. If countries thought that NATO was not able to ensure their defense, Russia would benefit if it is seen as the only country capable of doing this. So far, Russia has a better understanding of how to actively tailor the narrative to a population because "It is vital that those seeking to use narrative strategically pay as much attention to the reception and interpretation of narratives as to their formation and projection since it is here that meaning is made and any attractiveness, engagement and scope for persuasion are located and experienced" (Roselle et al., 2014; Skuse et al., 2011). Russia controls the strategic narrative through disinformation on both social media and traditional media to reach their target audiences with tailored messages and affect their decision making processes. They are especially effective at reaching their Russian-speaking audiences in the Baltic states (Teperik et al., 2018). NATO, however, cannot communicate one message that reaches all audiences equally effectively. To address this issue, NATO must try and create a sense of confidence in its strategic narrative. Strategic communication is "the purposeful use of communication by an organization to fulfill its mission" (Hallahan et al., 2007). In this case, 'mission' can be replaced with NATO's desired strategic narrative. NATO must use communication to cooperate and coordinate with member states to create more individualized narratives on a country-by-country basis. NATO needs to regain control of the strategic narrative on social media to reduce Russian ideological influence and reaffirm faith that democratic systems and the Western alliance can provide for security and stability in a chaotic age.

Current Solutions to Disinformation

Let us now focus on the question of how NATO members can use strategic communication to combat disinformation campaigns and promote their own strategic narrative. NATO member states, especially those in the European Union, are constantly threatened with disinformation campaigns that seek to divide, distract and deceive their citizens as well as potentially influence the outcome of elections through traditional or social media (Szafranski, 1995; Thomas, 2004). The concept of targeting civilians with disinformation was present in U.S. military circles of thought as a potential vulnerability of the U.S. in cyber war before it was implemented in these disinformation campaigns (Szafranski, 1995). There has not been any large-scale attempt to mitigate disinformation campaigns by educating citizens, which makes little sense in the age of disinformation and fake news.

Currently, there are many proposed solutions for addressing disinformation campaigns. Suggested proposals include improving cybersecurity defenses for political parties and newspapers because they have become targets for hackers. This is a necessary change that should be made to increase the security of democratic institutions and prevent meddling in elections. However, it does not seek to change the strategic narrative. Other proposals are more offensive in nature. Sanctions to freeze Russia's financial assets in response to disinformation campaigns are another suggestion but may inflame relations because it is difficult to prove if the Kremlin organized or financed the campaign. One suggestion is for the U.S. to sign the Organization for Economic Cooperation and Development's (OECD) financial reporting agreement to make states disclose whether Russian companies spent money in U.S. territory (Galeotti, 2018). That may improve knowledge of Russian efforts to spread disinformation in the United States, but it does not improve the security situation of those who are geographically closest to Russia.

What could improve NATO's security in the face of Russian disinformation and information warfare is a promise to support NATO allies when they can confirm that they have been victims of a cyber-attack or disinformation. This would involve promoting the strategic narrative that agrees with NATO's objectives to increase security in Europe in new areas. NATO countries have several options to defend their strategic narrative and try to stop Russia's from becoming more believable, even though it is based on disinformation. One way to approach this challenge is to actively engage the enemies' strategic narrative. In Russia's case, the general narrative is to paint NATO as corrupt and decadent

through disinformation. NATO countries can approach this by confronting and countering that narrative through fact-checking and refuting the official accounts of events in Russian state media and claims by government officials (Hellman and Wagnsson, 2017). One example of using this method is the Ukrainian-run organization StopFake. StopFake takes time to debunk Russian state media's attempts to spread disinformation and tries to disseminate it to the largest amount of people who are targeted by these attempts. Recently, StopFake debunked an article written by RT and RIA Novosty claiming that the javelin missiles the U.S. sold Ukraine were defective. The article was based on a fabricated military document stating that the missiles failed to fire due to being 'expired' ("Fake," 2018). This method applies well to traditional media but not to social media. There are far too many posts to effectively counter at once. Another method is to block the information flow of Russia's strategic narrative (Hellman and Wagnsson, 2017). An example of that is Latvia blocking the broadcast of Rossiya RTR during the months following the invasion of Crimea¹. However, blocking will not be acceptable for most democratic countries because it threatens free access to information which is an essential part of democracy. The method that will now be proposed is confrontational, defends NATO's general new strategic narrative, and relies upon cooperation.

Using Collective Impact

NATO members can combat disinformation campaigns using the principles of collective impact and strategic communication. Collective impact is built upon five key conditions that must be met for the project to succeed. From the Stanford Social Innovation Review, collective impact is "the commitment of a group of important actors from different sectors to a common agenda for solving a specific social problem" (Kania and Kramer, 2011). Collective impact is different from collaboration between NGOs, governments or other organizations because there is a backbone structure that "leads to a common agenda, shared measurement, continuous communication and mutually reinforcing activities" among actors (Kania and Kramer, 2011). This principle was tested in the U.S. education system. 300 community leaders were brought together by Strive, an education nonprofit, to work together to improve the education of children in Cincinnati, Ohio.

¹ See for example message o Latvia's public broadcaster's site: *Latvia suspends Rossiya RTR channel*, available at: <https://eng.lsm.lv/article/society/society/latvia-suspends-rossiya-rtr-channel.a177088/> [12 November 2018]

What matters here is not that there were 300 people, but that they were all part of organizations with different agendas but the same goal, same shared standards to measure, and the same definitions of the problem. At the conclusion of the initiative, 34/53 success indicators had positive growth (Kania and Kramer, 2011). What made this initiative successful is the adherence to the five things quoted above that make collective impact different from independent efforts to improve education. This is a prime example of how collective impact can work to achieve a goal that organizations were addressing individually. The individual efforts of states and NGOs listed above are a step in the right direction, but they need more coordination to achieve an impact on a greater scale.

The first principle of a collective impact initiative to address disinformation campaigns is a common agenda. A common agenda means that all participants who want to work together to mitigate disinformation campaigns must have a shared definition of the problem and agreed-upon goals for the project. In this case, participants must agree which method they want to use for fighting disinformation. Since social media and traditional news media is so prevalent and an easy place for disinformation to spread it should be the focus of a NATO collective impact initiative. NATO members need to agree on whether they are going to address bots, trolls, and ideological posters. They also must agree on how to respond to the Russian media that spreads fabricated articles. Member states could conduct an education campaign for citizens to be more aware of the content on social media. The core of the initiative should focus on education about Russian disinformation first because it most closely aligns with democratic values on speech and freedom of information. There can be different initiatives for research into the cybersecurity or sanctions areas of combating disinformation conducted by separate parts of government and other NGOs.

Another critical area of collective impact is creating a shared measurement system to collect data on progress among all organizations. This aligns the efforts of the participants and holds them accountable to one another (Kania and Kramer, 2011). Member states need to develop a plan to measure citizen media literacy and ability to verify information accuracy. Citizens should also be able to recognize when discussion has been deliberately inflamed or steered towards a certain divisive topic on social media. Collective impact also hinges on mutually reinforcing activities. It is not that collective impact hinges on the number of participating organizations, but their ability to coordinate their different areas of effort to contribute to the shared measurement system (Kania and Kramer, 2011). For example, NGOs with a larger social media presence should direct their efforts on social media to reach the largest amount of the intended audience. Governments should occupy more of a research role or outsource it to other

NGOs. This part of the solution operates like an octopus' tentacles: each part of the solution has its own intelligence, exactly like a tentacle. Tentacles learn for themselves and share the information in a manner that the octopus understands, just like member organizations in collective impact initiatives must communicate their findings and progress with other organizations. Continuous communication is also required for success. Regular meetings with participating NGO and government leaders must happen often to build up trust, shared understanding of goals and a common vocabulary that can be used to clearly communicate progress and intentions (Kania and Kramer, 2011).

StratCom as a Backbone Organization

Backbone organizations are the most vital component of collective impact initiatives. Without a backbone organization, a collective impact initiative is doomed to an early failure. They guide organizations, facilitate their communication, help them develop shared standards and measurements, common languages, and ultimately indicate long term progress (Turner et al., 2012). Therefore, NATO's StratCom is uniquely suited to transform into a backbone organization.

StratCom states that part of its objective is to: "use various channels, including the traditional media, internet-based media and public engagement, to build awareness, understanding and support for its decisions and operations. This requires a coherent institutional approach, coordination of effort with NATO nations and between all relevant actors, and consistency with agreed NATO policies, procedures and principles." This mission statement directly coincides with the principles of having a backbone organization to coordinate the relevant actors in a collective impact initiative. StratCom is based on the principle of strategic communication, which within the context of facilitating communication between organizations can mean "purposeful communication activities by organizational leaders and members to advance the organizations' mission" (Hallahan et al., 2007). This definition aligns with StratCom's mission of promoting understanding of their policies and building awareness for their decisions and operations. NATO's fundamental mission is "to safeguard the freedom and security of all its members by political and military means" A collective impact initiative with StratCom as a backbone organization is one way to prevent the effects of Russian disinformation.

Why is this initiative so important? If StratCom can become a backbone organization for a collective impact initiative to fight disinformation, NATO can effectively aid people in discerning what is real from what is fake. The ideal

situation for NATO is for the majority of citizens in member states to be aware of Russian influence on social media and for them to fact check their traditional media to see if the information has been manipulated or outright fabricated. That means citizens believe the strategic narrative that Russia is trying to influence elections and is interfering in government and national security. Citizens will then believe NATO's narrative that they are doing everything possible to work together and increase information security in Europe as well as physical security. That is a great success for NATO's post-2014 strategic narrative.

Things to Consider

It is no secret that NATO member states have different goals for their own security, their own definitions of common security issues in member states and different language to describe common problems. A problem that could be faced by this proposed solution is that states like to keep information for themselves and try to advance their own security agendas before NATO's. Even though there is a desire among member states to advance their own agendas first, which hinders communication and cooperation, there needs to be a baseline level of cooperation and information sharing. There are security issues which affect every single NATO member state and disinformation is one of those critical issues. Even though the effects of disinformation may be quite different depending on the country, it is indisputable that the member states should work together to address it. At the minimum there should be an agreed upon definition of what disinformation is, and some shared baseline goals for outcomes. Disinformation directly affects how NATO is perceived. If NATO member states cannot cooperate, public opinion of the treaty becomes worse. If NATO can achieve more cooperation, they are perceived much more positively. NATO must convince citizens that their desired strategic narrative is in place and implement this solution to create effective change in addressing disinformation.

Sun Tzu's lesson "He will win whose army is animated by the same spirit throughout all its ranks" rings true. Collective impact is the spirit.

Chapter 2

A Violent Psyche

Bianca Canal

Abstract

The following scientific paper attempts to relay psychological triggers as well as situational factors that contribute to the formation and action of terrorist organizations. The research explores topics such as mental health, reasoning, and personality traits of terrorists. The question at hand: What qualities make a person more inclined to join a terrorist cause and carry out heinous crimes? Over several analyses, the attempt will be made in this paper to exhibit a consistent portrayal of certain characteristics seen in terrorist groups and individuals. Terrorists are rarely mentally ill and more often provoked individuals with certain personality traits encouraging behavior that resorts to radical violence for political attention. Characteristics such as a desire for clear ingroup and outgroup, harsh socioeconomic influences and a need to purify society creates an “Us vs. Them” mentality. This mentality is essential in the formation of terrorist organizations and the follow through of terrorist crimes. The arguments are divided into three sections: mental health and its impact, reasons for terrorism beyond the individual, and consistent characteristics.

Mental Health and Its Impact

Terrorism has taken on a new meaning in the last few decades with the help of technological change and the media. For the terms of the research conducted by the author, this paper will abide by the following definition supplied by the European Union. Terrorist crimes can be defined as (Spaaij, 2010, pp. 854–870):

“intentional acts that are committed with the aim of seriously intimidating a population, or unduly compelling a Government or international organization to perform or abstain from performing any

act, or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization.”

In the first issue of this paper, the author hopes to uncover whether mental health is a common denominator in terms of terrorist actions. Are those diagnosed with a mental illness more inclined to participate in violent, specifically terror related, crimes? Do groups target people affected by mental illness to commit heinous crimes? How can understanding and addressing this question reduce terrorism or approach it in a new way?

It is worth noting that stigmas against mental health make it difficult to gather research of this kind. First, people will rarely admit they experience symptoms of mental disorders. In fact, “[a]bout two-thirds of people suffering from mental disorders will never seek help because of discrimination and the stigma attached to such conditions” (Zuidewijn and Baker, 2016, pp. 42–49). Some cultures and groups are even more hostile to such accusations, especially right-wing or conservative extremist groups. Second, terrorism research is limited in a more obvious sense because of its nature. Terrorist organizations are underground, highly secretive and supply information in ways that will spread their ideas or benefit their cause (Gambetto and Hertog, 2016). An environment for gathering sufficient empirical data on such a topic simply does not exist. Perhaps there are undercover agents who are also social scientists gathering intel from the inside; then again, the government never shares such data with the public for reasons of “national security.” More often than not, facts covering terrorism are supplied to the public in a way that will benefit that federal agenda (Gambetto and Hertog, 2016).

Overall there is little evidence for mental disorders contributing to terror related crimes. In a case study with over 100 lone-actor terrorists, only 35% showed any sign of mental illness (Zuidewijn and Baker, 2016, pp. 42–49). Compare this to the World Health Organization’s statistic: 27% of the population suffers from a mental disorder. Presence of mental disorders among terrorists does not substantially deviate from that of the general population².

With this in mind, an important discovery amongst lone wolf terrorism depicts sufficient evidence for a correlation between school shootings and mental disorders. First, school shooters are responsible for 63% of mental health cases in the aforementioned study. Often, the mental disorder these school shooters are

² Furthermore, the case study that approximated 35% recorded “any indication of” a mental disorder. This closes the gap between the tested group and the general population even more.

prone to is a product of social isolation (Zuijdewijn and Baker, 2016, pp. 42–49). The study further reveals that school shooters with predisposed mental disorders resulting from social isolation often did so at the hands of bullying. Social isolation can lead to mental and personality disorders that contribute to lone actor terror attacks in school settings. The good news is that this progression of personality disorder to radical violence is understandable and predictable. While this does show evidence for a correlation between mental illness and lone shooters, this does not necessarily fit into the EU’s definition of terrorism. School shootings usually lack the political factor necessary to qualify as terrorism. In this case, political motives are replaced with a personal vendetta. However, the information is still useful for change regarding emotional awareness in early education.

Despite the significant findings within the field of lone actor terrorism, mental health is a widely controversial topic to attribute to any form of violence. The question creates an insensitive view of those suffering from psychiatric disease. One social scientist suggests that Western perspectives hold a lack of objectivism when interloping mental health with terrorism (Aggarwal, 2010, pp. 379–393). He says these scholars forget to consider the varying values and cultures across the world that alter social behavior. The difference in values and expectations among cultures allows Western scholars to diagnose symptoms that would not apply if they took a different perspective into consideration. Assuming mental illness must be involved in terrorist activity also suggests that the morals of the West are superior to those political thoughts and ideologies found elsewhere. Pinpointing radical violence on those suffering from mental illness is merely a coping mechanism of the public perpetuated by the media. The conclusion exists to satisfy a level of comfort denying the far more disturbing reality. Generalities have a way of simplifying complex and layered truths about humanity: “the conceptions they convey are always incomplete, [and] what is gained in extent is always lost in exactitude” (Tocqueville, edited by Mansfield and Winthrop, 2000). Believing that mental health is to blame for radical violence falls guilty of being an overgeneralized statement with little thought.

Furthermore, terrorist organizations do not seek out mentally ill recruits. In fact, “most tasks require an element of secrecy, calibrated violence, and technological know-how. Educated, psychologically healthy, and normal volunteers tend to be preferred for this particular reason” (Corner and Gill, 2015, pp. 23–34). Seeking unstable people for layered and high-risk situations could be detrimental. This means most of the time, political motives are strong enough to motivate radical violence. When acting individually, there is a stronger likelihood that someone is suffering from mental illness (Spaaij, 2010, p. 866). Mental illness is also more present in individuals who have less ideological reasoning

to back their attacks (Zuijdewijn and Baker, 2016, p. 44). This may suggest that group mentality affects “normal” people in large ways, causing them to behave in ways they wouldn’t otherwise. It appears that “a clear consensus exists that it is not individual psychology, but group, organizational and social psychology, that provides the greatest analytical power in understanding this complex phenomenon” (Corner and Gill, 2015, pp. 23–34).

Overall, it was found by the author that the connection between mental health and terrorism is weak. What, then, motivates people most when considering radical and violent political attacks? The answer to this new question, “reasoning behind radical violence in society” holds complexities that a large volume book could hardly hold. The remainder of this paper will relay the essential and rudimentary reasonings behind radical violence and terror attacks.

Reasons for Terrorism Beyond the Individual

Scientists agree that terrorist crime occurs when individuals and groups behold an active aversion towards society and the government. Radicals act when they feel the government is corrupt and simultaneously useless in creating an ideal society. A person would feel inclined to behave in active ways if they were passionate about a political cause but could not imagine addressing that cause in their own government in a civil or bureaucratic way. Another factor scientists can agree upon is that there is a plethora of reasons for terrorism that are interconnected and influence one another.

Sebastian Wojciechowski, a sociologist and author from Poland, presents data from several social scientists to further understand the current discussion at hand and develop his own take on the issue itself. The study conducted has overflowing amounts of evidence with overlapping conclusions. Wojciechowski then compares and summarizes these theories to find his own.

He argues religious and cultural zeal propagates terrorist attitudes. He states that there has been an increase in religiously motivated attacks since the 1960s. These religious and culturally conservative reactions may be in response to the increase in social movements and equality throughout this time period. When faced with change, many cultures fear their traditional values will disappear and meld into universal customs. This paired with worldwide intervention, a theme of the twentieth century, can lead to violent outbreaks for the sake of preserving identity and tradition.

This transitions us to the portion of his argument that presents socio-economic, political and historical issues. Political leadership influences terrorist

attitudes. This occurs whether these elites are combating or collaborating with said terrorist threats. Combating could result in an increase in vigor, though they attempt to eliminate the group altogether. Collaboration with terrorist organizations may also increase the importance and influence of these groups. Such situations have been seen in countries like Iraq, Iran, South Korea, and Sudan, where involvement occurred at some point to alleviate tension or inadvertently implement martial law. Additionally, migration can be the reason for an increase in terrorist attacks. Immigrants are vulnerable to recruitment by terrorist groups of similar ethnic background and ideology. On the opposite end of the spectrum, xenophobic terror attacks have been committed on immigrants and the institutions that support them. Socio-economic factors such as poverty are sometimes seen as triggers for violence and rebellion. The correlation is not sound though. Many terrorist organizations require financial support and several organizations are made up of people from middle and upper-class backgrounds. Historical patterns contribute to the rise and intensity of terror organizations as well. The memory of disenfranchisement, real or imagined, taints and motivates bodies of people to rebel. Furthermore, the collapse of communism propelled the world into radical change in the realm of international relations. This new juggling act of sovereignty has paradoxically made it possible for rebellious groups to operate.

Wojciechowski includes territorial and ethnic influences to explain the influx in terrorist attitudes. He points out that 3500 nations exist in today's world and only 195 are recognized as states (Wojciechowski, 2017, pp. 49–70). Most have accepted their lack of recognition, but much unrest exists among those who wish to gain sovereignty. These desires for establishment can translate to radical outbreaks.

Wojciechowski then speaks to the psychological aspects. He suggests the belief that one idea, even if it may be targeted towards an evil or decision about right and wrong, put above all else (even the quality of someone's life or one's own life) can be seen as evidence for psychopathy: "In many cases we encounter terrorism when a given individual or group considers a certain attitude or idea to be of the utmost importance, one which all other matters should unquestionably be subordinated to" (Zuijdewijn and Baker, 2016, p. 44). However, the author would argue that this idea is used by countries all over the world. It is a historical motivation for achieving sovereignty. It is indeed an idea America, along with several other countries with an established branch of defense, feeds its troops. It is an idea that has incited war again and again since the beginning of our existence. "Give me Liberty or Give me Death" ignited the American Revolution. Perhaps Patrick Henry was a psychopath, but if that is the case, then so is everyone who

has ever wished to rise in society. Human behavior has consistently shown that its desire for some unattainable idea of freedom and power trumps all other values, including one's own life and the lives of others. For is a life of oppression worth living? It can be argued that with the right persuasive language, a certain degree of oppression, and a culmination of experiences to shape political thought, terrorist acts and attitudes are probable for any human.

Lastly, Wojciechowski analyzes movements and ideas that implicitly add to the growth of terrorism. Globalization, specifically the spread of the "West," weakens communities, for it often introduces new economic burdens and demands social transformation (Wojciechowski, 2017, pp. 49–70). Many places feel their local identity being threatened. Challenges present themselves through cultural clashing as a result of these varying social expectations. One example of this is the introduction of progressive individual rights defined in communities with varying views of freedom and oppression. Other theories like the domino effect and the role of the media also come into play. As W. Laqueur puts it, "terrorists need the media and the media finds the components of an exciting story in terrorism" (Laqueur, cited in Wojciechowski 2017, p. 58). With the domino effect, violence usually responds to and motivates other forms of violence. This is pushed further with the media. The media latches onto the bait terrorists provide. They supply a juicy story that is reported on incongruently with reality. The threat is proliferated because of the media's desire for attention.

Wojciechowski finally narrows his data, claiming there are three main determinants in modern day terrorism: various ideas and ideologies, selected socio-economic conditions and various psychological processes and factors (Wojciechowski, 2017, p. 63). With varying ideologies, clear ingroups and outgroups are formed. This allows organizations, ethnic groups and countries to isolate themselves while dehumanizing the "outgroup." This is essential in the formation and cultivation of terrorist bodies. These groups often form when they believe they have suffered from the status quo. This usually takes shape in terms of economic and class status. The lower socioeconomic class becomes envious of the upper class, especially in societies where large gaps between the classes exist. This jealousy and feeling of unfair treatment can intensify to the point of violence. This process does not encompass all terrorist personalities. However, it does characterize a majority of prominent groups. Lastly, as analyzed before, psyche influences terrorist acts and mentality. The combination of "us vs. them" ideology and the act of placing an idea of freedom above one's quality of life can lead to a dangerous outcome.

It is listing and specification such as this that creates the never-ending reasoning behind an almost abstract issue on violence. Ultimately, Wojciechowski's conclusion

is indeed that one does not exist because “despite the multitude and diversity of the above theories, none of them comprehensively explains the emergence and escalation of terrorism. They point, however, to how numerous and different the potential factors are. These theories are frequently interdisciplinary and combine elements of psychology, as well as sociology, pedagogy, economics or philosophy” (Wojciechowski, 2017, pp. 58). Many studies attempt to uncover some “secret” or single characteristic of terrorism. Such a solution does not exist with a topic so abstract and uncontrollable. The author found this conclusion, however, to be just as comforting as it was infuriating. These discoveries still beg the question: what characteristics define the people of these groups? What characteristics make a person more inclined to join such a radical extremist group? With the help of narrowing the focus area, it is possible to gather specific conclusions that paradoxically reveal universal truths about radical violence.

Consistent Characteristics

Perhaps answering one question about a specific demographic of terrorists could inevitably uncover consistencies across several lines of characteristics and personalities. Diego Gambetta and Steffen Hertog unveiled helpful information using this tactic. In their book, *Engineers of Jihad*, they study the behavior of engineers in terrorist organizations. These social scientists prove the undeniable flow of engineers into radical violent groups and seek to uncover why this group exists and what it says about the average extremist. In the end they studied 4,000 individual identities, comparing different backgrounds, disciplines and ideologies to the control group: engineers. Tracking the education of terrorists offers significant insight about the individual. The individual chooses the kind of education they want, and this in turn supplies hints about their personality and socioeconomic upbringing. Studying the reasoning and psychology of political motives relays helpful information about consistent traits among terrorist group. “The evidence that political attitudes are linked to personality traits, all the way down to variations in brain structure, is mounting rapidly—whether derived from surveys, experiments, or measurable neural processes—and is just too compelling to dismiss wholesale” (Gambetto and Hertog, 2016, p. 129). Ultimately, they conclude that engineers are undeniably overrepresented in right-wing, conservative and religiously motivated terror organizations. Conservative right-wing terror attacks are often committed by people who have degrees in engineering or exhibit left-brained, attention-to-detail characteristics.

The characteristics this group shares include proneness to disgust, a need for certainty and closure and a desire to distinguish the ingroup from the outgroup. There is a correlation between right-wing ideology and a desire for social purity. Right-wing radicals “desire to keep their social environment pure and reject intrusion by alien forces perceived as corrupting” (Gambetto and Hertog, 2016, p. 130). Today this takes the form of opposing gay rights and abortion, issues that fall in line with preferring a society tightly bound to conservative tradition. Personalities of right-wing thought also seek closure. A need for cognitive closure, or NFC, is closely related to conservative thought (Gambetto and Hertog, 2016, p. 129). Those of NFC personalities often see the world in black and white and wish to live in an authoritative society operating through strict social obligations. Lastly, right-wing conservatives show an aversion towards open-minded views of others and complex categorization. This falls into the desire for ingroup and outgroup. Those of conservative thought exhibit an inability to denote the “outgroup” with simultaneously positive and negative connotations. All three aspects of right-wing extremism inform one another and follow a line of strict, conservative thought with little tolerance.

Engineers often fall into the radical right-wing parties because the personality traits that attract people to engineering fields are similar to the traits that attract people to conservative political thought. Engineers share an intolerance of ambiguity with right-wing extremists. Like mentioned in the previous paragraph, conservatives dislike complex answers to political issues often coupled with social change. Similarly, engineers desire one clear answer to technical problems. The field thrives on complex mechanical patterns with simple one answer solutions. It is no surprise that the personalities that make up the engineering field seek the comfort of singular solutions in real life.

In addition, this theory exhibits overlap with the main determinants in Wojciechowski’s conclusion, especially the desire for clear ingroups and outgroups. *Engineers of Jihad* also proves the claim “relative deprivation increases radicalization,” continuing to fall in line with another main determinant of Wojciechowski’s: selected socio-economic conditions. Lastly, the book confirms the idea that putting one idea, or mechanical solution, above all else contributes to the fuel of radical violence.

Conclusion

The complexity of terrorism mirrors the complexity of humanity over time. Both are primarily a result of technological change. When boiled down, terrorism

finds its origin in radical violence: something inevitable that occurs when humans are responding to government corruption, escalating social change and cultural clashing. Slowly chipping away at the reasoning behind it allows scholars to understand the complexities of global interaction that has exponentially challenged human interaction. The answer to these challenges could be an increased awareness of the role mental health amongst the general population, the understanding of violence and global conflict as well as the exposure to well-rounded education will best combat the characteristics that frequently lead to radical violence. Teaching what is natural, how humans are susceptible to group mentality and how to cope with violence and media, can attribute to building a more understanding and empathetic society.

Chapter 3

Retweeting Radicalization: Radicalization and Recruitment to Terrorist Organizations in the Information Age

Nicole Wojtkiewicz

Abstract

In a time of technological advancement and media domination, terrorist organizations are evolving their means of recruitment and radicalization. It is imperative that an accurate light is shed on this phenomenon. This article aims to explain how Jihadist terrorists and terrorist organizations are utilizing technological advancements, like social media, in their recruitment tactics. It is important to define what is meant by information age, radicalization, and recruitment as it relates to the research conducted. There appears to be a lack of research, consensus, and understanding pertaining to actual social media usage and effects by these organizations. Drawing from varying perspectives, research, and studies, what is occurring through Internet sites like Twitter, Facebook, and YouTube, and the realistic threats that this usage is posing will be examined. In an effort to alleviate misunderstandings and disproportionate reactions, the article will outline practical counter efforts that can be deployed to combat these ever-evolving recruitment tactics. Finally, certain criticisms and limitations pertaining to research, policies, and misinformation are pointed out. All the information outlined leads to the concluding notion that although an effective aid in recruitment tactics, Internet and social media use is not alone enough to create a terrorist.

Introduction

In a time referred to as the “information age”, “digital age” or the “media age” there has been much speculation concerning the role of technological advancements and its aid to terrorist organizations; specifically speaking, the ability to utilize things such as the Internet and global communities to recruit and radicalize for the organization. When referring to the Information age, this article utilizes Manuel Castells (2010) ideas concerning the rise of a network society. This refers to a period in the 2nd millennium. During this time the world experienced social, technological, economic shifts altering society into a modern network society. A focus of this article consists of communication shifts from traditional mass media to a more decentralized and horizontal society surrounding the Internet. This allows new means of varied and efficient communications (Castells, 2010, pp. 17–18). Terrorists no longer must solely rely on the media and news networks to spread their propaganda, attacks, and fear. They now possess the tools to spread their messages themselves through online networks with social media platforms, but what is it exactly that terrorist organizations are trying to spread and accomplish through their use of the internet?

What is clearly of most concern is terrorist organizations modern ability to radicalize and recruit efficiently through social media. The terms radicalize and recruit will be used in this paper in similar contexts. By recruit is defined as convincing someone to join a cause. When discussing radicalization throughout this paper, it will refer to Chatfield et. al., (2015) interpretation as

‘Increasing extremity of beliefs, feelings, and behaviors in support of political violence in a context of strong group identification and response to perceived threat to the in-group’ (p. 7).

An observable and possibly obvious pattern, that should be understood to follow this paper is the necessity of radicalization to recruit people to terrorist organizations.

With this basic background knowledge, the paper will continue to observe the ways that the Internet is exploited by terrorists and organizations and how this is built off their traditional recruitment methods. Next, the actual threats that this Internet is posing and its implications are highlighted. Following this, practical steps as to how to combat the ever-evolving use of the Internet to radicalize and recruit to illicit organizations will be outlined. Once the use, threats, and solutions of this Internet use are explained, this paper points out limitations and

criticisms concerning studies, public opinion, and policies regarding Internet use by terrorist organizations. This all adds up to the concluding point that the Internet can influence radicalization and recruitment, but it alone cannot create a terrorist.

How the Internet is Actually Utilized by Terrorist/ Jihadist Organizations

Social media platforms have freed terrorist organizations like Al Qaeda and the Islamic State of Iraq and Syria (ISIS) from relying on mainstream media to communicate and disseminate information. They would normally have to rely on dramatic events and threats to be picked up by news outlets. This would then spread their messages and their so-called victories. Now anyone can participate. The fact that social media, blogs, and file sharing apps are low cost, quick, and anonymous, they are able to reach greater audiences efficiently (Klausen, 2015, p. 4). There seems to be a misconception concerning what and how terror organizations are using these social media platforms. From analyzing several studies, the author has come to find three common uses that are present. This section will describe this straightforward social media and Internet use in terms of communication and connectedness, boosting visibility, and promoting and advocating attacks.

To begin with the most basic use of social media for terrorists, one must understand how it is used to promote communication and connectedness. Klausen (2015) explains that the ways illicit organizations use social media to communicate vary. Although some militants consistently update their social media profiles, many are not able to communicate at all. For example, new recruits must turn over their cellphones when arriving at training. So, what may seem as spontaneous communications uses, are actually calculated and controlled (Klausen, 2015, p. 2). A commonly held threat of the Islamic state is the ability to now communicate globally with potential sympathizers and recruits. A clear example illustrating connectedness and communication is the twitter page “@shamiwitness” which Chatfield et. al., (2015) analyze. They collected and examined 3,039 tweets from this known information disseminator for the Islamic State cause. The results reveal “Shamiwitness” mentioning 877 users, which creates dynamic social networks. Their findings produce evidence of the presence of distinct twitter populations, which include international media, regional media, actual Islamic fighters, and Islamic State sympathizers. These

networks transcend international borders and directly ask users to join their cause (Chatfield, et al., 2015, pp. 4–11). Richards (2014) points out that in 2014 ISIS had 9,000 foreign fighters and around 3,000 were western recruits and attributes this phenomenon to the use of social media to communicate across borders. In her article, she mentions a study on social media of foreign fighters, which expose the direct influence of Australian ISIS supporters. Only 35 twitter accounts create a network of 18,223 specific users. These online accounts created by terrorists and their organizations are able to reach an unprecedented amount of users. In Michael Steinbach's (2016) Statement before the Senate Committee on Homeland Security and Governmental Affairs, he explains the dangers of evolving communications by giving the example of an unnamed individual apprehended for providing aid in facilitating an associate's travel to Syria to join ISIS. He revealed that the individual had several connections through social media with "like minded individuals". The fact that terrorist organizations' means of communications have improved is undeniable, what must be examined next is how they utilize this communication and connectedness to boost the visibility of their messages and propaganda.

Terrorist organizations not only deploy social media networks effectively to communicate and connect with others, but to boost the visibility of their messages and propaganda. They have seized the opportunity to spread their messages to a wider range of communities with similar ideologies as theirs. Propaganda throughout history has been essential to terrorism. The idea of propaganda by deed is intensified and altered through these Internet platforms. This is the idea that acts of violence will serve as a catalyst to political change and revolutionary movements. In order for this process to be effective, they must reach the greatest audience possible. To begin with, terrorist organizations will magnify external threats from outsiders and the government. They then attack their governments which in turn elicits a sometimes-violent response (Chatfield et. Al., 2015, p). Taking Nizar Trabelsi as an example of this, he claimed that he made the decision to carry out an attack as an associate of Al Qaeda after seeing pictures of a killed Palestinian baby on the Gaza Strip (Archetti, 2015, p. 55)³. Many saw this picture, but after it spread, it reached a person willing to kill for a terrorist organization. Klausen (2015) elaborates on the ISIL (ISIS) offensive

³ Nizar Trabelsi was once a pro football player from Tunisia who conspired with Al Qaeda, specifically Osama bin Laden, to carry out a suicide attack targeting Americans in Europe. He was arrested in Belgium before he could complete his attack. To read more about Nizar Trabelsi please visit <https://archives.fbi.gov/archives/washingtondc/press-releases/2013/alleged-al-qaeda-member-extradited-to-u.s.-to-face-charges-in-terrorism-conspiracy>

of 2014, which included graphic photos of beheadings that forced American involvement. These photos are not only meant to incite fear but to illustrate the organizations unconstrained power. Although these gruesome photos are what most hear about, groups like ISIS and Al Qaeda spread photos of their normal day-to-day lives. There are photos of propaganda that show groups of men with guns in hand enjoying a pizza. These clearly staged photos exist to manipulate possible sympathizers into believing that life as a jihadist can be rewarding and even normal (pp. 12–13). Organizations take the message they want and can spread them on a multiplicity of social media pages creating the redundancy necessary to ensure their propaganda reaches wide audiences. A few may not see the immediate threat in spreading propaganda, but the threat is undeniable when calls advocating for and praising individual attacks begin to appear.

An immediate threat that the use of social media networks by terrorist organizations poses is the call to arms. Many go beyond trying to persuade sympathizers to join their fight, but rather to take the fight into their own hands, wherever they might be. They have the direct ability to inspire what some call “lone wolf attacks” around the globe all from behind a computer screen or just a smartphone. Looking at the attack in San Bernardino in 2015 and in Orlando in 2016, we see the Islamic State does have the ability to inspire some sort of attacks without any direct contact or control over the attackers. According to Daniel Byman (2017), both attackers claimed allegiance to the Islamic State but were not directly controlled or involved with a terrorist group. These so-called “Lone Wolves” managed to kill 63 Americans (Byman, 2017)⁴. Terrorist organizations can be more specific with their goals for lone attackers. For example, United States Military personnel were targeted when a list of hundreds of names of serving members was released and spread through social media by terrorist affiliated networks (Steinback, 2016). The ability to attack around the globe outside of specific illicit organizations is only growing as social media grows.

This section explains in simple terms how terrorists and their illicit organizations utilize social media and the Internet. After reviewing several of the cited sources which include news article, studies, and research three common

⁴ Daniel Byman explains in his article “Beyond Iraq and Syria: ISIS’ Ability to conduct attacks abroad” that although the two examples of “Lone Wolf” attacks mentioned in this article claim some affiliation to the Islamic State and ISIS claimed ownership of the attack, there are several other potential factors that contributed to their attacks that have nothing to do with terrorism at all. To read further about this go to <https://www.brookings.edu/testimonies/beyond-iraq-and-syria-isis-ability-to-conduct-attacks-abroad/>

uses of the Internet by terrorists that are relevant to this paper were picked out. The use is outlined in terms of communication and connectedness, boosting visibility, and promoting and advocating attacks. What must be analyzed next are the actual threats these uses pose.

The Realistic Threat That Terrorist Organizations Use of the Internet is Posing

There appears to be a panic within the media and policymakers concerning the weaponization of the Internet and social media sites to aid terrorist efforts. The threat cannot be completely dismissed because access to the Internet does raise the efficiency of the tactics the terrorist organizations employ. Unfortunately, many think that with the use of the Internet, terrorist organizations could radicalize people into terrorists around the globe. This causes an unnecessary demonization of the Internet and social media sites. In turn, many lose focus of the larger picture of recruitment, which includes a social aspect that exists beyond the Internet. This section elaborates on two facets that need to be taken under consideration when assessing threat levels. First, terror organizations deploy similar tactics that they have been using throughout history, but it is just now applied to the Internet. Next, that the Internet alone is not enough to radicalize and recruit an individual.

There are traditional tactics that terrorist organizations employ which seem to be sparking a panic due to the use of the Internet. For example, a common tactic to recruit to organizations is to target the Islamic youth, specifically males that may be looking for a place to fit in. They proceed to recruit by attempting to strengthen their identification within a group (Chatfield et. al., 2015). This is now accomplished online in various steps which are explained by JM Berger (2015) as discovering a vulnerable recruitment target, creating a micro-community around him or her, isolating them from friends and family, privately communicating with them, then finding out what actions the recruit would be willing to do and encouraging them. The only difference is that now this is being applied through social media sites like Facebook, Twitter, and YouTube. Although these sites are helpful tools in the process of radicalization, they alone are not enough to complete the process.

Social media networks make the radicalization process for organizations more efficient, but Archetti (2015) explains that radicalization and extremism happen in a social sphere that is constituted by several overlapping networks.

Individual narratives compose these networks. By narrative, Archetti means that each individual person has his or her own mentality at any moment in time. Any information that an individual receives from terrorist organizations is taken into and interpreted through their own narrative at that moment in time. A person's relationships and narratives are consistently changing. Whether a person is receptive to recruitment tactics is dependent upon the connection with that potential recruit's narrative and a member of/or the group's narrative. These social media platforms are a tool but the operators, networks, and the tactics they implement are central to radicalization. To simplify this idea, the Internet cannot radicalize without a preexisting narrative that is open to the idea of extremism. Looking at the example of Nizar Trabelis again, who attempted an attack after seeing a picture of a killed child on the Gaza Strip, thousands saw the picture of the child but only he was persuaded to organize an attack. Archetti (2015) stresses that this occurred because he was the one individual who already possessed a narrative receptive to radicalization (Archetti, 2015, pp. 53–54). What the Internet is able to do is spread a message wide enough to reach an individual with the potential to be radicalized, and that threat cannot be fully dismissed.

Part of what makes Jihadist organizations use of social media platforms successful is volume. With the creation of these platforms, organizations can mobilize supporters and fundraise in more efficient ways. They can reach a broad audience with a greater opportunity to connect with sympathizers. Doing most of this online, they are often working anonymously. All these things are reasons that many consider the Internet to be a modern weapon for terrorism. The existence of these threats is not something to be disputed. What can be stated is that the reaction to these developments is disproportionate. Two important factors are explained that touch on the idea that the main factors pertaining to radicalization and recruitment are not the Internet at all but rather their use of traditional tactics, and importance of individual and group narratives. Since many do not argue the existence of a threat, one should consider potential counter efforts to keep up with rapidly advancing technology.

What We Can Do

It is not enough to discuss how terrorists utilize the Internet and social media in their recruitment tactics and the threat levels surrounding this activity. Arguably the most important portion of this paper is outlining potential efforts to minimize and counter the damage done by terrorist organizations online.

These ways include evolving law enforcement tactics, taking a community-based approach, and finally holding our media and news networks accountable.

To begin with, the most obvious defense to any terrorist activity is law enforcement. Michael Steinbach (2016) explains how pertinent it is for all law enforcement to be familiarized and be able to monitor the latest communication tools that terrorist organizations utilize. Steinbach does highlight some challenges that accompany this task. The forms of communication in the information age are outpacing the ability of our government agencies to keep track of them. Normally, law enforcement agencies have the ability to access stored communications with a lawful process but there are services developing that do not store any information at all. The lack of familiarity with new communication technologies is what Steinbach refers to as “going dark.” JM Berger (2015) suggests a consistent analysis of social media, which can detect communities affiliated to Jihadist groups. Following confirmed recruiter profiles, law enforcement can discover potential supporters. At times, the shift from public to private communication can be spotted, and it is at this point that law enforcement must intervene. With the current social media platforms present at this time, there are only so many methods of interaction. Berger states that with the monitoring of social media sites of the recruiter, we can possibly discover the process being commonly implemented. Unfortunately, with evolving technology and its vast span, it would be difficult to monitor every social media account. For that reason, it is important to go beyond the Internet.

Where we may fall short on counter efforts through the Internet, we must make up for with community approaches. There have been attempts to put forth narratives to juxtapose those being circulated by terrorist organizations. This method is ineffective since the narratives constructed by ISIS for example, include all aspects of life. They discuss career opportunities, home life, and attempt to create a sense of community for any potential recruits (Steinbach, 2016). They have an elaborate network to circulate these narratives. Any message sent out by a government agency or organization will fall short. We do not possess the proper networks to receive and circulate any counter messages we may attempt to create. This is where building a community connection becomes essential. Long-term engagement within a community gives the possibility to gain understanding into what Archetti (2015) calls “local narratives” (p. 56). It is also important that this engagement does not consist of solely impersonal communication, but rather through meaningful action. We can become involved through social movements, local charities, and personal communications (Archetti, 2015, p. 56) There is no formula that can discover a potential terrorist, but this is a way to gain trust within societies and begin to recognize why one might be susceptible to terrorist

recruitment within a community. This may be a daunting task to accomplish and control but something that is clear is the use of news media outlets.

Some may argue ensuring that news media sources are not making a situation worse is a clear and simple task. In a democratic country with freedom of speech, like the United States, it is almost impossible to control what news media outlets put out. This can aid the efforts of terrorist organizations. As previously discussed, terrorists require large audiences to succeed with their terror tactics. In the past, they would rely on media to spread their messages by continuously reporting and broadcasting them. The way they would force this is by choosing a large symbolic target, like the World Trade Center to attack. Their goal can be explained with a Chinese proverb “Kill one- frighten ten thousand” (Klausen, 2015, p. 2). The current use of social media has changed the dynamic of media reliance. Now that terrorist organizations have their own platform, they choose what to circulate and the media then picks up on it and reports it. They still get the media coverage required to build an audience but now they have more control as to what is being reported and spread. JM Berger (2015) stresses that mainstream media can play a helpful role in not spreading terrorist propaganda and fear by ensuring that the amount of coverage on any incident is proportionate and responsible. Unfortunately, medias disproportionate reporting can be seen with most terrorist attacks in the western world. Media outlets normally lead with the most interesting and often gruesome stories for views, and if there had been a terrorist attack or threat, this will normally lead for a greater period than is appropriate.

Arguably the most important portion of this paper is exploring potential solutions and counter efforts to combat recruitment tactics. The first means of defense is law enforcement tactics. This cannot provide the most comprehensive countermeasure to recruitment since it is impossible to say with certainty who is susceptible to radicalization online. For that reason, taking a more in-depth community-based approach is stressed. Finally, holding our media and news networks accountable is something we have the potential to do within our own countries. Perhaps more solutions could be discovered and explored but there are limitations to this field of study.

Concluding Thoughts and Limitations

Terrorist organizations use of the Internet and social media is a young field of study. It appears that illicit use of the Internet and social media is developing quicker than our ability to analyze it. Although there are several mass media

reports on recruitment through online media sources, there is a lack of academic studies on the topic. Not only is there a lack of studies and research on the topic, there also appears to be a lack of consensus on the matter and threat level it possesses. Some contrasting viewpoints have been illustrated in this paper. Another limitation to this field of study is social media policies that both hinder terrorist's capabilities to communicate but also researcher's abilities to research. Chatfield et. Al., (2015) explain when analyzing the "@shamiwitness" twitter account that social media sites like Twitter and Facebook have a policy in place to suspend or terminate any account associated with a terrorist organization. These accounts are disappearing and reappearing with similar but different names to go undetected, making it difficult to track their activity.

Chapter 4

Can We Identify the Next Shooter? Preventing Mass Shootings and Active Shooters by Identifying Concerning Behaviors of the Shooter Prior to the Attack

Casey Guthrie

Abstract

There are numerous assumptions that arise from mass shootings and active shooters. Unfortunately, a large portion of the public may be unaware of certain concerning behaviors that can identify potential shooters. A common assumption is that the attack could not have been prevented in any way. This paper will discuss specific observable behavioral characteristics exhibited by shooters, which could be useful to identify them, prior to the incident. Educating the public about common pre-attack behaviors displayed by past offenders can increase the chances of a bystander detecting and disrupting the attack. It is imperative that the collective and collaborative engagement of all members of a community participate in preventing a mass shooting incident. This research paper will provide definitions of the terms “mass shooting”, “active shooters”, “stressors”, and “mental health” as they pertain to the research conducted. The common assumption that mass shooters and active shooters are mentally ill, and the research that contradicts this belief will be discussed.

Introduction

The majority of planned mass shootings and active shootings follow a period where the actions undertaken by the shooter could be identified as concerning. When the public is aware and alert for observable behaviors, potential shootings can be disrupted and prevented, and hundreds of lives can be saved. Although there is no single list of behaviors or certain prevention strategies that has been proven to work in all shooting incidents, there are multiple approaches that are worth the effort they require. The number of casualties each year caused by these tragic events is appalling. The Federal Bureau of Investigation (2018) designated 50 shootings in 2016 and 2017 as active shooter incidents. Of these 50 shootings, 943 casualties were declared, consisting of 221 killed and 722 wounded (p. 2). These statistics are excluding the shooters. There is no single definition for the terms “mass shooting” and “active shooter”, and because of this statistics on the subject are diverse. For the purpose of this paper, when using the term “mass shooting” it will refer to the definition stated by Bjelopera et al. (2013):

‘Incidents occurring in relatively public places, involving four or more deaths – not including the shooter(s) – and gunmen who select victims somewhat indiscriminately. The violence in these cases is not a means to an end such as robbery or terrorism’ (p. 4).

The Federal Bureau of Investigation (FBI) defines an active shooter as one or more individuals actively engaging in killing or attempting to kill people in a populated area (Silver et al., 2018, p. 1). When using the term active shooter, it is in reference to this definition stated by the FBI. The term “stressors” will also be discussed, which according to the FBI in this context are physical psychological, or social forces that place real or perceived demands or pressure on an individual and which may cause psychological and or physical distress (Silver et al., 2018, p. 15). A very important stressor in this context is “mental health” which indicates that the active shooter appeared to be struggling with (most commonly) depression, anxiety, paranoia, etc. in their daily life in the year before the attack. (Silver et al., 2018, p. 17) I will often use the term “shooter” when referring to both mass shooters and active shooters. With consideration to their differences, the qualities that are being discussed are applicable to both terms. Unfortunately, it is impossible to create a demographic profile of shooters, as there are very few demographic patterns or trends other than gender that can be identified. For this reason, it is more appropriate to identify a shooter based on behavioral characteristics rather than relying on demographic characteristics.

This paper will discuss the possibility of preventing mass shootings and active shooters by identifying the shooter prior to the attack by being alert for observable, concerning behaviors. With this background knowledge on the topic, the paper will go on to explain the many aspects and controversial theories on this subject. It will start by describing the planning and preparation processes of the attack by the shooter. The discussion of various stressors that are considered when analyzing shooters will be explored, including mental health as a stressor. Next, concerning behaviors exhibited by the shooter and then transition into the subject area of analyzing the primary grievance, and or cause of the shooter's distress or resentment will be analyzed. Finally, the prevalence of suicide ideation and attempts among shooters will be discussed. With this information considered, this paper will conclude with detailed findings of various behavioral, statistical, and scientific research by restating my opinion that mass shootings and active shooters can be prevented by educating the public about common pre-attack behaviors displayed by past offenders.

Planning and Preparation of the Attack by the Shooter

Many factors are involved in the process prior to the shooting incident. The two aspects often examined when studying a shooter's pre-attack life are the time spent planning the attack and the time spent preparing for the attack. These time periods are related and they include the various decisions and actions undertaken by the shooter. In one study conducted by the FBI, 63 active shooting incidents that occurred between 2000 and 2013 were analyzed and compared to one another⁵. In the context of this study, Silver et al., (2018) states that:

'Planning includes the decision to engage in violence, selecting specific or random targets, conducting surveillance, and addressing all ancillary practical issues such as victim schedules, transportation, and site access' (p. 13).

This specific time frame that the planning process began is often very difficult to establish. This is due in part to the fact that planning is often started with an internal thought process known only to the shooter. In every case

⁵ This study is the second phase of a report published in 2014 by the FBI titled *A Study of Active Shooter Incidents in the United States Between 2000 and 2013*. To read more information about the two phases of the study please refer to: <https://www.eagletechnology.com/wp-content/uploads/2018/06/A-study-of-the-pre-attack-behaviors-of-active-shooters.pdf>

studied by the FBI there was at least some evidence to indicate that the shooter planned the attack, and that the attack was not a spontaneous response to a single immediate stressor. To determine the amount of time that is spent planning the attack by the shooter, evidence such as conducting pre-attack surveillance of the target and or engaging in conversations with others regarding stressors, tactics, the venue or potential victims is examined. Other materials are also considered, such as journals and computer hard drives that belong to the shooter. These items are more difficult to discover prior to the attack and are more commonly found following the incident. Actions undertaken by the shooter prior to the incident like conducting surveillance are often easier to identify and can be reported as concerning to authorities. The same study conducted by the FBI was able to determine the amount of time spent planning the attack in 34 active shooter cases. Most perpetrators spent less than two months thinking about their specific attack strategy, while over 9% of the cases showed 13 to 24 months of time spent planning (Silver et al., 2018, p. 13). Over these months, there are possible opportunities to identify actions undertaken by the shooter in the planning process of their attack.

The time spent preparing for the attack in this context involves actions rather than internal thought processes. Silver et al., (2018) states:

‘Preparing was narrowly defined for this study as actions taken to procure the means for the attack, typically items such as a handgun or rifle, ammunition, special clothing and/or body armor’ (p. 14).

Activities in this area were more easily noticed by others, such as ammunition being delivered or visiting a gun store. More evidence relating to preparing for the attack was found by the FBI than evidence for planning the incident. In more than half of the cases studied by the FBI where the time spent preparing was known, shooters spent one week or less preparing for the attack (Silver et al., 2018, p. 14). This creates a smaller window of time to notice concerning behaviors and interrupt the execution of the attack. With this information considered, in four cases where shooters took less than 24 hours to plan and prepare for their attacks, all had at least one concerning behavior and three had an identifiable grievance (Silver et al., 2018, p. 15). Although statistics show that many of the shooters did not spend a significant time preparing for the attack, there were many actions displayed by the offender that could be identified prior to the incident.

Stressors

Almost all people confront stressors in some way in their daily lives and find resources and coping skills to overcome such challenges without resorting to violence. Unfortunately, mass shooters and active shooters cannot properly handle this distress and react with violent behavior. The FBI states that “stressors are physical, psychological, or social forces that place real or perceived demands/pressures on an individual and which may cause psychological and/or physical distress” (Silver et al., 2018, p. 15). Stressors that are often assessed in studies of mass shooters and active shooters include financial pressures, physical health concerns, interpersonal conflicts with family, friends, and colleagues, mental health issues, criminal and law issues, and substance abuse. Data shows that shooters were typically experiencing multiple stressors, (an average of 3.6 separate stressors) in the year before they attacked⁶ (Silver et al., 2018, p. 16). The largest area of stress is relational conflicts with partners, family, peers and at work or school (Schults, 2018). Again, the majority of society faces conflicts with others on a daily basis, but what is examined among shooters is their ability to navigate this conflict.

Mental health as a stressor applies to a significant proportion of mass shooters and active shooters. The stressor “mental health” is not meant to imply that the individual is diagnosed with a mental illness. This stressor in this context indicates that the perpetrator appeared to be struggling with depression, anxiety, paranoia, etc. in their daily life in the year before the attack. A study at the University of Glasgow found that 28% of multiple killers were believed to suffer from autism spectrum disorder (ASD) and 21% had suffered a definite or suspected head injury in the past (Dearden 2014). Although this appears to be a significant proportion of shooters that are believed to suffer from mental illness, it is not 100% of shooters, as many people may believe. Vintiadis states that “there is substantial research that shows that the correlation between mental illness and violence is much lower than is commonly assumed and that mass shooters are not in their majority mentally ill” (Vintiadis, 2018). Associating mental illness with violence is, in a certain aspect, a way to try to understand mass shootings. Evidence contained in the clear majority of research states that only a small percentage of shooters are mentally ill. It is unfair and misleading to generalize the whole population of shooters as mentally ill.

⁶ “The variables were treated as binary, that is, either the stressor was present or not, without regard for the number of separate circumstances given rise to the stressor. So, an active shooter who had conflict with one family member and a shooter who had conflicts with several family members were both coded as “yes” for “conflict with other family members” (Silver et al., 2018, p. 16).

Concerning Behaviors

Violent situations like mass shootings and active shootings rarely develop “out of the blue.” If the public is aware of warning signs, there are typically enough hints to alert those who are paying attention (Goodman, 2018). There appears to be a complex combination of behaviors and interactions with bystanders that may often occur in the days, weeks, and months leading up to an attack. Some of these behaviors include interpersonal interactions, physical aggression, potential symptoms of mental health issues, quality of the shooter’s thinking or communication, recklessness, firearm behavior, violent media usage, impulsivity, and changes in hygiene and weight⁷. A common behavior of potential shooters is also to blame others for their problems and go as far as to express a desire for revenge. The public should also be concerned if they observe an individual react inappropriately to other shootings or violence in the news, or not reacting to a tragedy in a serious manner. Continuously talking about previous incidents of violence involving themselves or others should also be considered a red flag for potential violence, or empathy with individuals committing violence. An increase in unsolicited comments about firearms and other dangerous weapons is another behavior that should be noted as unusual and potentially violent. In the workplace, there are additional behaviors that all workers should be aware of to indicate someone potentially acting out in a violent manner. These behaviors can include repeated violations of company policies, resistance and overreaction to changes in policy and procedures, increasingly talks of problems at home, escalation of domestic problems into the workplace, and talk of severe financial problems (Department of Homeland Security, 2008, p. 10). This puts workers in a unique position with insights to inform a threat assessment, given the high prevalence of financial and job-related stressors as well as conflict with peers and partners in the workplace.

The widespread perception that shooters tend to be cut off from those around them has been proven to be false. In the previously stated study conducted by the FBI, the majority (64%) of the shooters age 18 and older did live with someone else, and all of the shooters either lived with someone or had significant in-person or online social interactions (Silver et al., 2018, p. 18). The observable behaviors displayed by the shooters were most commonly noticed by the individuals who

⁷ “The FBI looked for documented confirmation that someone noticed a facet of the shooter’s behavior causing the person to feel a “more than minimal” degree of unease about the well-being and safety of those around the active shooter” (Silver et al., 2018, p. 18).

knew the shooter best, such as family, friends, classmates and co-workers. The people that are most likely to notice concerning behaviors of offenders are also the people that are less likely to act on these concerns. The family members and friends of the perpetrator may feel uneasy reporting the individual to authorities because of loyalty, disbelief and/or fear of the consequences (Silver et al., 2018, p. 20). Oftentimes, because of this, the concern is either brought up and stays between the person who noticed the behavior and the shooter, or nothing is done. Most often the unusual behaviors are noticed through verbal communication by the shooter or observing physical actions of the shooter. Other ways of noticing these types of behaviors include written communication and observing behavior that is displayed online. The majority of shooters demonstrate concerning behaviors that can be noticed in multiple ways. The study conducted by the FBI concluded that each active shooter displayed four to five concerning behaviors over time. While it may only be the interaction and cumulative effect of these behaviors that would cause alarm, early recognition and detection of growing or interrelated problems may help to mitigate the potential for violence (Silver et al., 2018, p. 19). Keeping in mind that there is no single warning sign, checklist, or algorithm for assessing behaviors that identifies a prospective shooter, individuals must always be aware of their surroundings and alert for certain behaviors. The challenge is having the situational awareness to observe a potential threat and then direct the appropriate resources towards the person in question before it is too late (Spicer, 2015). Although identifying the potentially dangerous behavior may seem like the difficult task, the task of reporting information to authorities to ensure that the individual does not cause harm to anyone or themselves is just as difficult and important.

Primary Grievance/Motivation and Suicide Ideation and Attempts

By studying past offenders, researchers have found that there is a wide variety of motivations that could lead someone to complete such a violent act of shooting. There is often a desire to “right the wrong” and achieve a measure of revenge. The previously stated study conducted by the FBI states that:

‘A grievance is defined for this study as the cause of the active shooter’s distress or resentment; a perception – not necessarily based in reality – of having been wronged or treated unfairly or inappropriately’ (Silver et al., 2018, p. 21).

It is possible that a shooter might have multiple grievances, but there is often a primary grievance that builds the majority of the anger in the perpetrator. There are also some cases that the primary grievance of the offender could not be determined due to insufficient evidence or there appeared to not be one. According to the FBI, those that did not leave any evidence of a primary grievance for the attack still displayed concerning behaviors, were under identifiable stressors, and engaged in planning and preparation activities (Silver et al., 2018, p. 21). There is also a significant percentage of offenders that experience a precipitating event related to their grievance shortly before the shooting, such as firing, romantic break up, or unfavorable legal outcome. While these events are very common among people in their everyday life, if someone reacts very poorly to an event like this it should be considered a red flag. It is not fair to generalize everyone who goes through a hard event and reacts poorly, but if someone becomes violent or displays any concerning behaviors it should be taken seriously.

It is not uncommon for potential mass shooters and active shooters to have suicide ideation or engage in a suicide attempt(s) prior to the shooting. Nearly half of the shooters studied by the FBI in the certain study had suicidal ideation or actual attempts at some time prior to the attack. Of these shooters, several made actual suicide attempts, and nearly three quarters of these behaviors occurred within one year of the shooting (Silver et al., 2018, p. 24). These behaviors are noteworthy as they represent an opportunity for intervention, and possible prevention of the attack. As stated by Silver et al., (2018):

‘Without stigmatizing those who struggle with thoughts of self-harm, researchers and practitioners must continue to explore those active shooters who combined suicide with externalized aggression (including homicidal violence) and identify the concurrent behaviors that reflect this shift’ (p. 24).

It is very important to not generalize all shooters or all of those who struggle with suicidal ideation. Many mass shooters and active shooters carry out their attack with no prior suicide thoughts or attempts, but it is a key behavior to be alert for in anybody.

Concluding Thoughts

In order to successfully prevent a mass shooting or active shooter, a combination of both people being aware of their surroundings and alert for concerning behaviors and reporting these observations to authorities needs to be present. Unfortunately,

there is no exact checklist to look for to identify an individual that could carry out such a tragic event. Simply being aware of the common behaviors displayed by past shooting offenders can potentially save lives. The most difficult part of disrupting a potential attack may be gaining the courage to report the individual to authorities, mainly because the person who is often noticing the concerning behaviors has a close relationship with the offender. Without being aware of the behaviors that may be concerning, there is no chance of them getting reported as potentially dangerous.

It is very clear that it is not a simple task to interrupt the planning and preparation of a mass casualty event like a shooting. There are many considerations regarding this topic, most importantly that it is not realistic that the shooter always shows any warning signs or leaves any traces of evidence prior to the attack. This is a very rare occasion, but unfortunately there would be no way to stop these attacks. Another limitation in this subject is that what caused shooters to act the way they do cannot be explained simply by the presence of a grievance (Silver et al., 2018, p. 22). It is often difficult to trace the interaction of various psychological stressors and operational considerations that lead them to carry out the attack until after the fact. It is important to note that simply because some shooters do spend less than 24 hours planning and preparing for their attack, it does not mean that there are no potential warning signs or evidence of escalating grievance that exist and may be detected earlier. It is not to suggest that every concerning behavior calls for assertive intervention, as many of the concerning behaviors mentioned do not necessarily suggest deadly violence to a reasonable person. Unfortunately, the public may not start to believe that it is possible to prevent shooting attacks until more attacks happen, and possibly not until an attack involves someone that they know.

The purpose of this paper is to heighten the need for family, friends, co-workers and professionals to report the concerning behavior of individuals. If more people are aware of the warning signs to look for and even just one potential attack is disrupted, hundreds of lives could be saved. Although predicting a shooting can seem daunting, these events hardly ever happen “out of the blue”. It is important to understand that there are often opportunities before a shooting to recognize concerning behaviors that may suggest progression toward violence. By educating the public about these signs and behaviors exhibited by a shooter, the chances that a bystander will detect and interrupt a shooting prior to the attack increases. Although there are no prevention strategies for shooting attacks that have been proven to work in every situation, there are prevention approaches that are worth the effort they require. Information on this subject will only get stronger and more in depth with further research and will potentially save many lives.

Chapter 5

Framing Grey Area Violence in Media and Politics: A Framework for Decision Making

Abigail Kuchek

Abstract

This paper creates a decision-making framework for determining best practices for media and political accounts of acts of violence that may reasonably be described as terrorism but are not definitive cases of terrorism. The framework seeks to explore the ethical and practical dimensions of using the term “terrorism” to describe these “grey area” acts of violence. Relevant texts in social psychology, security studies, and philosophy of language are consulted to develop a multi-disciplinary approach.

Background

What differentiates terrorism from political violence?⁸ Despite a \$70 billion global increase in homeland security investments since 2001, “*one man’s terrorist is another man’s freedom fighter*” is still tossed around as experts debate the exact definition of “terrorism” (King, 2008). Although this cliché is often used by

⁸ There are many more aspects of the definition of terrorism that are still debated, but this paper is primarily concerned with the blurred line between terrorism and political violence (justified or otherwise).

political leaders to disguise terror campaigns as “revolutionary violence” and “national liberation movements,” there is a legitimate basis for discussion on the definition of terrorism (Ganor, 2002, p. 124). There is a category of violence that is undeniably terroristic, but some violence also exists in a proverbial “grey area.” The choice to label such violence terrorism is neither simple nor inconsequential. In order to better understand the term’s significance when describing such violence, this paper seeks to provide an account of the effects of employing the term in media and political settings and to construct a framework for making the decision to use or avoid the label in these settings.

For the purposes of this paper, the term “grey area violence” will be used to describe acts of violence which could reasonably be labeled terrorism (especially in public discourse where competing conceptions of terrorism are given equitable platforms) but which are not blatantly obvious acts of terrorism. For example, attacks coordinated by recognized terrorist organizations such as Boko Haram or ISIS are textbook acts of terrorism. However, in ordinary usage, ideologically motivated active shooters may be termed terrorists by some and common criminals by others. This paper will not venture to form a more specific definition of grey area violence in order to keep the term appropriately interpretive, but the way the term would be employed in ordinary usage serves as a useful rule of thumb. Moreover, the usage of the term terrorism discussed here will be termed “media and political usage,” but this terminology is also left intentionally broad. Media usage generally refers to employment of the term in media coverage of terrorism, political violence, and other forms of political violence. Political usage refers generally to the use of the term in statements and speeches from politicians that are directed toward their constituencies or the public at large; this usage seeks to exclude formal intra-governmental policy debate.

Given that grey area violence is an increasingly salient threat, this paper has two goals⁹. Firstly, the paper seeks to examine the ramifications of labeling grey area violence “terrorism” in media and politics through an examination of relevant literature in philosophy and social psychology. Secondly, the paper seeks to produce a framework for making the choice to use the label “terrorism” when discussing acts of grey area violence in media and political usage. The way

⁹ For example, rates of lone wolf terrorism have risen markedly in the U.S. since the 1950’s (Spaaij, p. 860). The European Union defines lone wolf terrorism as “intentional acts that are committed with the aim of seriously intimidating a population, or unduly compelling a Government or international organization to perform or abstain from performing any act, or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization.”

grey area violence is portrayed in the media and in politics plays an important role in co-opting the public as a partner in counterterrorism efforts, and thus plays an important role in advancing international security interests. Therefore, policy suggestions made in this paper will primarily be to the end of advancing national and international security. However, the paper will conclude with a brief discussion of the ethical elements of the decision.

Philosophy: The Significance of Labeling Grey Area Violence Terrorism

To understand the significance of the term “terrorism,” it will be helpful to pick apart its functions using the philosophy of language. Eric Reitan produced a particularly useful account of the term terrorism in his paper *Defining Terrorism for Public Policy Purposes: The Group-Target Definition*. Reitan asserts that “terrorism” is an *essentially contested concept*, meaning that it is characterized by “competing definitions unified by a common appraisive meaning and a shared set of paradigms” (Reitan, 2010, p. 255). This means that the term does not have a singular definition; rather, its usage indicates a condemnation of whatever it is used to describe and may be appropriately used to describe things that fit a *loose* set of criteria. While Reitan thinks that “contested concepts perform the valuable function of preventing some voices from being cut out of public debate by a kind of *definitional fiat*,” a precise definition is necessary for professional usage in order to draft coherent public policy aimed at addressing a *specific* threat (Reitan, 2010, pp. 255–256).

By definition, contested concepts have a descriptive and evaluative character, but terrorism also seems to have a *prescriptive* character that Reitan does not touch on. For example, when one says, “The toilet is broken,” the term “broken” prescribes fixing, or asserts that someone *should* fix the toilet. Similarly, a sentence like “Active shooter violence is terrorism” prescribes a need to control and combat that violence. This is, at the very least, true in the cultural context of the United States and Europe, where counterterrorism plays a significant role in political debate and, to an extent, patriotism and national identities. Using the term “terrorism” in societies with this context to describe an act of violence indicates that it is not simply a random act of violence beyond a given society’s control, but that it is part of a class of violence that the U.S., the European Union, and many other societies across the globe have made a concerted effort to combat. While this prescriptive character does not necessarily imply a specific course of action or assign obligations to a specific actor, it clearly does indicate a need for *some*

course of action by *some* actor. This prescriptive character is an important part of the ordinary usage of the term and, by extension, the way the public understands the term.

The public's conception of terrorism and other forms of political violence is important to counterterrorism and international security efforts, especially for forms of grey area violence that are especially difficult for intelligence agencies to anticipate. Family members and close friends of potentially violent people on a path of radicalization are in the best position to intervene, either by dissuading the individual or by contacting authorities (RAND, p. 24)¹⁰. Given the significance of public cooperation with counterterrorism efforts, the descriptive, evaluative, and prescriptive character of "terrorism" should be carefully weighed before being employed. Using the term in a media and political setting to describe a form of violence communicates not only condemnation and categorization of that violence, but a call to action to combat it.

Reitan sought a definition that could be used to shape public policy while acknowledging that creating a clear-cut definition for ordinary usage would be both impossible and irresponsible. This paper deals in the space between Reitan's public realm and policy realm. It would be misguided to construct a strict definition for media and political usage given the significance of the word, the importance of public cooperation in counterterror efforts, and the complexities of public response to perceived threats of terrorism. Creating a *framework* for media and political usage decisions will be a more appropriate path forward.

Social Psychology: The Impact of Terrorism and Media Coverage of Terrorism

The first step toward understanding the repercussions of labeling grey area violence terrorism in media and politics is understanding the social psychological impact of terrorism on a society. For the purposes of this paper, it will be best to analyze the societal response to terrorism using the concept of *relative risk appraisal*. This is the process wherein human beings evaluate future risks to their health and safety based on indicative events. Studies have indicated that events with high *Dread Risk*, meaning events that are extremely "catastrophic, uncontrollable, and inequitable," and events with high *Unknown Risk*, meaning events with

¹⁰ According to the RAND Corporation's report on lone wolf terrorism, *Stray Dogs and Virtual Armies*, an estimated one-third to one-half of known [lone wolf terrorist] cases began with a tip from within the Muslim community.

“characteristics such as not being observable, not knowing when one is exposed, and not knowing the mechanism of potential injury,” contribute to high *signal potential* of a given hazardous event. Signal potential “functions as a warning sign that a new ongoing threat has entered the environment” (Marshall et al., 2007, pp. 308–309). High *Dread Risk* and *Unknown Risk* also tend to produce “attitudes towards the [threat] such as willingness to pay for safeguards and demands for regulation” (Marshall et al., 2007, p. 308).

Acts of terrorism have a high signal potential because they have high *Dread Risk*, high *Unknown Risk*, and because the ideological character of terrorism can be collectively understood by the targeted society as indicating the existence of an *ongoing* threat rather than an isolated incident. The way that politicians and media present information on terrorist attacks have a major impact on the signal potential of such events. For example, psychologists have linked media exposure of the 9/11 attacks to PTSD symptoms in U.S. residents who were not directly threatened by the attack. They proposed that the relationship formed because “unlike most media coverage of disasters, specific aspects of the 9/11 attacks – its scale, unpredictability, novelty as a threat, and implications for future safety, together with media saturation of graphic images and frequent government warnings of future attacks—carried the signal potential that there was a significant ongoing threat, with greatly elevated risk for being harmed in additional attacks” (Marshall et al., 2007, p. 309). Both the nature of terrorism and the way that journalists and politicians depict it contribute to the threat’s high signal potential. This high signal potential causes disproportionately intense relative risk appraisal.

Exaggerated relative risk appraisal can account for the drastic uptick in hate crimes committed against people of Middle Eastern descent and people of color in the U.S. in the weeks following 9/11. The relative risk appraisal was also likely responsible for the 20% decline in air passenger travel in the last four months of 2001 (Marshall et al., 2007, pp. 310–311). The increased rates of avoidance behaviors and racially motivated violence illustrate the grave psychological, social, and economic impacts distorted relative risk assessment can have on a society when it occurs *en masse* as the result of large scale violence.

Research has also indicated that acts of terrorism produce a heightened need for *cognitive closure*. The desire for cognitive closure is defined as “aversion toward uncertainty and ambiguity, with a preference for firmness and stability in beliefs and expectations” (Orehek et al., 2010, p. 280). Subjects who exhibited an aroused need for cognitive closure when confronted with terrorism threats showed reinforced ingroup and outgroup identification, enhanced feelings of solidarity amongst ingroup members, and heightened negative attitudes toward

outgroups (Orehek et al., 2010, p. 288). Affected subjects also showed higher levels of support for tough counterterrorism tactics, including costly measures and “controversial ones at apparent odds with individual rights and humanistic concerns” (Orehek et al., 2010, p. 281). Support for severe counterterrorism policies was shown to be positively related to optimism about future safety from terrorism (Orehek et al., 2010, p. 286). Group identifications and bolstered support for tough counterterrorism policies were termed the “rally around the flag effect.” Finally, research indicated that subjects confronted with terrorism that show heightened need for closure are more likely to support decisive leaders and less likely to support indecisive leaders, and perceived failure of a given counterterrorism policy may prompt individuals in this psychological state to shift support to other leaders or other courses of action (Orehek et al., 2010, p. 289). This research illustrates that terrorism has a significant impact on public sense of security and political and social orientation.

Extensive research has been done on the social psychological impact of terrorism, but the research outlined here is the most pertinent to the question of media labeling of grey area violence. In the subsequent sections, this paper will attempt to create a guideline for making the choice to label or not label a given act of grey area violence terrorism. All the research explained in this section will play a crucial role in that framework, but special attention should be paid to signal potential and need for cognitive closure. These are foundational features with significant social, political, and economic ramifications and thus must be considered very carefully.

Theoretical Analysis: Foundations of a Best Policy

The research presented thus far serves as the basis for constructing the best policy because it gives a preliminary account of both the linguistic function of the term “terrorism” and the concrete repercussions of terrorism on the public. A framework for decision making should function on both a theoretical, linguistic level and a concrete, evaluative level. It should also focus on the application of the research to media and political usage and the unique features of grey area violence as opposed to traditional forms of terrorism. Therefore, the framework constructed here will have two distinct parts: the first will be a theoretical foundation for decision making, and the second will be a practical analysis of expected societal impacts of media and political usage. This section will serve as the theoretical foundation, exploring how labeling grey area violence terrorism alters the meaning of that violence and how this affects the

way the public understands both the given form of violence and terrorism as a broader class of violence.

The linguistic function of the term terrorism, when applied to grey area violence, must be understood according to both the previously explored philosophy and social psychology. The term “terrorism” can be conceptualized as a marker or tag that alters the context of grey area violence. The descriptive character of the word indicates simply that the qualities of a given act of violence fit the definition of terrorism. The evaluative character marks the form of violence that the term describes as being condemnable and unjustified. Most importantly, the prescriptive character of the term marks the form of violence as one that *should be combatted* as part of the larger counterterrorism effort. In this way, the prescriptive character means that choosing to label an act of grey area violence an act of terrorism is a framing mechanism. The label changes the way that the event is understood by the public by communicating the idea that it is not merely an isolated incident of indiscriminate violence, but a single incident in a larger pattern of terrorism. The event is thus contextualized as indicative of a threat that is targeted, ongoing, and presently being combatted. By extension, this can alter the public’s conception of terrorism by making it appear broader, more varied, and thus, potentially more difficult to combat. Therefore, framing an act of grey area violence as terrorism affects public understanding of that event, the type of violence that the event exemplifies, and the nature of terrorism. The linguistic action of the term is, therefore, the foundation for shifts in cognition and, in turn, behavior.

Note that this linguistic function can be performed regardless of whether a given act of violence fits neatly into widely accepted professional definitions of terrorism or not because of the dissonance between professional and ordinary usage discussed in Reitan’s paper. In fact, the linguistic action is especially significant because it has the potential to inspire the psychological responses to terrorism that otherwise may not have occurred in citizens who would not have considered an act of violence an act of terrorism without framing in media and political usage. Consider an act of grey area violence wherein a perpetrator, acting alone, uses a knife to attack civilians in a crowded public area. After being arrested, the perpetrator indicates that the attack was motivated by political ideology and intended to send a message to the public. However, the attacker is not involved in or ideologically aligned with any existing terrorist organization. An attack like this would be considered terrorism according to many professional definitions, but ordinary usage would likely diverge on this case as many would only consider such a perpetrator a common deranged criminal rather than a calculated terrorist. In such cases, media and political usage of the term “terrorism” has the

potential to manufacture a specific set of social psychological responses unique to terrorism.

This is to say that framing instances of grey area violence by labeling them terrorism lends them a stronger signal potential. An act of violence that ordinary usage would diverge on would more likely be understood as an act of senseless, random violence rather than an indicator that more similar violence is to come. Calling an act of grey area violence terrorism could give the impression that the given form of violence is likely to recur and that the threat of terrorism is diversifying. This is clear in the way that lone wolf terrorism is understood as an extension of “traditional” terrorism. Both effects would clearly be to the detriment of the public’s sense of security and can result in a plethora of other effects. Some of the most salient potential effects will be analyzed in the next section.

Practical Analysis: Consequential Framework of a Best Policy

The previous section explored the theoretical shifts in cognition that framing grey area violence as terrorism produces. This section will explore the changes in societal behavior and political attitudes that have the power to produce tangible consequences in society and counterterrorism efforts. To do this, expected societal responses to the framing of grey area violence (and their consequences) will be organized into two categories: potentially positive and potentially negative. These will be categorized primarily according to their impact on state security.

The potentially positive effects position encourages the public to be a more effective partner to organized counterterrorism efforts. The most significant potentially positive effect is that framing a form of grey area violence as terrorism communicates a greater level of severity of such violence. Although assigning more gravity to a threat can harm the public’s sense of security, it can also result in a greater level of awareness of a given form of violence. The public is more likely to make countermeasures a political priority and support expenditures on and enactment of such measures (Marshall et al., 2007, p. 308). They are also more likely to enact a “see something, say something” mantra and contact appropriate authorities when they are aware of signs of such violence. This is extremely important for combatting forms of grey area violence like lone wolf terror, which is otherwise extremely difficult to detect in advance. A public awareness and understanding of a given form of grey area violence, thus, lends itself to greater public partnering in efforts to counter that violence.

The “rally around the flag” effects may be aggravated by a perception that the terrorism threat is growing and diversifying and a decimated sense of security. These effects are best understood as a double-edged sword. The potentially positive side of these effects include a bolstered sense of patriotism, heightened support of state counterterrorism measures, and support for decisive political leaders. In a democracy, public political “rallying” around a given course of action has significant power in enacting desired policies through electing leaders who support the given policies and through constituencies pressuring their elected officials to support those policies. A shared vision and sense of unity in a democracy can go far in producing desired results. Again, these “rally” effects are positive because they improve the public’s ability to act as a partner in counterterrorism efforts.

However, the potentially negative side of that sword is the dark underbelly of nationalism. An aggravated sense of ingroup and outgroup identification in a society can exacerbate racism and provoke hate crimes, as was the case after 9/11 (Marshall et al., 2007, p. 311). A sense of insecurity can result in a hunger for populist leaders, and a dissatisfaction with policies perceived as ineffective or not appropriately severe can result in a push for policies that are inhumane or sacrifice important rights like privacy. In that vein, note that counterterrorism measures often involve much stickier policy debates, weighing human rights, restrictions on weapons, and personal privacy against measures to increase public safety. There is also concern about security policies discriminating against religious minorities and people of color. Public support for more extreme measures has the potential to steamroll these nuanced pieces of the conversation. In short, labeling grey area violence terrorism has the potential to further attack the public’s sense of security, and this has the potential to push portions of the population toward bigotry and extremism.

The heightened sense of insecurity can also produce avoidance behaviors in a society. The relative risk appraisal of an act of violence associated with terrorism can produce a public fear of a given place or activity that the threat of violence appears to have rendered less safe. The resultant avoidance behaviors can have economic ramifications. This occurred after 9/11 when air passenger travel rates plummeted, harming the industry (Marshall et al., 2007, p. 310). It can be argued that this sense of fear, its resultant avoidance behaviors, and increased political instability produced by a surge in populism and extreme views “*give the terrorists what they want.*” The significance of this point and the question of whether this encourages more radicalism and terrorism can be debated, but the notion is worth considering when deciding whether to label grey area violence terrorism in media and political usage. The notion, as well as the effects that feed into it, are important potentially negative effects in a framework for decision making.

Conclusion: Limitations and Ethical Considerations

Ultimately, the choice to label or not label an act of violence will likely produce both positive and negative outcomes including, but not limited to, those previously described here. This paper seeks to present some of the most salient of these possible effects. However, analyzing the power of the word “terrorism” and then enumerating its possible outcomes is an isolating and highly abstract approach. In reality, social response to mass political violence is extremely complex. There are too many moving pieces to keep track of, and they interact with each other in ways that mute some effects while amplifying others. Therefore, this paper is limited to producing a framework for decision making. It seeks only to offer “something to chew on” when making the choice, but not to offer a single “yes” or “no” answer to the question, *should the media label a given act of grey area violence “terrorism?”* There are no simple answers to this question and striving to produce one would be a fool’s errand.

Moreover, there is a moral layer to the question that must be addressed alongside pragmatic considerations. There are ethical questions lying beneath every security concern explored in this paper. For example, the use of the term “terrorism” as a framing mechanism can have real repercussions on complex policy debates. Framing can influence a society to blindly support security measures at the expense of rights like privacy. There is an ethical dimension here that has the potential to offset security considerations. While it may aid the state in counterterrorism efforts to render a society more supportive of such efforts, even this potentially positive effect borders on a fearmongering technique that capitalizes on violence to further state ends. Moreover, this increased support comes at the expense of the public’s sense of security and runs the risk of producing economically and socially damaging consequences like avoidance behaviors and hate crimes. Framing—both in terms of the choice to use terrorism to describe grey area violence and, in a broader sense, the way media and politicians portray violence—is a question not only of efficacy but of ethics.

Chapter 6

“If it Bleeds it Leads”: How Mainstream Media Shapes Public Opinion on Terrorism

Hazal Bulut

Abstract

The purpose of my research is to discover and understand how ‘mass media’ can shape public opinion on terrorism. When the information is represented through media mechanisms such as television, radio, newspapers and social media, the majority of the public considers it to be true. Manipulation is something the public is unaware of. This paper will start by discussing how the media has changed over time with the advances of technology and with the emergence of social media, the number one source for many people in this new informational age, and how this has advanced terrorism. When utilizing the term ‘informational age’, it is referring to the digital, computer age or the new media age. The paper will also talk about how the concept of terrorism emerged after the progression of the mass media, how media tends to incite panic within the public for views and how it’s linked to terrorism by giving examples from several studies and research that shows that terrorism cannot exist without the media due to its need to spread messages of propaganda by using new-media (known as social media) tools such as Twitter, Instagram, and Facebook. The paper will conclude by arguing how we can prevent third parties, that are often not trustworthy, to change our perspectives and views on happenings in the world.

Introduction

One of the most powerful communication tools in today’s world is media. It is considered the best source to know about the happenings of the world. In fact, the public’s interest in terrorism surfaced after the evolution of the mass

media. As technological advances started to increase rapidly, public awareness started to increase rapidly and resulted in a global change in news coverage. As a larger market emerged for media, the competition grew among rival news organizations for larger market shares and audience views. This leads us to the new media age where a technique referred to as “yellow journalism” is used. When employing the term yellow journalism, it refers to ‘the use of cheaply sensational or unscrupulous methods in newspapers, etc. to attract or influence readers’ (HarperCollins Dictionary, 2018). We all know that media satisfies our essential need to stay connected and relevant, but what we do not realize is the effect it has on our lives and how it has the power to influence our thoughts and our perspectives. Trusting a source, especially nowadays, without considering its accuracy can be dangerous. Mass media is a very powerful weapon that can and will change one’s perspective in a split second.

The change in media not only affected the happenings in the world, but also the public and their thoughts. We simply think that we are being offered a simple access to a global stage, but it is much more. The biggest terrorist organizations evolved after the change in the media. They started utilizing every social media platform¹¹ for their propaganda (Weimann, 2004, p. 6). Many terrorist groups use these resources every day because the Internet is the cheapest, quickest and the most anonymous way to spread propaganda among many other materials. What is more important than any of the other listed factors is that the internet is an interactive platform. They can recruit, inform and train new members for their organizations (Weimann, 2003, p. 8). Each video is prepared carefully with the aim of reaching many individuals. They can reach specific groups when needed by using a direct, young language and images or videos with a high emotional impact. The propaganda is multi-lingual with easy access. It is basically a safe environment to advertise themselves. The Internet can be considered a stage for the terrorist and the world is watching them.

The Evolution of Terrorism and Mass Media Technology

A prevalent question asked throughout history is, what are the drives of terrorism, the government, public, individuals, military and businesses. From the beginning, most terrorists’ and terrorist organizations’ end goal is not the killing itself but to send a message. Ideology always plays a part when selecting targets for attacks. What would I get out of this attack? What kind of a message would

¹¹ Facebook, Twitter, Youtube, Instagram

be sent to the world? How can this attack be worldwide? In today's world with the advances of technology, training and level of education observes can place attacks in context, anticipate the next attempt if examined closely. Technology has become a weapon for terrorist groups. Powerful terrorist organizations like ISIS, PKK (Kurdish Workers Party), Hamas and many more have a deep knowledge about the communication techniques used by the internet. They can now shorten their terrorist attack cycle¹² by selecting their targets using the internet. Experts stated that the number of websites containing terrorist material increased drastically since 1998 (Weimann, 2004). Terrorist groups are now exploiting darknets, computer networks with restricted access that is used mainly for illegal peer-to-peer file sharing, which are increasing the number of terrorist operated websites. Propaganda is not the only purpose, they use it for secure communication, fundraising, buying false documents, gathering information, software distribution, purchasing weapons and stolen card data, doxing and psychological warfare (The use of the Internet, UNODC, 2012).

Technology is the foundation of modern society, therefore, it is natural for terrorists to benefit from it. Cyberspace is a platform without boundaries. Terrorists and terrorist organizations can launch attacks everywhere in the world. Many technological advances, such as smartphones, have made it easier to conduct surveillance operations, to use remote cameras to monitor potential targets, and utilize internet-based platforms for training new recruits and teaching techniques on how they use and produce their weapons. Ghost Security Group chief operating officer Michael Smith II told the Christian Science Monitor (Detsch, 2015):

'They want to create a broadcast capability that is more secure than just leveraging Twitter and Facebook. Increasingly what you will see is the focus on developing means to control the distribution of their materials on a global scale.'

There are many examples of distributing terrorism through the internet, like al Qaeda producing detailed videos on how to use and make homemade explosives and Jihadists having an online university where they have an interactive learning environment with encrypted video conferences. All these implements create a habitat where planning attacks are much easier. Social media serves the modern

¹² As listed in STRATFOR Analysis "The Terrorist Attack Cycle: Deployment and Attack" available at <https://worldview.stratfor.com/article/terrorist-attack-cycle-deployment-and-attack#:~:tar=get-planning-deployment-attack-escape-exploitation>

terrorism and these past couple of years it has reached a global dimension because of the emergence of new media and technology.

How do Terrorists and Terrorism Organizations Manipulate the Media?

There is an ongoing change in the media right now as technology and social media become rapidly more important than printed newspapers. Agencies have less control over the news, which makes it easier for terrorist organizations to utilize social media and address the public directly through social media tools and web-based magazines. The unfiltered media exposed a high amount of terrorist propaganda. They were using the ‘oxygen of publicity’ (Thatcher, 1985)¹³. Before social media platforms it was hard for people to encounter terrorist propaganda, videotapes, and audio messages, but with today’s advanced technological tools, terrorists and terrorist organizations can easily record and upload their attacks on the internet. Everyone who has access to the internet have access to these videos. Terrorists have always altered their behavior to best use the media and they know from the start what would attract the media the most for them to use it on the news. It is becoming harder and harder to control the platforms and what we do not realize is that terrorists and their organizations are becoming their own media. Brian Jenkins, an International Terrorism expert, said (Jenkins, cited in Marthoz 2017, p. 10):

‘Terrorist attacks are often carefully choreographed to attract the attention of the electronic media and the international press. Terrorism is aimed at the people watching, not at the actual victims. Terrorism is a theater.’

After the drastic changes in how the media operates there is a clear link to changes in terrorist attacks including frequencies and types. The idea that the attacks are acts of propaganda is becoming more vivid. Terrorists and terrorist organizations utilize attacks to manipulate the media into spreading their messages and panic. Terrorists becoming more active in the 1960s and 1970s quickly adjusted to the idea of television. Video footage is more powerful than printed sources. There are several examples of such acts like the kidnapping and

¹³ Term used by former British PM, Margaret Thatcher to describe the terrorists’ dependence on the media.

killing of Israeli athletes in 1972 at the Olympics in Munich, which was the first Olympics to be televised live. The terrorist group called "Black September" kidnapped and killed 11 Israeli athletes. Then followed the 1975 hostage crisis at OPEC (The Organization of Petroleum Exporting Countries) in Vienna where attackers took more than 60 hostages. Several were injured, and the attack ended after two days, when the attackers walked away after sending their threat message. The target was not only televised events or big headquarters that would be on the news. For example, in 1985, it was the hijacking of TWA 847 (Trans World Airlines) and in 1988, the target was the Kuwaiti Airlines 422 flight, then of course the most viewed hijacking was the United Airlines Flight 93 on September 11, 2001. These events, particularly 9/11, created a global sense of terror and that is when the wait started for many similar world events to come. American hostages who were taken to Beirut in 1985 is one of the best examples of terrorism's capability to draw attention and manipulate the media. This is the point where television changed, and news channels expanded to become available 24/7/365. Many experts agree that the most destructive effect of this crisis is the confirmation of terrorism as a tactic.

Attacks like these happen in different stages. "*Minimanual of the Urban Guerilla*," a book written by Carlos Marighella, a Brazilian terrorist, discusses different ways of taking advantage of the mass media for terrorism purposes, attracting attention through violence, and spreading a message.

A study from Gabriel Weimann from Haifa University in Israel explored how one terrorism act affects the media and shows that terrorist organizations manipulate the media in a way that makes them 'rationalize' the act (Nelson & Scott, 1992, pp. 329–339). If terrorists have social or political motives, the reasons behind them are represented in a way that the public feels sympathy for the terrorists. They now use the media to ensure promotion, publication and distribution. As a result, terrorist acts have improved over the time and nobody stopped the news channels, newspapers, social media tools or radios.

How does the Mass-Media Change the Public Opinion for Views and Ratings?

There is a well-known motto in the journalist community, "If it bleeds, it leads" which means the more immediate, negative, and panic-leading the event is, the more it will get attention. The coverage of terrorism has increased rapidly since the 1960s and 1970s. Television channels tried to take a step back from covering minimum 30-minute terrorism news, but they would still use a 3-minute video

to advertise it for their viewers, which meant ratings. It got to a point where the smallest terrorist attacks, that meant no danger to the public for the media to warn or inform, had a great news coverage amount. According to the Gallup Poll, 51% of Americans feared for their lives and families more and more every day. This data shows us that the 'media' does more damage to the public than the attacks itself.

Informing about dramatic terrorism events such as kidnapping, hostages, international terror, events that involve kids, means more public attention, which means more views, and ratings that will benefit media companies' profit. Every percentage of rating increase raises the annual income by millions of dollars. Editors seem to only care about their profits and are not aware of the political implications and public trauma they cause. There are many examples of how the media interrupted counterterrorist operations due to irresponsible behaviors. Television crews approached too closely to the hostage area complicating rescue team's actions and newscasters released too much information. By giving major publicity to terrorist actions, the media is increasing public pressure on government representatives to give in to their requests. There are many cases when journalists took the responsibility of negotiating with terrorists. CBS White House correspondent Lesley Stahl once stated (Diamond, 1991, p. 133):

“We are an instrument for the hostages... We force the Administration to put their lives above policy.”

As much as terrorism organizations and terrorists manipulate the media and how the media seems unaware of what is going on, nothing is pursued to stop this cycle. Ratings, profits and views are more important than the sanity of the public. The propaganda by terrorist groups that is open to the public is a very strong psychological weapon. It greatly increases the outcome acts from the public that leads to panic. It is a 'show business' that the media is putting on and the public is getting fed by it.

Concluding Ideas and Thoughts

As much as it is important for the media to be the first to release information on happenings it also very important to collect as much detail and data as possible. This is another example which media and terrorists have in common; after the story is created, they both want to keep it alive for as long as possible. The greater the drama, the longer reporting about it holds the audience attention that is in the interest of both media and terrorists.

Terrorism and media are bound together and complement each other. What we, as a public, need to do is very simple. Awareness is the number one key point. What needs to be kept in mind is that the news we hear, or watch might not always represent the facts. Being biased should not be an option. News agencies need to check and make sure of the news before spreading, leave general stuff to the agencies and leave non-official sources. If we want to make this world a peaceful place, we need to work on it together as a whole.

Chapter 7

United States Mass Shootings Placed in Context with Media and Public Discussion

Charles Schmidt

Abstract

Mass shootings: have there been over 2000 cases in the last 5 years or 314 cases in the last 134 years?

Mass shootings are a staple of modern media news and public conversation, but actual rates are easily misreported and misinterpreted. In this article, the difference between mass shooting research will be examined with examples from government agencies, university research and media coverage of the events. Firstly, the most recent crime data will be explored to frame the discussion of how mass shootings fit into the overall crime picture. Next, the issue of defining a mass shooting will be discussed with different definitions and the breakdown of why defining a mass shooting is difficult. Finally, different mass shooting studies and/or databases will be examined to show how the rates are easily confused if not placed into the correct context of each study.

Introduction

Research on mass shooting is at the forefront of the United States national debate over possible answers to mass shooting events. Empirical and peer-reviewed research is the basis for all political, public and media conversation that takes place surrounding a mass casualty event. As the media shapes the public discussion by drawing from the academic research, it is vitally important that the conclusions of the academic community are interpreted properly and within the

correct context of what each report sets out to accomplish. The research itself is riddled with complications stemming from the definitions of these events, the inclusion or exclusion of events, and the potential biases that each set of data is recorded in. Each one of these issues has the ability to shape media and public perception with incorrect or misinterpreted empirical research.

Crime data put in perspective

In order to first understand what mass shooting research sets out to accomplish, it must be mentioned how mass shootings compare in context to other violent crimes. The first issue to understand is the relatively rare nature of mass shootings in the overall crime and specifically violent crime context. In the most recent fully published Federal Bureau of Investigation's Uniform Crime Report (UCR) for 2016, a total of 9,167,220 crimes were reported to law enforcement in the United States. The majority of crimes are property crimes at 86.4%, contrarily violent crimes make up just a fraction at 13.6% of all crime reported (Crime in the U.S., 2016). The total number of violent crimes reported totaled 1,248,285; aggravated assault amounts to the majority of violent crimes at 64.3% (803,007). Homicide comparatively, comprises the smallest amount at 1.4% (approximately 17,250 crimes) of violent crimes and less than.0019% of all crimes for 2016 (Crime in the U.S., 2016)¹⁴. The 2016 UCR goes on to state that the long-term statistics demonstrate that the murder rate has been on an overall decline from 1997 to 2014¹⁵, although from 2015 to 2016 the rate appears to have started on a slight upward trend (Crime in the U.S. 2016). This upward trend is upheld in the preliminary 2017 UCR statistics, as murder has risen approximately 1.5% since 2016 continuing the upward trend in murder percentage, but violent crime surprisingly has dropped.8% from 2016 (*Preliminary Semiannual Uniform Crime Report, January–June, 2017*).

The recent upward movement in murder statistics must not be confused with the long-term trends which paint a different crime picture. Examining the long-term statistics from the 2016 UCR report indicate that murder and especially violent crimes themselves are at a significantly lower rate from 20-year and even 10-year averages. The 20-year violent crime average from 1997–2016 is down

¹⁴ Data is based on reported crimes to law enforcement agencies in 2016. The data does not include arrest or clearance rates of each crime. More data can be found at the 2016 FBI About Crime in the U.S. (CIUS) <https://ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/cius-2016>

¹⁵ Violent crime in the United States peaked in the mid-1990's.

36.8% along with the overall murder rate which is down 22.1% in the same time period. Looking into the shorter term 10-year statistics from 2007–2016, violent crime has decreased 12.3% with murder rates down 6.0% as well¹⁶.

What does the crime report mean?

These statistics are included in this article to disprove that the common myth that murders and mass murders are an everyday part of the United States culture. As much as media pushes the notion that crime is on the rise, the long-term statistics demonstrate a significant decrease in the last 20 years in violent crime rates. In a Congressional Research Service Report, Nathan James argues that the fluctuation of crime in recent years could be due to a newly surfaced phenomenon called the Ferguson effect. ‘This theory suggests that in the wake of recent high-profile officer-involved deaths, the police have become reluctant to engage in proactive policing, thereby emboldening criminals’ (James, 2015, p. 11). In this explanation for the increase, law enforcement is more cautious in the way they handle each situation for fear of accusations of racial profiling or targeting. Thus, creating a distrust between the community and the police causing tensions to boil over resulting in an increase in violent crimes. This theory could explain why the violent crime rates are swaying at the moment¹⁷. But, no matter what the reason for the slight rise in crime, the primary takeaway from the UCR should reflect that the violent crime rate in 2014 is at the lowest rate in since 1970 and the homicide rate is at the lowest since 1960 (James, 2015, p. 6).

Mass Shooting terminology difficulty

One interesting issue concerning mass shootings is how the terminology has developed. During this research, multiple different definitions have been found that will cause drastic differences in the results of each study. The definition controversy partially stems from the FBI in the 1980’s determining a classification system to “aid law enforcement in investigation though criminal profiling and not statistical data collection purposes” (Ressler et al., as cited by Krouse &

¹⁶ The Data is compiled from the FBI *Crime in the U.S. 2016* data UCR Report. Crime related statistics are in the context of per 100,000 inhabitants.

¹⁷ The application of the Ferguson theory is still being studied as multiple plausible explanations exist for the increase in violent crimes/murders in the last 2–3 years.

Richardson, 2015, p. 11)¹⁸. Primarily, the distinction from the FBI was needed to differentiate long period serial killers from one-time event murderers (Morton et al., 2008, p. 17). The FBI later clarified a mass murder in a 2008 Report as,

‘Generally, mass murder was described as a number of murders (four or more) occurring during the same incident, with no distinctive time period between the murders. These events typically involved a single location, where the killer murdered a number of victims in an ongoing incident’ (Morton et al., 2008, p. 17)¹⁹.

The FBI Definition of a Mass Murder is a starting point for all following mass shooter related terminology that are popularized in the media today (e.g. School shooter, Mall shooter, Rampage Shooter, Lone wolf etc.)²⁰. Each one of these buzzword terms has been popularized in media reporting to attempt to categorize a rare event (i.e. mass shooting) for the public understanding. The term active shooter, on the other hand, was introduced by the Department of Homeland Security (DHS) in 2008 as part of a response guide to inform the public on how to respond to a mass shooting²¹. An active shooter situation is what the event is called during the action itself primarily for police response, opposed to a mass shooting which is the term used after the incident has taken place (Schildkraut & Elsass, 2016, p. 18). The distinction would be nominal, but as a mass shooting event is taking place the multitude of definitions is enough to overwhelm the public while the media is waiting for more information to report on as a situation evolves.

The definition issue does not stop at the media or law enforcement agencies, researchers themselves have difficulty finding a consensus on the best way to define a mass shooting although recent studies have started to become more consistent. The biggest issue throughout the research is the distinction between

¹⁸ To see more about the history of the changing definitions of mass murder see Chapter 2 of Schildkraut, J, & Elsass, J (2016) *Mass Shootings: Media, Myths, and Realities* and the Congressional Research Service Report from Krouse, J. William & Daniel, J. Richardson. (2015) *Mass Murder with Firearms: Incidents and Victims, 1999–2013*.

¹⁹ Some examples for a Mass Murder using the 2008 FBI definition include the 1984 San Ysidro McDonalds incident in San Diego, California; the 1991 Luby’s Restaurant massacre in Killeen, Texas; and the 2007 Virginia Tech murders in Blacksburg, Virginia as given in the FBI Report by Morton, Robert ed. et al. (2008) *Serial Murder: Multi-Disciplinary Perspective for Investigators*.

²⁰ The terminology as it relates to this paper: Crime → Property + Violent → Homicide Murder → Mass killing/ Mass Murder → Mass shooting → other terms such as active shooting, school shooting, mall shooting, lone wolf shooting, etc.

²¹ Department of Homeland Security, Active shooter: How to respond. 2008 pdf

dead, injured, and potential targets²². As the FBI definition states “four or more” must be dead in order for it to be considered a mass murder. When applying this base definition to a mass shooting it does not consider injured or all other potential targets present at the time of the attack. The injured persons and other victims present at the attack could have easily been casualties but due to rapid response by first responders, active-shooter training, intervention of some kind, or just pure luck the total number of murdered decreased²³. An example of an intervention occurring is shooting at 888 Bestgate Road in Annapolis, Maryland on June 28th, 2018. As reported by CNN, CNBC, NBC, and WTOP after the shooting was first called into 911 the first police officers were on scene in less than 60 seconds. Since the response was so quick, as Governor Larry Hogan stated in a WTOP interview “I think that the law enforcement that responded on the scene deserve a lot of credit... They got there within 60 seconds. They prevented further deaths” (Moore, 2018). Hypothetically, if a law enforcement officer just happened to be in the building at the time of the first shot, the death toll potentially could be zero²⁴. And thus, this could have been an “attempted” mass shooting and not counted in mass shooting statistics even though the shooter had the motive to kill as many as possible, the ammunition, and with “170 people (in) the building” with the case of the Annapolis shooting (Silverman, DiGiacomo and Simon, 2018). But since this is just theory, the top-notch response by law enforcement personnel was the mitigating factor in reducing the death toll, as the quick response was able to catch the offender off guard.

The death toll criterion is not the only definition difficulty, multiple other areas need to be addressed, such as the location (e.g. indoor, outdoor, confined

²² Consistent with a research article from Jason R. Silva & Joel A. Capellan (2018) titled the media’s coverage of mass public shootings in America: fifty years of newsworthiness. On page 7–8 the methodology defined the issue of including “A death-toll criterion ignores random and systemic factors...that may impact whether or not a perpetrator seeking to become a mass public shooter actually becomes one” as cross referenced from the 2016 Schildkraut & Elsass Book.

²³ An example of an intervention would be of ten cases in Eugene Volokh’s Washington Post article from 2015 titled Do citizens (not police officers) with guns ever stop mass shootings? In the article 9 out of 10 cases (one case meets the definition of a mass shooting of four or more killed) of potential death in each mass shooting were reduced or averted altogether due to intervention with a firearm. Note: The article was looking at the issue of if cases existed of citizens stopping a mass shooting with a firearm. Not all the 10 cases would have fully met the definition of a mass shooting as is, but had the ability to evolve into one given the opportunity.

²⁴ Another example of an issue with the four or more dead criterion is the situation of a shooter shooting down a hallway with 20 people in it. If the shooter misses every person, that would not be a part of the total casualties or noted in statistics even though they had the potential to kill 20, people but did not injure a single person.

space, physical address) which can change during a single mass shooting without qualifying it as a longer-term mass casualty event. There has been a consensus to include some sort of broader “public platform in a 24-hour time period” in the definition to help broaden the scope without adding too much ambiguity. Another issue is a mass shooting must not correlate with terrorism, gang-related activity, or organized crime. This distinction starts to get into the issue of the true motive behind the attack. Including those criminal activities inflates statistics with unrelated criminal activity. This issue was partly analyzed in a study done by Schildkraut and Elsass in 2016, out of 312 identified mass shootings, 46.8% of the shooter(s) were killed leaving 53.2% alive after their rampage. With a little less than half of all shooters dead after the rampage combined with the surviving shooters not always cooperating with the investigation, the nature behind each shooting may be speculated upon but the true reason why every shooting occurred will never be fully understood. Thus, the ideologically driven reason behind each mass shooting is difficult to differentiate and quantify between specific cases.

How do Mass Shootings fit in the public discussion?

Mass Shootings in the United States have become a hot selling, attention grabber of modern media culture and a very hotly debated topic with proponents of possible solutions in many different areas²⁵. No matter the reasoning or solution, researchers must push past personal biases to produce the most reliable and trustworthy data to inform the public conversation. As it is becoming difficult to consistently put the data researched into the correct context for discussion²⁶, the purpose of this section is to inform on the research findings, definitions, data sets, and potential biases of the examined studies/databases.

Mass Shooting Tracker

Mass murder statistics fluctuate on the definition and bias of the author of the study or database as previously described. A prime example of this fluctuation

²⁵ E.g. education, gun control, preventive measures, mental health, debates on the application of amendments in modern times.

²⁶ Examples of incorrect usage of data or research include misuse of statistics to defend one’s own political opinion or using one statistic in a media article with no background and information of the study. To learn how to use statistics properly see the resources at the end of the article.

is seen with a cursory search of the internet using the search parameters “mass shooting data” the website of Mass Shooting Tracker (MST) appears in the top results. This website states before the data, reasons, or potential causes of mass shootings that it has been “featured (on) CNN, MSNBC, The New York Times, The Washington Post, The Economist and more” (Mass Shooting Tracker: About the Mass Shooting Tracker, 2013). The MST then states that it uses data from a volunteer group based in the forum centered website Reddit. To start the analysis, the Mass Shooting Tracker defines a mass shooting as,

“We define a mass shooting to be an incident of gun violence in which 4 or more people are shot in a single shooting spree. This may include the Gunman himself, or police shootings of civilians around the gunman. We do not consider the motive of the shooter.. We include the shooters death” (MST, 2013).

This definition is problematic as is pointed out in the 2016 book from Schildkraut and Elsass titled *Mass Shootings: Media, Myths, and Realities*, which states taking a relatively rare event i.e. mass shooting and combining said event with a vague definition, varied statistics will ensue that cause drastic differences as to the actual rates of mass shootings. This issue is seen in the Mass Shooting Tracker’s database as the definition used states it does not differentiate between motive. Without the motive differential, it includes all gang-related, organized crime, and terrorism influenced or related attacks. These other criminal acts are important to study, but they have no influence on mass shootings as they are ideologically different and must be treated as such²⁷.

Since this data is compiled from nonspecific volunteers from Reddit, the bias of the reporting must be taken into consideration which is noted in the ‘About the Mass Shooting Tracker’ section. It states that the “primary purpose of the database is to include all deaths and injuries of mass shooting events that would otherwise go unnoticed” (MST, 2013). The study has further, anti-gun leanings as further on they mention “punching a hole in the NRA argument that if mass shootings are televised, more mass shootings will occur via copycats” (MST, 2013). Since the MST openly admits that it opposes all gun related deaths, reasonably one would assume that since the definition is so broad the statistics would be higher compared to other studies.

²⁷ Grouping all of these criminal activities together is important for overall crime rates to see long/short term trends. But it is counterproductive to group all crime together and search for a solution without understanding why each type of crime occurs.

Now to the actual statistics, from 2013 to the date that the website was accessed for this research article on July 6th, 2018, the MST database has cataloged 2,153 cases of mass murder in the United States totaling 2,770 murders and 8,322 injured. The number of cases, murdered, and injured people in the database are visibly high compared to other studies on mass shootings, which will be compared later in the article. The database includes the shooter's deaths in the murdered statistics which artificially inflate the rate. Although the website does not state if the shooter's injuries are included in the statistics, logically the shooter's injuries would be included in the statistics due to the tone of the website as an anti-gun awareness platform thus increasing the numbers further. The MST, however, does state in the definition that it includes police shootings of civilians around in response to the shootings, but it does not state if the police deaths/injuries related to the shooting are included. With all these unknown extra factors that are thrown in to boost the overall numbers, the boasting of multiple media sources using the website, and the ominous nature of the publishers, the ability to claim a reputable non-bias study that informs the public on mass shootings diminishes with examination.

The Media's disproportionate coverage of Mass Shootings

Studies on Mass Shootings have started to investigate the media coverage of these events to try to inform the public on the skewed media coverage. Since studies have a difficult time conforming to a single definition and as these events still occur the total number of mass shootings will vary with each study. One of the most recent studies, *Mass Shootings: Media, Myths, and Realities* by Schildkraut and Elsass in 2016, studied the relationships between identified mass shootings, common stereotypes, media coverage associated with the stereotypes and the changing nature of the field of study associated with mass shootings. In the book, a considerable amount of research was dedicated to showing how the definition of mass shooting events have evolved and continue to change²⁸. In the book after much contemplation, the definition of a mass shooting is as follows,

“[a]n incident of targeted violence carried out by one or more shooters at one or more public or populated location(s). Multiple victims (both injuries and fatalities are included) are associated with the attack, and

²⁸ For more of the history of the definition see Chapter 2 in *Media, Myths, and Realities* by Schildkraut and Elsass (2016).

both the victims and location(s) are chosen either at random or for their symbolic value. The event occurs within a single 24-hour period, though most attacks typically last only a few minutes. The motivation of the shooting much not correlate with gang violence or targeted militant or terroristic activity.” (Schildkraut & Elsass, 2016).

Using this definition, the first mass shooting in the study occurred in 1880 with 306 mass shooting events identified as of 2014²⁹. Some of the stereotypes that were brought up involved the standard of “young white males brandishing assault rifles who commit suicide after their attacks” (Petee et al., 1997, as cited by Schildkraut & Elsass, 2016). The study used the research data to disprove, among other things, the exclusivity of these claims in attempt to demonstrate the bias of the media coverage. In the research, the main goal was not only to disprove each one of the three “standards” but to caution the media and public in both describing a mass shooting as an “outlier” or a so called “usual” case. Both terms cause confusion of the actual mass shootings rates when rapidly interchanged during the public reporting and conversation encompassing mass shootings.

In each case of gun violence, the initial reaction is to either group it into a “textbook incident” which would receive less attention by the general public/media or describe it as an outlier attack which will receive increased public attention. In a 2017 a follow up study by Schildkraut, Elsass, and Meredith the hypothesis examined was to determine which incidents received the most coverage within articles in the New York Times. According to Chermak (1995) as cited by Schildkraut, Elsass, and Meredith (2017),

“newsworthiness may be assessed based on five criteria – the violent nature of the crime, demographic nature of the victim and offender (such as age, gender, race, and occupation), characteristics of the news agency, the uniqueness of the event, and the event’s saliency” (p. 4).

These characteristics defined by Chermak are evident in the research results that identified from 90 mass shootings from 2000–2012 using the 2016 Mass Shooting: Media, Myths and Realities definition³⁰. The study collected only

²⁹ To see all of the findings of the study, see Chapter 4 in Mass Shootings: Media, Myths, and Realities by Schildkraut and Elsass (2016).

³⁰ Only 90 mass shooting are identified in this study, due to only analyzing the New York Times database with strict qualifiers. And to determine how high-profile mass shootings, specifically The Columbine High School Shooting, had affects on media coverage. More on Pg. 10 of Schildkraut, Elsass, and Meredith 2017.

stories and editorials for a lifespan of 30 days after each of the 90 incidents (Schildkraut, Elsass, and Meredith, 2017, p. 10). One of the most interesting findings states that the 10 most important cases “account for 70% of the total number of articles printed (in the study), as well as 75% of the total number of words written” (Schildkraut, Elsass, and Meredith, 2017, p. 11). The cases with the top coverage included the Sandy Hook Elementary School Shooting (2012) and the attempted assassination of Gabrielle Giffords (2011) with 130 and 89 articles respectively (Schildkraut, Elsass, and Meredith 2017: p. 12). In the study, the goal was to determine which of the most important factors would include or exclude extensive media coverage of a mass shooting³¹. The research results can be seen below.

Coverage of mass shooting incidents by perpetrator and event characteristics

Actual incidents		
	N	Percent off incidents
Shooter gender		
Male *	85	94,4
Female	5	5,6
Shooter age		
17 and younger	9	10
18–24	19	21,1
25–35	16	17,8
36–50	32	35,6
51 and older	14	15,6
Shooter race / ethnicity		
White *	52	57,8
Black	18	20
Hispanic	10	11,1
Asian	5	5,6
Other	5	5,6

³¹ The sample population of the study was small with only 90 events included in the study from the time period 2000–2012. This study excluded the 1999 Columbine School shooting, in the attempt to show how the public perception and news coverage of these events has changed (Schildkraut, Elsass, and Meredith 2017: p. 7).

The Media's disproportionate coverage of Mass Shootings

Shooter dead		
Yes	50	55,6
No *	40	44,4
Total victims **		
2-5	33	36,7
6-9	33	36,7
10 or more	24	26,7
Median income		
Less than \$55,000	10	11,1
\$55,000-\$59,999	13	14,4
\$60,000-\$64,999	17	18,9
\$65,000-\$69,999	16	17,8
\$70,000-\$74,999	16	17,8
\$75,000 and greater	18	20
Location(region)		
Northeast	11	12,2
South *	25	27,8
West	27	30
Midwest	27	30
Location		
School *	26	28,9
Workplace	21	23,3
Restaurant/club/bar	8	8,9
Mall	7	7,8
House	5	5,6
Other	23	25,6

Note: Variable frequency percentages for actual incidents by category may not total to 100% due to rounding error.

* Reference category

** Total victims represents the aggregate of the number of people killed and wounded in the shooting.

(Schildkraut, Elsass, and Meredith, 2017, p. 9)

In 2018, a study from Silva and Capellan expanded on the conclusions of Schildkraut, Elsass, and Meredith in 2017. The study specifically looked at which casualties, locations, and ethnic factors would increase the predictors of coverage by the media. Using a 50-year time period from 1966–2016, 314 mass shootings³² were identified. Out of all cases, the most used firearm with 54.7% of mass shootings is the handgun alone, the shooter had some sort of relationship with the victims 61% of the time, and the most common location is a business with 36.4% followed by schools at 26.7% (Silva & Capellan, 2018, p. 10). These findings are consistent with other research studies, especially the firearm used and the location of the shooting³³. Disclosure: the study does include non-state sponsored ideologically driven shootings such as the Orlando, Florida Night Club Shooting and the San Bernardino, California Shooting³⁴.

The 1999 Columbine High School Shooting was the most covered event with 503 articles and 503,269 words. Columbine had double the articles and total words of the second most covered event, the 2012 Sandy Hook Elementary School Shooting that had 248 articles and 253,036 total words (Silva & Capellan, 2018, p. 11). These two shootings are synonymous with mass shootings due to the unexpected factor in both of them specifically the elaborate, movie-like, nature of the Columbine Shooting and the preparation that Sandy Hook took to prevent a mass shooting event from happening. Both of these events garnered immense media fueled attention and public outrage which helped shape new media procedures and laws in an attempt to prevent more mass shootings.

The media coverage of mass shootings is not only skewed to the top two stories in the study, as the top 15 news generating mass public shootings received 68% of the total articles written and 71% of total words written of the entire 314 cases identified (Silva & Capellan, 2018, p. 11). As Silva and Capellan put it “Less than one-half of a percent of these incidents drive the information and consequently our understanding of these incidents” (p. 11). With such a small percentage of incidents talked about consistently on a public platform, the

³² A mass public shooting is defined in this study as “An incident of targeted violence where an offender has killed or attempted to kill four or more victims on a public stage. In line with current research...three more elements were added to this definition: (1) it could involve more than one offender at multiple related locations within a 24-hour time period; (2) the main weapon had to be a firearm; and (3) the shooting was not related to state-sponsored or profit driven criminal activity” (Silva & Capellan 2018: p. 7).

³³ Consistent with (not 100% conclusive) 2016 Schildkraut & Elsass, 2017 Schildkraut & Elsass & Kimberly, 2018 Silva & Capellan, and the 2014 Blair & Schweit studies on mass shootings.

³⁴ More on why these cases are included can be found on p. 7–8 of Silva & Capellan, *The media’s coverage of mass public shootings in America: fifty years of newsworthiness*.

overall picture and context of these events gets lost. To effectively report on mass shootings in the media, each event must not be thought of as an outlier and reported on as a freak incident (e.g. Columbine and Sandy Hook) that “no one saw coming” or grouped in to the “average incident” and only used in statistics to boost the findings of each report³⁵. The top 15 news producing mass shootings are below with the 1966 Texas Tower shooting surprisingly making number 15³⁶.

Fifteen most news producing mass public shootings

Incident	Year	Total articles	Specific articles	General articles	Total words	Specific words	General words
Columbine High School Shooting	1999	503	127	376	503,269	113,612	389,657
Sandy Hook Elementary School Shooting	2012	248	45	203	253,036	44,985	208,051
Colorado Theater Shooting	2012	212	78	134	210,877	61,391	149,486
Tucson Shooting	2011	207	96	111	209,060	92,696	116,364
San Bernardino Shooting	2015	206	16	190	240,723	22,323	218,400
Virginia Tech Shooting	2007	198	83	115	208,595	62,890	130,069
Orlando Night Club Shooting	2016	175	41	134	192,959	50,681	157,914
Charleston Church Shooting	2015	161	50	111	208,336	52,883	150,453
Fort Hood Shooting	2009	159	73	86	162,288	53,418	108,870

³⁵ In the 2018 Silvia & Capellan study found that 28% of cases did not receive national coverage and 50% of cases received less than 4 stories (p. 11). In the 2017 Schildkraut & and Elsass found similar results, 23% of cases did not receive coverage and two cases with victim counts over 10 did not receive media coverage at all.

³⁶ The Texas Tower Shooting is widely regarded as the first wave of increased media attention on mass shooting. Just like The Columbine High School Shooting in 1999 and the Sandy Hook School Shooting in 2012.

Incident	Year	Total articles	Specific articles	General articles	Total words	Specific words	General words
Long Island Rail Road Shooting	1993	106	87	19	98,957	69,380	29,577
Westside Middle School Shooting	1998	77	21	56	83,363	25,566	57,797
CIA Headquarter Shooting	1993	46	20	26	41,576	12,893	28,683
Brooklyn Bridge Shooting	1994	40	33	7	31,741	26,309	5,432
Washington Navy Yard Shooting	2013	35	13	22	41,789	14,842	26,947
Texas Tower Shooting	1966	32	9	23	41,364	83,00	33,064

(Silva & Capellan, 2018, p. 11)

The coverage of mass shootings fluctuates depending on other factors. For example, more than 90 percent of mass shootings were covered if the shooter is Middle Eastern, ideologically motivated, involved a religious location, or had four or more killed in the attack (Silva & Capellan, 2018, p. 12). More than 80 percent of stories are covered if the shooter's age is 20 or less, the shooting is carried out against strangers, the shooter used a combination of weapons, is located in a school or open space, injured victims are more than four, or the attack occurred in the northeast (Silva & Capellan, 2018, p. 12).

In the next two charts, the first demonstrates the percent of incidents based on basic variables of mass shootings and the next chart demonstrates the media coverage of each variable in the parameters of articles and words written. All of the variables that have high coverage rates are hot sellers in news stories. They are very easy to publish as headline articles that have a catchy title in an attempt to draw from a larger pool of consumers.

The dangerous part of putting mass shootings or any news in a quick 10-word summary is the overall context and purpose gets traded for views. This is seen particularly with the variable of a Middle Eastern Shooter among others. If a Middle Eastern Shooter was a variable, 90% of cases were covered even though they only make up 3.4% of all mass shooting cases (Silva & Capellan, 2018, p. 10,12). Not only did Middle Eastern shooters have a high coverage percentage, but the mean total number of articles and words written about each average case was more than double any other variable (Silva & Capellan, 2018, p. 12).

Suggesting that if a Mass Shooting case involves a Middle Eastern shooter the case will receive disproportionate media stories. This can be seen with such shootings as the Orlando, Florida Night Club Shooting in 2016 and the San Bernardino, California Shooting in 2012.

Basic characteristics of mass public shootings, 1966–2016

	N	Percent off incidents
Male	307	96,5%
Age	318	35 (Avg.)
Race		
White*	193	60,6%
Black	67	21,0%
Latino	25	7,8%
Asian	12	3,7%
Middle Eastern	11	3,4%
Confirmed/suggested mental illness	138	43,7%
Relationship		
Strangers	124	38,9%
Relationship with victims	194	61,0%
Ideologically motivated	43	13,5%
Type of weapon(s)		
Handgun	174	54,7%
Shotgun	26	8,1%
Rifle	37	11,6%
Combination	72	22,6%
Location		
Business	116	36,4%
Government	41	12,8%
School	85	26,7%
Religious institution	12	3,7%
Open space	38	7,8%
Conclusion		
Arrested	145	45,9%
Killed	53	16,6%
Suicide	119	37,4%

	N	Percent off incidents
Death toll	318	3.3 (Avg.)
Injured victims	318	4,2 (Avg.)
Location(region)		
Northeast	56	17,6%
South*	35	11,0%
West	129	40,5%
Midwest	98	30,8%

(Silva & Capellan, 2018, p. 10)

Understandings of mass shootings are shaped by the media coverage and research data that is the backbone of public and political discussion. One of the biggest problems is the ability to place mass shootings into the proper context of the overall crime spectrum. Crime news is often cut up and used against the publishing bodies' desire to push pre-decided political or personal agendas. Mass shooting studies have felt pressure to have a consistent research base as they have started to similarly define a mass shooting. This consistent research base is still a work in progress as divergent thoughts of what to include in the mass shooting definition as well as the plethora of other mass shooting related terminology causes confusion in the public debate. The research results comprised by research studies and federal agencies were included in this paper to show the difference/similarities between researchers, data sets, and common stereotypes associated with mass shootings.

In the end, precautions must be taken to prevent mass shootings, but these precautions must not drastically alter everyday life since these shootings are so rare to begin with. The ability to be vigilant of common place interactions to look for abnormalities cannot be understated for a plethora of reasons including mass shootings. Media coverage of mass shootings must also be consumed with a grain of salt in general, but especially when details are vague or emerging. It is the media's responsibility to report the events to the public, but they may accidentally (or purposefully) sensationalize the coverage. But that should not discourage coverage of mass shootings or possible solutions since as new coverage campaigns such as "names no names" emerge to call ethical journalism principles in to question.

Media coverage by characteristics of mass public shootings

	Percent covered	Mean no. Articles	Mean no. Specific articles	Mean no. General articles	Mean no. Words	Mean no. Specific Words	Mean no. General words
Female	63.3	4.5	2.6	1.9	3613.8	2131.4	1482.4
Male	73.2	11.3	5	6.3	11,464.9	4179.9	7284.9
Age							
20 or less	81.8	16.2	5.6	10.6	16,128.5	4168.8	11,509.6
21-40	75.1	15	6.6	8.3	15,831.5	5,805.8	10,025.9
41-59	66.6	3.63	2.48	1.14	3,276.8	1,934.3	1342.5
over 60	57.8	3.4	2.4	1	2380.2	1524.3	855.8
Race							
White	74.3	11.4	4.9	6.5	11,408.5	4116.8	7291.6
Black	73.1	4.8	3.4	1.3	4638.1	2837.7	1800.4
Latino	60	1.9	1.1	0.7	1809.9	854.0	955.9
Asian	75	19.5	9.5	10	19,105.0	7139.9	11,965.1
Middle Eastern	90	70.3	21.9	48.4	75,834.2	20,070.4	55,763.8
No known mental illness	72.8	5.5	2.8	2.8	5716.1	2282.5	3433.5
Mental illness	72.4	18.4	7.8	10.5	18,376.2	6496.5	11,879.6
Stranger	81.1	15.5	7.2	8.3	15,866.4	6324.2	9542.1
Relationship with victims	67.5	8.4	3.5	4.8	8300	2721.3	5578.7
Non-ideologically motivated	70.2	7.9	3.5	4.3	7680.9	2777.3	4903.5

	Percent covered	Mean no. Articles	Mean no. Specific articles	Mean no. General articles	Mean no. Words	Mean no. Specific Words	Mean no. General words
Ideologically-motivated	90.5	34.5	14.8	19.7	36,850.1	13,676.3	18,482.0
<i>Type of weapon(s)</i>							
Handgun	68.9	9.3	4.6	4.6	9197.7	3792.0	5405.7
Shotgun	57.6	2.6	1.6	1	2558.8	1267.1	1291.6
Rifle	72.9	7.1	3.8	3.3	7042.3	2982	4060.4
Combination	89.8	22.3	7.8	14.4	23,088.1	6967.4	16,120.7
<i>Location</i>							
Business	61.7	5.6	2.7	2.8	5481.3	2172.4	3308.8
Government	75.7	16	6.1	9.9	16,594.5	5088.2	11,506.3
School	80	16.1	5.9	10.2	15,795	4713.7	11,081.2
Religious institutions	91.6	20.7	8.08	12.6	24,156.2	7836.8	16,319.4
Open Space	84.2	13.8	8.6	5.2	13,861.8	7581.3	6280.5
<i>Conclusion</i>							
Arrested	69.8	10.5	5.5	4.6	9911.4	4284.7	5626.6
Killed	76.9	12	3.8	8.1	13,740.3	3819.7	9920.57
Suicide	74.7	12.1	4.8	7.2	11,774.9	4052.4	7722.4
<i>Death toll</i>							
3 or less	61.9	3.2	2.2	1	2909.2	1573.4	1335.7
Over 4	95.2	27.3	10.5	16.8	28,319.5	9346.5	18,972.9

<i>Injured victims</i>							
3 or less	65.6	4.6	2.3	2.2	4484.4	1842.4	2642.3
Over 4	84.9	22.8	9.5	13.3	23,256.08	8,174.6	15,081.4
<i>Region</i>							
Midwest	76.7	3.2	2.5	0.76	2664.7	1649.7	1015
Northwest	88.5	16	8.4	7.6	14,885.2	6995.0	7890.2
South	70.5	10.8	4.8	5.9	10,795.7	3979.7	6815.9
West	67.3	15.2	5.4	9.7	15,550	4709.7	10,840.2

(Silva & Capellan, 2018, p. 12)

Final Thoughts

Understandings of mass shootings are shaped by the media coverage and research data that is the backbone of public and political discussion. One of the biggest problems is the ability to place mass shootings into the proper context of the overall crime spectrum. Crime news is often cut up and used against the publishing bodies' desire to push pre-decided political or personal agendas. Mass shooting studies have felt pressure to have a consistent research base as they have started to similarly define a mass shooting. This consistent research base is still a work in progress as divergent thoughts of what to include in the mass shooting definition as well as the plethora of other mass shooting related terminology causes confusion in the public debate. The research results comprised by research studies and federal agencies were included in this paper to show the difference/similarities between researchers, data sets, and common stereotypes associated with mass shootings.

In the end, precautions must be taken to prevent mass shootings, but these precautions must not drastically alter everyday life since these shootings are so rare to begin with. The ability to be vigilant of common place interactions to look for abnormalities cannot be understated for a plethora of reasons including mass shootings. Media coverage of mass shootings must also be consumed with a grain of salt in general, but especially when details are vague or emerging. It is the media's responsibility to report the events to the public, but they may accidentally (or purposefully) sensationalize the coverage. But that should not discourage coverage of mass shootings or possible solutions since as new coverage campaigns such as "names no names" emerge to call ethical journalism principles in to question.

End Notes

This article was created to demonstrate the differences between mass shooting studies and is not exclusive as only the reports that pertained to the research topic were included. Not every study was referenced. The recent high-profile Las Vegas Mandalay Bay Mass Shooting is only included in the Mass Shooting Trackers Database results as no empirical research is published as of the writing of this article.

The terminology from largest to smallest as it relates to this paper: Crime → Property + Violent → Homicide → Murder Mass killing → Mass Murder → Mass

shooting → other terms such as active shooting, school shooting, mall shooting, lone wolf shooting, etc.

United States crime data can be found in the FBI UCR report published annually. This report is the most accurate source for all modern trends in crime. <https://ucr.fbi.gov/>

To learn more about how to ethically read statistics one may visit the 2018 report prepared by the Committee on Professional Ethics of the American Statistical Association. <http://www.amstat.org/ASA/Your-Career/Ethical-Guidelines-for-Statistical-Practice.aspx>

Chapter 8

Defend and Collaborate: Information Security Considerations for Every Business Organization

Jacob M. Schmitt

Abstract

This research publication investigates multiple aspects of information and cyber security as it relates to all sizes of business enterprises. Because everyone utilizes technology that connects to the internet, all businesses are exposed to cyber security risks. This paper reviews basic principles of cyber security management for business leaders by investigating the human user security challenges in IT systems, new techniques of active defense and the nuances of cyber security insurance policies. The publication continues by highlighting ways that governments, businesses, and industry associations can and do cooperate with much success. The importance of obtaining industry certifications for more efficient coordination of responses to cyber intrusions are also discussed. The author emphasizes the need to focus on the human security aspect of access control because it is, universally, the primary weakness of any businesses' IT infrastructure even after utilizing other standard defenses like modern IT infrastructure and cyber security insurance to protect against catastrophic losses.

Introduction

Businesses of every size handle sensitive information such as transaction receipts, customer data and sensitive information pertaining to their business's decisions. Almost every business also utilizes technology that increases their efficiency

which also exposes them to increasingly extensive and pervasive risks. A 2017 report estimated global damages from cybercrime at \$600 billion or nearly 1% of global gross domestic product (Economic Impact of Cyber Crime, 2018, p. 3). A joint report between Cybersecurity Ventures and the Herjavec Group projected an increase to \$6 trillion in annual economic losses by 2021 (Morgan, 2017, p. 3). If a company's leadership fails to manage these risks properly, they face catastrophic losses to sales, reputation and assets. Powerful tools that were once wielded solely by sophisticated government actors are now relatively easily available on the internet as a standalone software program or as a service by talented criminals, often for a small fee. As governments grapple with regulating rapidly changing technology, businesses must take the initiative to protect themselves, cooperate with others in government and their industries, and work closely with their information technology (IT) service providers. Even if a small business does not sell goods or services outside their home country, connecting to the internet in any manner exposes them to malign actors who often operate in spaces of weak governance that can evade even the strongest domestic laws and regulations. The challenges of bringing justice to these offenders and receiving settlement for damages without international cooperation cannot be overstated. This publication will highlight cyber security management principles that are applicable to any sized businesses, highlight opportunities for security collaboration between public and private entities while stressing the need to take the initiative in defending one's own business interests in this complex and rapidly changing threat environment. Having read this publication, the reader will have a better understanding of the complexities of managing cyber security in businesses and will learn industry best practices that apply to every organization.

Defending Business Information

The sophistication of Enterprise Risk Management and Security vary greatly between organizations. Large multi-national corporations often require a large team of professionals to manage legal compliance, travel security, physical security, executive protection and internal investigations. Sole proprietors and small businesses don't have the same needs or resources when it comes to cyber security, but they face the same threats. The actors who look to exploit weaknesses do not discriminate in their targets if they have a way to benefit from it. In 2016, several small police departments in the United States experienced a ransomware attack on their outdated computers. The departments were using older computers and had failed to receive critical security updates. Some departments refused to

pay the ransom while one department was attacked twice and paid both ransoms (Francescani, 2016, p. 1–2). If a computer connects to the internet, there is always a security risk; even for smaller organizations and local law enforcement.

The Human Factor

The weakest link in many IT systems tends to be the human end users who have legitimate access to a given network as part of their jobs. Recent cyber security research by the University of Maryland summarized, “Humans are often identified as the weakest link in cyber security, since any technical security solution is still prone to failures by human error” (Gratian, et al., 2017, p. 345). Many companies invest vast sums of money on network security infrastructure and the latest automated protective software services only to be undermined by weak passwords and compromised email files.

The University of Maryland research team advanced research in the human elements of cyber security by identifying cyber security behaviors based on demographic factors, personality traits, risk-taking preferences, and decision-making styles (Gratian et al., 2017, p. 345). Their research added to Egelman, Harbach and Peer’s Security Behavior Intentions Scale which investigated IT system user’s security awareness, password strengths, timeliness of security updates, and the physical security of their devices (Egelman, Harbach, Peer, 2017, p. 5257–5261). Gratian, et al. concluded that technical minded people, like engineers, had better security awareness and stronger passwords than their humanities student colleagues. Interestingly, the data showed that women, between the ages of 18 and 25 years old who are humanities students tended to have weaker passwords and were more susceptible to phishing attacks (Gratian et al., 2017, p. 351–352).

This type of research helps organizations focus their finite security budgets on the most vulnerable aspects of their security infrastructure. A small business that has limited funds to invest in security can focus on training employees in cyber security practices to minimize these risks in the most economical manner. Such research could invite criticism if the training response is perceived as discriminatory, so security managers should act with prudence. Another weakness of this study is that the sample population was relatively small and exclusively students and faculty at a university. Nonetheless, this type of research provides valuable lessons and insight on one of the biggest security challenges of business organizations. Businesses must also focus on safeguarding portable devices like tablets and cell phones that are used to access their networks remotely.

Following the United States' Federal Bureau of Investigation (FBI) guidelines for business travelers, companies should educate their employees on simple but effective security practices of not leaving their devices unattended, clearing internet browsers after use, avoiding use of non-company provided electronic devices for work, and not connecting storage devices to phones or laptops (Safety and Security, 2016). "The company should also utilize Virtual Private Networks (VPNs) to establish secure connections to the company's servers whenever their employees are out of the office. The next greatest threat to business infrastructure is through "social engineering" attacks where an outside entity attempts to access the network by compromising a legitimate system user (Goldschmidt, 2018, p. 1–3).

The technical details of designing and developing security infrastructure is beyond the scope of this publication but assume that a professional IT team manages the infrastructure and subscribes to the latest malware and malicious software detection services. With such robust security, malign actors target legitimate employees who have regular access to a targeted IT system as a normal part of their employment. This type of threat seeks to circumvent individual security practices and exploit any gaps that are discovered. In the hacker's "approach", sensitive information is either manually obtained, "socially engineered" by manipulating a targeted person with legitimate access, or "reverse socially engineered" where a criminal gets an unaware person to come in to contact with them and then asks for a "favor" to lessen suspicions.

Criminals also use technical means of capturing a password and trying it in different websites or using "key logging" malware that transmits everything that is typed on a keyboard (Krombholz, et al., 2014, p. 114–116). All users should be aware of a usual form of attack called "phishing" where malicious attachments are sent to unsuspecting users who subsequently open these detrimental email attachments. This attack begins by gathering information on the victim by analyzing the victim's social media accounts and searching public records. In a classic example of a phishing compromise, the attacker finds an important friend or family member on Facebook and then sends a fake email from that person to trick someone into opening an infected file. Skilled attackers have learned what types of emails have the best success rate and repeatedly use that template in future attacks. These prosperous emails are constructed with an urgent call to action involving a request for help or disguised as an important business invoice. When the victim opens the malicious email attachment, it infects the target computer subsequently giving the hackers access to the network. The virus autonomously sends files back to the attacker or allows for remote access to the targeted system.

Again, cyber security awareness is essential in protecting businesses against these types of threats. In 2018, you cannot allow your employees to edit your companies' financial reports while chatting on Facebook from a hotel business center's computer, having logged in with the password "123456"! The attacks are obvious in hindsight, but it takes proactive training to help employees think about their actions on the company's IT system and recognize suspicious emails. Showing examples of other attacks and hacking methods helps to inoculate employees against this form of attack. After employing a capable and professionally managed IT infrastructure, strengthening employees against pervasive social engineering, some companies are taking an even more proactive approach to their information security management.

Active Defense

As cyber security attacks increase in number and sophistication, businesses are looking for ways to be more proactive in their responses. The idea of private entities "hacking back" to defend themselves raises numerous legal and ethical questions but principles of "active defense" have increased in popularity recently among IT infrastructure managers. The SANS Institute defines passive cyber security (PCD) as "systems added to the architecture to provide consistent protection against or insight into threats without constant human interaction" where an entity employs "firewalls, anti-malware systems, intrusion prevention systems, anti-virus, intrusion detection systems, and similar traditional security systems" that don't require constant IT system staff interaction (Lee, 2015, p. 8).

In contrast, Active Cyber Defense (ACD) is characterized by system responses that engage with the attacker once the traditional forms of cyber security have been breached. The SANS Institute explains this difference as "the process of analysts monitoring for, responding to, learning from, and applying their knowledge to threats internal to the network" (Lee, 2015, p. 10). Active defense calls for an analysis of the attack to understand the threat actor, attack vector, vehicle and malicious tools used to deliver the attack. An IT team using basic ACD principles will review the event, analyze system logs to disable accounts and update firewall criteria as each threat is identified (Overill, 2003, p. 163). A more dynamic ACD technique involves using a "honey trap" to draw a threat into an isolated "sandbox" where the threat can be observed and studied (Overill, 2003, p. 163).

The most aggressive and controversial forms of ACD call for "mount(ing) a Denial of Service (DoS) reprisal attack against the presumed source" or

“launch(ing) a retaliatory malicious software strike” (Overill, 2003, p. 164). The latter two types of responses are what most people think of when they hear the term “Active Defense” but business organizations are usually restrained by legal and moral operations against conducting such “hack backs”. In any type of response, business leaders must consider numerous aspects of their responses including “(their) authority, third party immunity, necessity, proportionality, human involvement, and civil liberties” similar to the military’s principles on the use of force (Denning, 2014, p. 111–112). Aggressive ACD could violate the Computer Fraud and Abuse Act (CFAA) of 1986 in the United States. The CFAA explicitly prohibits “knowingly cause(ing) the transmission of a program, information, code, or command... (that) intentionally causes damage and loss” (“18”, 1986, p. 1030).

Becoming frustrated with these restrictions, private businesses in the United States encouraged their government representatives to enact legislature due to the challenges of these rapidly changing threats. In October 2017, the Active Cyber Defense Act (ACDA) was brought to Congress for consideration. This recognized updated ACD principles and would allow businesses to “not only identify the attackers, but even destroy information originally stolen from their network” (Kulik, 2018, p. 1–2). The bill has not been passed at the time of this writing, but many scholars and legal experts are concerned at the precedent it would set. Some argue that it would weaken law enforcement’s ability to prosecute some entities for cyber intrusions citing dubious claims of self-defense. Other criticisms include the inability to precisely attribute an attack to one person or entity and varied skills among IT staff to carry out these aggressive counter-attacks skillfully without proper training (Kulik, 2018, p. 2).

Proponents of the bill say that the intent of the bill is to gather information to share with security researchers and law enforcement. Others argue these aggressive tools are necessary to counter emerging threats, especially when private organizations now face highly sophisticated attacks from foreign actors backed by nation-state level funding. This also begs the question: how does a business navigate the legal and moral complexities of defending against a foreign adversary that could be backed by another government? This is an ongoing challenge that has yet to be solved or even tested in international courts. To protect against these outsized risks, companies are now turning to sophisticated and specially designed insurance products as part of their comprehensive security policies.

Cybersecurity Insurance

While businesses continue to experience increasingly numerous and sophisticated cyber intrusions, Enterprise Risk Managers seek ways to reduce catastrophic economic losses from these events. Having employed talented IT personnel, invested in the latest secure infrastructure, and invested in training and awareness for their staff, business leaders still require additional safeguards to overcome crises. Insurance companies have responded by developing new insurance vehicles to transfer risk of cyber intrusions and data losses. The United States Department of Homeland Security (DHS) recognizes the benefits of these emerging products which are designed to “mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage” (Cybersecurity Insurance, 2016, p. 1). The DHS explains the benefits of Cybersecurity Insurance, “(1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured’s level of self-protection” (p. 2). When a business purchases Cyber Liability Insurance Coverage known as “CLIC”, they generally receive assistance with investigation of a malicious intrusion, compensation for business losses, privacy notification aid, and legal support against lawsuits and extortion (Lindros, Tittel, 2016, p. 2).

Research by Lloyds of London, one of the world’s largest insurance providers, indicate that “92% of businesses experienced a data breach in the last 5 years” but only “73% of business leaders have limited knowledge of cyber insurance” (Cyber Risk, 2016, p. 7) Insurance industry experts recommend that companies use insurance brokers to obtain these policies because they are complex and available coverage varies significantly between insurance providers and policies. Secondary benefits of obtaining CLIC insurance policies is that the underwriters require a comprehensive audit and risk assessment of the policies’ information security infrastructure and security protocols (Closing the Gap 2017, p. 32–35). Improvements are frequently required before a cyber security insurance policy is developed while companies benefit from these recommendations. The underwriters assess not only the current state of the system but also make predictions of future security needs while working with all stakeholders. These products should be considered when taking a holistic view of any companies’ information security plan.

These new policies are frequently criticized due to their costs but the DHS is optimistic that they will become more affordable as they develop and more entities start using them. Another concern of Cybersecurity Insurance

is that companies will forgo spending in other areas of their information security plan and narrowly rely on their expensive insurance policies should a cyber intrusion or data loss occur. After all, we are paying for this expensive protection, why not use it? The moral hazard of this mindset is another downside of cybersecurity insurance. Critics warn that companies will either cut security spending in other areas to pay for insurance or will rely too much on their policy and act carelessly with customer's data because they are covered either way. Callous attitudes towards information security could become more common as insurance policies become more affordable. Business leaders will always look to minimize costs, especially on their security, because it does not add value to their profits; security is often viewed as an inconvenient expense. Companies can better manage emerging risks with new insurance policies but need to ensure they practice due diligence in obtaining policies so that they receive this essential coverage.

Cyber Security Collaboration

To confront an already extensive and growing risk of cyber intrusions, business leaders will have to work with resources outside of their immediate organizations. Using government resources, networking with other organizations in their industries and utilizing experts in information security is vital to combatting these rapidly changing threats.

Public-Private Cooperation

Government organizations in Europe and the United States have been established to assist private enterprises in protecting their information systems and data. The European Cyber Security Organization (ECSO), enacted by the European Commission in July 2016, aspires to “foster cooperation between public and private actors at the (initial) stages of...(the) research and innovation process... (and) allow people in Europe to access innovative and trustworthy European solutions” (About the cPPP, 2018). Through this organization, the European Union is investing €450 billion euros in their “Horizon 2020” initiative to expand European produced security solutions. Large European companies like Ericsson, F-Secure Corporation, NXP Semiconductors B.V., and many others, recently established working groups with European Union/Commission representatives. These working groups are divided into areas of expertise that work on challenges

in training, standardization, certification, research, etc. Recent accomplishments of the ECSO include supporting European Commission legislation on the Cyber Security Act, Industrial Cybersecurity Policy and establishing several Cybersecurity Competence Centers throughout Europe (ECSO Public Session, 2018). In the United States, the Department of Homeland Security is the main governmental organization tasked with defending against cyber security threats and performing post-incident analysis for governmental and non-governmental entities (Information Sharing, 2018). In compliance with the Cybersecurity Act of 2015, the Department of Homeland Security administers the Automated Information Sharing (AIS) system that “enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed” (Automated Indicator Sharing, 2015, p. 1). Businesses can enroll in a program that automatically shares anonymized threat information with DHS while simultaneously receiving updates and information on emerging threats sourced through other businesses in the program. This system emphasizes speed and errs on the side of sending more information than less so that any potential threat can be reviewed (Automated Indicator Sharing, 2015, p. 2).

Another resource in the United States is the InfraGard public-private partnership between the Federal Bureau of Investigation (FBI) and “business executives, entrepreneurs, military and government officials, computer professionals, academia and state and local law enforcement; each dedicated to contributing industry specific insight and advancing national security” (InfraGard, 2003, p. 1). InfraGard gives focused assistance on critical infrastructure industries, maintains 82 chapters throughout the United States with regular information sharing events, publishes FBI news feeds, and boasts 400+ members from Fortune 500 companies (Partnership for Protection, 2003, p. 1). Considering the initial successes of European and American public-private collaborations, the model of closely coordinating government and private enterprise resources to combat cyber security threats should be expanded and encouraged by other countries.

External Resources

Sizeable government resources in intelligence and law enforcement are helpful to domestic enterprises but are limited by slow international coordination between governments and gaps in governance. Private enterprises are less constrained because they can react quickly and share information with international peers in their industry. Numerous innovations in the information technology space are created by private enterprises and organizations. International associations and

certifying organizations are great resources for businesses as well. Rapid sharing of information and standardized training allows IT professionals from different regions to work closer together using common language. One of the most recognized security certifications is the Certified Information Systems Security Professional (CISSP) issued by (ISC)² after demonstrating extensive knowledge and passing a threshold of work experience (Cybersecurity Certifications, 2018). The International Association of Privacy Professionals (IAPP) offers a Certified Information Privacy Professional (CIPP) certification to formalize their education in information privacy practices (International Association of Privacy Professionals, 2018). Both organizations offer numerous specialty certifications along with the widely respected Global Information Assurance Certifications (GIAC) that are board certified through the SANS Institute (Certifications, 2018). Companies should encourage their security staff in obtaining these certifications and to be active in their industries associations to continue learning and keep pace with the brisk speed of security threats.

Conclusion

When reviewing a business's cyber security policies, all stakeholders should focus on the human factors which constitute the biggest weaknesses in their systems. Making employees aware of best practices in cyber security is not only a cost-effective way of combatting cyber threats but will benefit employees in their personal cyber lives too. Everyone benefits from good cyber hygiene! After focusing on the greatest weakness in their systems, managers should focus on maintaining the best infrastructure that their budgets allow using active defense, automated threat detection services and well-trained staff members. A comprehensive security policy should also have a foundation of cyber liability insurance to protect against catastrophic losses. It is important for businesses and organizations to defend themselves first in the current environment of quickly changing measures and counter measures. Once sufficient local resources are established, business security leaders should seek out assistance from their respective industry associations and mean of cooperating with government entities who can offer unique support in responding to international actors and help investigate complex intrusions. Unfortunately, government tends to move slower than the threats in terms of cybersecurity laws and reactions to cyber security intrusions from abroad because they must consider wider international relations implications. To win in cyber security, leaders must proactively defend their organizations and collaborate as much as possible.

Chapter 9

Hybrid threats – how is the security environment in Central and Eastern Europe changing?

Krzysztof Liedel

Abstract

The following paper is an attempt at diagnosing the changing security environment in Central and Eastern Europe. The author treats the Republic of Poland as an example state that faces threats stemming from the chaotic international security environment. The goal of the paper is to showcase threat perception as well as attempts to define new risks and form the strategy to counter those threats.

The dynamics of changes in the Polish security environment have been increasing noticeably in recent years. One of the most important reasons for the changes is the emergence of new strategies and tactics for international action by active regional actors. Additionally, the changes in dynamic are influenced by the end of the Cold War 25 years ago as this created an exhausting safety bonus. And then explain safety bonus.

During the last fifteen years, we have witnessed an extraordinary transformation of the perception of international security threats. The conviction that the history of both the Second World War and the Cold War had largely eliminated the threat of a classic military conflict marked the 1990s, Fukuyama went as far to claim that this period after War marked „the end of history” (Fukuyama, 1992). This prognosis of the “end of history” and the concept of increasing security verified the development of asymmetric threats, which were

primarily non-state actors, such as international organized criminal structures or terrorist organizations.

The turn of the nineteenth and twentieth century was the time of changes in the international environment that initiated the discussion on the need for reform of NATO. The Organization was to face the need to adapt to the new security environment which was devoid of challenges that accompanied the emergence and consolidation of NATO's position as one of the pillars of the global order.

The seemingly most critical moment of change in the perception of what constitutes the greatest threat to modern democratic state law were the events of September 11, 2001. The attack on the twin towers of the World Trade Center made it clear to the whole world that no non-state actor can shake up the global order. It also showed that even without a formal change, the North Atlantic Alliance would shape the security environment in the future world. For the first time in history, in response to the threat to one of the Alliance members, Article 5 of the North Atlantic Treaty was evoked and along with it the *casus belli*, an act or event that provokes or is used to justify war, enshrined in it.

A conviction that the international security environment has changed irrevocably permeated NATO's actions and declarations in the first decade of the 21st century. It lasted even despite the warning presented in the form of Russian-Georgian conflict in 2008. Tensions escalated in the region since early 1990. However, it was on August 7, 2008, that South Ossetia and Georgia accused each other of launching intense artillery barrages against each other. Georgia sent in its troops and on August 8, Russia launched air attacks throughout Georgia, and Russian troops engaged Georgian forces in South Ossetia (Nichol, 2009, pp. 4–10). The conflict was ended swiftly with the assistance of the US and EU; however, it became evident that conventional conflict is not unimaginable in the region.

It can be attested to by the provisions of the Strategic Concept adopted at the NATO summit in Lisbon in 2010. The description of the security environment in this document began as follows:

“Today, the Euro-Atlantic area is at peace and the threat of a conventional attack against NATO territory is low. That is a historic success for the policies of robust defense, Euro-Atlantic integration and active partnership that have guided NATO for more than half a century” (The New Strategic Concept, 2010, p. 10).

This belief also influences the perception and interpretation of the legal basis for the functioning of the Alliance. Article 5 of the North Atlantic Treaty was one of the most analyzed:

“The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that [...], each of them [...] will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area” (NATO, 1949, art. 5)

These provisions are all the more critical because – just like in the case of the United Nations Charter – it is difficult to expect such developments on the international arena, which would allow a real reform of the treaty, adapting it to contemporary challenges. In the upcoming decades, we will base our security on the provisions of the international legal provisions that were established in the middle of the last century, and its effectiveness will depend on its international interpretation. The latter is a particularly important issue considering the phrase as mentioned above “**such action as it deems necessary**, including the use of armed force” (emphasis added).

Let us reiterate: the North Atlantic Treaty does NOT oblige the Member States to use force against threats to the territory of one or more members of the Alliance. It requires the steps “deemed necessary”. If, therefore, the Member State considers it necessary to provide humanitarian aid – and will grant it – it will fulfill its formal obligations. The principle of *pacta sunt servanda* – in good faith – nowhere is it as important as in the case of a military defense Alliance based on the formulated *casus belli*.

Those circumstances become more critical as we recognize new threats in our security environment. Daniel Freia, a Swiss historian and political scientist who studied relations between East and West in the dimension of security, considers the concept of how to shape the appropriate threat perception and assess the safety status. He diagnosed a problem related to the perception of security by pointing to four possible ways of such perception:

- insecurity – when there is a significant, real external threat, and the perception of this threat is correct (adequate),
- obsession – when a slight threat is perceived as significant,
- false security – when the external threat is severe and is perceived as small,
- real security – when the external threat is insignificant, and its perception is correct (Frei, pp. 17–21).

This concept is especially important in conjunction with problems not only in the assessment but also in defining threats in the international environment

and the “loosely” formulated obligation of mutual assistance enshrined in the mentioned article 5 of the North Atlantic Treaty.

For this reason, the discussion about definition issues at a university level is critical to security strategizing. In the mid-nineteenth century, Realpolitik was described by the author of this concept as the law of power governing states as the law of gravity governs the physical world (Bew, 2014). So to this “reality” of international politics – no matter how surprising it is, we must apply today.

One of the elements of this relatively new form of practicing the policy of facts is the use of indirect methods of conducting conflict, including armed conflict. Although there is no agreement – at least not full – of the nature of this phenomenon and the degree of danger it brings, indeed the “sign of the times” regarding the contemporary discourse on security is, therefore, a hybrid conflict.

However, we must remember the need to define a term in order to research its impact. Defining what the terms related to “hybrid conflict” is also important not only because of scientific curiosity but also since the dynamics of events on the international arena are far ahead of international agreements in the field of security. Frank Hoffman, the researcher from the American National Defense University, cited by the analytical study of the Estonian International Center for Defense and Security, defined hybrid war (hybrid warfare), as the:

“blend of the lethality of state conflict with the fanatical and protracted fervor of irregular war. [...] Sophisticated campaigns that combine low-level conventional and special operations; offensive cyber and space actions; and psychological operations that use social and traditional media to influence popular perception and international opinion” (Hunter and Pernik 2015).

The task of defining the conflict (hybrid war) for the needs of the Polish security system was taken over by the National Security Bureau. On the website of the Bureau in the “(Mini)Dictionary: proposals for new terms in the field of security” reads:

“A hybrid war is a war combining various viable means and methods of violence, including in particular armed regular and irregular actions, operations in cyberspace and economic, psychological, information campaigns (propaganda) [...]” ((Mini)Dictionary, 2015).

The definition of “hybrid war” taken from BBN should certainly be supplemented with other concepts included in the same study, which are necessary to fully understand the spectrum of threats resulting from the promotion

of hybrid tactics in state activities. The notion of subliminal aggression is particularly important in this context. Consequently, in the (Mini)Dictionary, 2015 it is defined as follows:

“Aggression under the threshold of war – warfare, whose momentum and scale are deliberately limited and maintained by the aggressor at a level below the unambiguously identifiable threshold of regular, open war. The purpose of aggression under the threshold of war is to achieve the adopted goals while causing difficulties in obtaining a decision consensus in international security organizations. “

It is essential to raise the question of the “underdetermined” provisions of Article 5 of the North Atlantic Treaty again. In the circumstances of an unfavourable political climate it may be one of the most severe threats for the cohesion and security of the transatlantic area. Expressly when there is a probability that the potential aggressor will skillfully apply the tactics of aggression under the threshold of war, which will deter the international community from unambiguously stating that act of war did take place. Another important concept that defines the existing international situation is the concept of “little green men.” Although it was coined as the current response to the development of the situation in eastern Ukraine – and therefore has a popular character – it refers to a phenomenon that must be treated as a dire threat. According to the (Mini)Dictionary, 2015:

“Little green men” – a term used commonly to refer to armed soldiers without military distinctions or other distinguishing features that would allow determining their nationalities, conducting armed regular and irregular actions on the territory of eastern Ukraine, against its integrity and independence.”

Considering the challenges in the area of responding to those threats, and particularly analyzing them in the context of events already taking place – for example in eastern Ukraine – one must remember that the usefulness of such tactics is different depending on the theater of antagonist activities.

The implementation of offensive actions of this nature is possible if certain conditions are met: for example, sizeable ethnic diversity, imperfect territorial control, and border traffic control. The likelihood of the unexpected appearance of the “little green men” brigades in Poland is much smaller than in the case of countries that are less stable and ethnically or politically varied. The system of defense and internal security of the Republic of Poland indicates Poland must be

much more sensitive to advanced attack methods remaining in the spectrum of the hybrid conflict.

These fields of the potential struggle, for which there is a need to take action and counter the threats, in two areas of activity in the hybrid conflict are the cyberspace and the infosphere. In particular, the informational struggle in both these areas, combined with the definition and political problems related to the hybrid conflict, remain at the forefront of the priorities regarding active countermeasures. Therefore, adjustments at the legal and strategic level are needed. In Poland, this kind of initiative was initiated in 2014, when the foundations of the “Cybersecurity Doctrine of the Republic of Poland,” adopted by the National Security Council, were created. This document, whose sources were both the National Security Strategy and the results of the National Security Review preceding its adoption, states that:

“the objective in the area of cybersecurity of the Republic of Poland, formulated in the National Security Strategy of the Republic of Poland, is to ensure safe functioning of the Republic of Poland in cyberspace, including an adequate level of security of national ICT systems – especially the ICT critical infrastructure of the state – as well as key business entities functioning in the society, in particular those included in the financial, energy and healthcare sectors” (Cybersecurity Doctrine, 2015).

Entries the infosphere and the information security of the Republic of Poland, were included also in the project “The doctrine of information security of the Republic of Poland.” This document, at the end of July 2015, contains a statement saying that “strategic element in the area of information security is to ensure safe functioning of the Republic of Poland in the information space, including information security of state structures (especially public administration, security services and public order, special services and armed forces), the private sector and civil society” (Information Security Doctrine, 2015).

It is easy to notice that the methodological approach in both documents is very similar and results from the Strategic National Security Review. A significant added value of both doctrines is the realization and verbalization of new fields of threats and challenges. Not new in the sense of the emergence of the threat itself, but rather in the context of prioritizing tasks and determining the most critical areas of activity in the changing security environment.

It is essential to notice that the broad nature of threats in cyberspace and information threats (influencing almost all areas of a state’s functioning) is their inherent feature. The necessity to create and optimize the functioning of relevant

physical elements of the national security and defense system (e.g., specialized military units and appropriate organizational units of special services) becomes one of the priorities of such organization of the national security system that enables its effective functioning.

Moving across the spectrum of resources that can be used to achieve operational and strategic objectives in a hybrid conflict requires skillful use of tools in these two areas. Not only do they allow for the possible control of the enemy's command and control system, but also for influencing public opinion – both nationally and internationally. Assuming that one of the most challenging aspects of crisis management resulting from hybrid threats is communication. Thus, obtaining universal situational awareness, cyberspace and infosphere become the most prominent fields of fighting and the first line of battle. Proper observation of the opponent's moves and the early warning system functioning correctly in these two areas will be the ability to complete preventive actions in other dimensions of conducting activities for the benefit of the security of the state and its citizens.

The presented efforts undertaken by the public administration units of the Republic of Poland, whose aim is to formulate a doctrinal response to new threats, show that threats related to a hybrid conflict are well recognized in Poland. The security environment of the Republic of Poland, defined during the Strategic National Security Review, was already perceived during analyzes related to this undertaking as extraordinarily complex and dynamic. It is worth emphasizing, however, that the White Book of the National Security of the Republic of Poland (White Book, 2013), published as a summary of the The National Security Strategic Review in 2013, does not yet use terms such as hybrid warfare or aggression under the threshold of war.

It was all the more important to formulate adequate definition base and to introduce to the public debate the concepts defining the international reality that surrounds us. Although these are not legal definitions, they may become the beginning of the formulation of the concept of response to such threats.

In the Polish situation, this task is all the more critical due to the expansionary policy of the Russian Federation, resulting in attempts to expand beyond the eastern border of Poland. The conflict on the territory of Ukraine is also a source of potential threats to stability in the region. The geopolitical change resulting from the evolution of Russian international policy remains one of the most critical factors affecting the security of the Republic of Poland and its citizens. However, it is easy to forget about this in the situation of current events, such as in connection with the ongoing immigration crisis, for which Europe has not found the right formula.

The need to adapt not only legal regulations but the conceptual basis for conducting defensive and offensive-defensive actions requires full situational awareness, realistic assessment of the means available to the opponent, his geostrategic goals, and his long-term intentions.

Opinions are stating that the introduction of the concept of “hybrid war” is unnecessary because in the history of humanity the conflict has always been carried out with all available means that could increase the probability of achieving the assumed goal. Selected researchers argue that instead of focusing on the creation of new concepts, one needs to focus on detecting and defining complex connections and combinations of available combat measures to be ready to counteract them (Puyvelde, 2015).

From the point of view of military tactics and operations carried out in the theater of war, subtle conceptual distinctions may be of little use. However, from the political point of view, the need to clearly distinguish the act of war as apart from any international response indicates that these definitions can be vital to determining solidarity between allies.

This solidarity, as well as a collective, coherent picture and assessment of the situation, can be crucial in a situation of potential conflict. The war doctrine of the Russian Federation from 2014 gives particular reasons for caring for this kind of solidarity in the context of hybrid threats. As it is worth recalling, the following entries appear in this document:

- the complex use of the armed forces, as well as political, economic, informational and other non-military measures, implemented with the broad use of the potential of public protests and special operations forces;
- striking at the enemy throughout its entire territory, in the global information space, air and extra-terrestrial space, land and sea;
- the participation in armed clashes of irregular armed units and private military companies;
- the use of indirect and asymmetric methods of action;
- the use of political forces and social movements financed and managed from outside (Darczewska, 2015, p. 21).

Given the provisions of this document – and its legal and political location – it is not difficult to conclude that regardless of using the nomenclature “hybrid”, a non-standard form of conflict using asymmetric, informational and indirect components has become an inherent part of the reality in which modern states function.

Analyzing the complexity and problems with defining the means and methods used, the low intensity of potential hostile actions and deprivation

of identification of forces involved in possible aggression, the formulation of an alliance response is a matter of political decision replacing the automatism resulting from international defense agreements. Supplemented with the problem of response in the form of such “action, which [the state] considers necessary” this situation is at the level of ensuring international security a challenge that will be an extremely complex problem to be solved.

For this reason, regardless of the conceptual purity criticizing the circulation of phrases such as “hybrid war”, one thing must be agreed: if we do not call this state of (un) security, we must be prepared to function in a security environment in which mixed conflict, using all available tactics, strategies, methods, and measures is a fact. Moreover, nostalgia for the times of the classic clash, clearly defined by the framework of the law of war, can likely not bring it back ever again.

Chapter 10

The narrative of terrorism: evolution of the message of violence

Paulina Piasecka

Abstract

The following paper is an attempt to examine the compelling narrative of modern terrorism. Describing the phenomenon in historical circumstances, it strives to determine the sources of its current popularity, also in the context of the new media usage and creating a “fashion” for violence among the younger generations.

For a few years after the fall of the Berlin Wall, it seemed that most citizens of contemporary countries understood the necessity of living in peace and cooperation to survive. Gradually we learned even to apprehend that the common enemy – or rather a common threat (these phenomena should not be excessively personified) – is climate change or, as some have wanted, the unusual activity of the sun. It seemed that as a species, we finally achieved an understanding that is instinctive at the individual level: first and foremost, we must survive. Secondly, we must, as liberalism’s supporters wanted, learn to respect the limits of our freedom wherever it violates the freedom of others. Optimists announced an increasing shift towards the so-called “soft power” (see for example: Treverton and Jones, 2005; Nye, 2004; Kurlantzick, 2007). It seemed a conceivable concept – if we were to see cooperation, why not use authority, influence, diplomacy, and mediation in international relations – in the end, we must cooperate to achieve our goals somehow.

The first rift in this positive vision of the human species' development were the Balkans – although, just like in the case of the Middle East, many wanted to perceive them instead as expiring conflicts or a decadent story from the turn of the 19th and 20th centuries. Another sign of change was the attacks on twin towers, the World Trade Center, which brought the beginning of the “Global War on Terrorism.” However, we wanted to believe that the history of wars ended; that the world has achieved a long-awaited state of “being civilized”; that violence will cease to be a natural state of humankind and will be diminished, as the only violent actors left were terrorist organizations. The first 18 years of the 21st century clearly show that those hopes were hollow and that the stage of development that would enable us to stop the endless wars is still far ahead of us.

The above framework is where we began the insight into the phenomenon of international terrorism. When considering issues related to terrorism and its narrative in the public domain, both on the part of the terrorist groups themselves, as well as governments, it is worth stopping for a moment at the very essence of terrorism and attempts to define it. For political reasons, achieving full compliance with the definition of terrorism at the level of international law has proved impossible, as demonstrated by even ongoing efforts to create a comprehensive convention on counteracting terrorism (Deen, 2014).

Academics and researchers, however, have made such attempts, and although the universal definition of terrorism still eludes us, it was possible to identify specific characteristics of the phenomenon that constitute the framework of its definition. Alex Schmidt was the precursor of research in which the term “terrorism” is analyzed through the analysis of constituent elements of its definition(s). He mentions such terms related to terrorism as (Hoffman, 1999):

- the use of violence, force or the threat of their use,
- political motivation of the perpetrators,
- acting to create fear,
- willingness to cause psychological effects and reactions,
- distinguishing the purpose of the attack and the direct victim,
- purposefulness and planning of activities,
- combat method,
- conflict with the rules of social behavior in force,
- extortion,
- using the media to search for publicity,
- a blind crime (random selection of victims),
- the use of symbolism,
- the unpredictability of the perpetrators' actions,
- the hidden nature of an organization using terrorist methods.

Comparative studies of existing definitions of terrorism show that the most critical determinants of the presence of terrorism were:

- violence and force (these phenomena, constituting the essence of terrorism, appeared in 83.5% of its examined definitions),
- political motive (65%),
- fear, terror (51%),
- threat (41%),
- psychological effects and anticipated reactions (47%) (Hoffman, 1999).

It is easy to see why phenomena such as fear, terror and related long-term psychological consequences are essential tools of terrorist groups. To stir them up and then use them properly, it is necessary to use a well-prepared information and propaganda campaign.

After September 11, 2001, terrorism ceased to be a phenomenon that remains in the sole interest of researchers dealing with exotic aspects of national and international security. It has ceased to be a niche phenomenon, affecting individual states with a unique history, and has entered the global scene of events. One of the most critical aspects of this international phenomenon that affects us all – citizens and rulers, soldiers and law enforcement officers, doctors and workers – is its internal and external narrative. Terrorism is at the same time a tool for describing and tool for shaping the reality, the driving force, and the subject of history in which we all become extras on the margins of the plot, doomed forever to react.

The history of the terrorist narrative intertwines with the history of terrorism itself. The best tool for its analysis is the concept created by David C. Rapoport, who in 2002 in his text entitled “The Four Waves of Rebel Terror and September 11” devoted to the issue of waves of terrorism, created a concept ordering the history of this phenomenon. He refined it in 2004 in the essay “The Four Waves of Modern Terrorism” (Cronin and Ludes, 2004), included in the work “Attacking terrorism. Elements of a grand strategy.” According to the Rapoport concept, we can separate four waves of modern terrorism (Cronin and Ludes, 2004, pp. 46–73).

As the first of them, Rapoport indicates the terrorism of Russian Anarchists, placing the wave in the 19th century (around 1880–1920). Its representatives described this wave as “propaganda of the deed.” They perceived terrorism both as an action and a message that was to carry with itself content profitable in public space.

The concept of “propaganda of the deed” likely comes from the writings of Carl Pisacane, who claimed that “propaganda with the idea is a chimera;

educating people – absurd. Ideas result from deeds, not the latter of the former of ideas, so education will not give freedom to people, but freedom will make it possible for education” (Grinberg, 1994, p. 220). This idea was at the basis of the new vision of communication, as evidenced by the fact that “we do not know today an anarchist journal made in this era” (Grinberg, 1994, p. 12).

This wave was specific also because of the place it had in the development of Western societies. After one of the incidents constituting the embodiment of this doctrine (the attack of Very Zasulicz on a policeman abusing power with political prisoners), a statement of the perpetrator appeared in public circulation which claimed that “she is not a murderer and a terrorist” (Rapoport, 2002, p. 51). It is important to talk about communication in the context of terrorist threats emphasizing the changing overtone of the word “terrorism” itself. In the language of the nineteenth-century anarchists, it did not have pejorative overtones, so the language itself categorized the terrorist as a “fighter for the cause.” In this sense, somewhat on the margins of the current analysis, one can notice a kind of counter-communication success – no one today considers terrorism as a phenomenon in any positive sense.

The next wave of terrorism identified by Rapoport is anti-colonial terrorism. This movement is connected with the progressive striving to regulate international relations following the principles of self-determination of nations. It was one of the waves of terrorism that achieved the most tangible results. The decade of independence (the sixties of the twentieth century) (Gorman, 2001, p. 151) is the period in which the method of political struggle represented by terrorism has proved useful. The fact is that without trends present in the international environment, direct effects would not be achieved. Terrorist attacks, reducing the economic efficiency of possession and increasing the political cost of ownership, were a contribution to change. Moreover, the existence of this wave of terrorism is directly related to changes in the perception of international reality that have occurred since the end of World War I.

Changes on the map of Europe, justified at the political level by the “right of nations to self-determination” indirectly undermined the legitimacy of the rule of European states in their colonies (Rapoport, 2002, p. 55). The above is another change in the “narrative of reality” that supports the transformation of reality itself.

The third wave of terrorism described by Rapoport is leftist terrorism, it is referred to in English as “new left terrorism.” The so-called “terrorism of the new left” was associated with the pursuit of democratization of social life.

The history of terrorism of the “new left-wing” is closely related to the development of new communication systems. At its sources, as a movement

of “social justice” and pacifism, the Left tended to personalized contacts and information to the face. The change that took place in this area had little to do with the decision of the new left-wing parties themselves (Gitlin, 1980, s. 22). The interest of the media created a specific need for an incident or a tragedy – which became the breeding ground for the symbiotic interaction of the media and terrorist groups of the new left.

In this context, Brian Michael, who more than 40 years ago wrote that „terrorism is taking place in the rhythm of carefully prepared choreography, which is supposed to attract the attention of the electronic media and the international press. [...] Terrorism is directed at people who look, not at the victims themselves. Terrorism is a theater” (Jenkins, 1976, p. 16). As Walter Laqueur also notes that most experts agree that terrorism means the use or threat of violence, the method of fighting or strategy for achieving specific goals, that aims to intimidate the victim by the state (...), and that publicity is an essential factor in the terrorist strategy” (Laqueur, 1986, p. 88).

A wave of terrorism	Ideology	Communication methods
Russian anarchism	Eliminating governments, „awakening the masses,” democratizing social and political life	„Propaganda of the deed”
Anticolonialism	The right of nations to self-determination, rebellion against metropolises	Change of language, change of auto-definition (from „terrorists” to „freedom fighters”), also to gain new supporters
„New Left”	The democratization of social and political life, ideology having sources in the Vietnam War	Return to the „theatrical” goals that ensure communication and publicity (including kidnapping and hijacking), the use of traditional media
Fundamentalism and religious extremism	The emergence of a global caliphate, the creation of the „Prophet’s state” and the introduction of sharia law in the world	The use of new media (creating communication mechanisms that disproportionately multiply the effect obtained by the attacks)

Waves of terrorism according to David C. Rapoport (own elaborations).

The wave of terrorism that Rapoport is currently dealing with is a wave of religious terrorism. The primary aim of this generation of terrorist groups is to lead to the establishment of a global caliphate, God's state on earth, which will be governed by a law based on the principles of religion as a basis for social coexistence. This terrorist wave is born, and the spread of the Internet and Network 2.0 and the maturing of the information society are growing.

The information society, and therefore the information and knowledge that has become as important in the production process as capital, labor, and land is the product of the information age and the growing networking of social relations. The production branches related to the manufacturing or mining industries have evolved into mostly secondary branches from information. In the agrarian society, the factor limiting economic development was the land, in the industrial society – capital, while the factor conditioning the economic development of the information society is the access to the information gathered, appropriately transformed into knowledge (Goban-Klas and Sienkiewicz, 1999, p. 48).

Network society, closely related – and identified by many researchers – with the information society is a social structure based on networks managed by information and communication technologies, using microelectronics and computer networks that generate, process and distribute knowledge based on knowledge gathered at nodal points of the network (Castells and Cardoso, 2005, p. 7).

The network, as Castells understands it, already had in the historical perspective unique features related to flexibility, adaptation, and evolution depending on the needs. However, only the technological change made it possible to transfer the network operating principles to a level other than small, private groups, giving such structures the ability to shape entire societies (information and communication networks have become a tool for coordination and decentralization of activities of even the largest entities – while maintaining the competence of the highest management structures) (Castells, 2005, p. 7). New methods of functioning of social structures have also emerged from new technologies. It also caused a change in communication carried out by actors taking part in international events – including terrorist groups.

There has been a kind of “borrowing” by these organizations from the Western world not only of forces (in the form of young, ready-to-fight people), but also funds (including the media, especially new media, with particular emphasis on the Internet). One of the essential characteristics of the way contemporary Western societies operate that was adopted – exceptionally effectively – by terrorist groups, is the network of activities. They use the network not only

to communicate between cells that make up terrorist groups, but also to take advantage of the opportunities offered by social networking sites.

The grouping and terrorist organizations in an extremely fluid manner have adapted to function in a networked environment. The network gave them access to information while ensuring the anonymity of the functioning of individual affiliates only at critical nodes. The network allows organizing conspiracy activities. What's more, it also responds to the tactical needs of asymmetric conflict, in which a small and much weaker organization faces centralized state-equipped tools and resources.

An essential element of information and propaganda campaigns carried out by modern terrorist groups and organizations is the Internet. In the context of their activity, it seems crucial to indicate the most important features that characterize this medium. Among these features should be pointed out especially (Weimann, 2004):

- easy access,
- little regulation, censorship or other forms of government control,
- potential access to a considerable group of recipients around the world,
- the anonymity of communication,
- quick information flow,
- low costs of using and maintaining an online presence,
- multimedia environment (the ability to combine text, graphics, sound, movie), allowing users to download materials,
- the possibility of shaping the message in traditional media, often using the Internet as a source of information.

The strength of the Internet is expressed primarily in the qualitative change regarding potential contact with the recipient. Previous terrorist waves had to rely on the use of public communication mechanisms that were under the control of their "hostile" forces – public or private media, controlled either by the government itself or by capital linked to it.

The Internet and new media have given terrorist groups a large degree of independence from such state-controlled media. In this way, they obtained the ability to produce and disseminate information and propaganda materials about their activities.

It is also worth emphasizing that in undermining the values at the root of Western civilization, the jihadist movement does not hesitate to draw from it patterns that have proven to be a symbol for the collective subconscious. Such activities include even the production of propaganda cartoons, the more

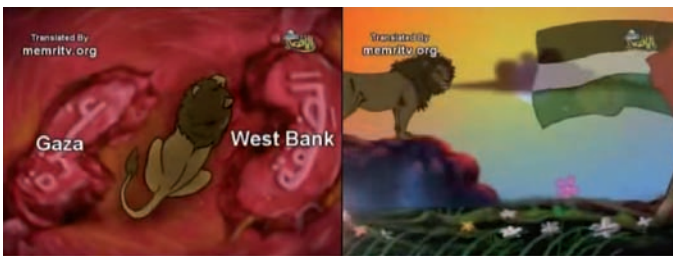
dangerous ones that are directed directly to the youngest recipient (A propaganda cartoon on Hamas-Fatah conflict, 2007).

Propaganda material by ISIS after Paris attacks as reported by NYT (November 2015)



Source: <http://www.nytimes.com/video/world/10000004166589/isis-video-appears-to-show-assailants.html> [05.08.18]

Animated propaganda cartoon regarding the Hamas – Fatah conflict, using motifs from Walt Disney’s “Lion King” (2007)



Source: Memri TV [<https://www.youtube.com/watch?v=3RxtBBSZ5js>]

A similar example of “appropriation” of modern methods of communication is the creation within the broad organizations of a narrower and more “exclusive” movement focused on religious sacrifice and self-denial (up to the readiness to carry out a suicide attack). Also, the terrorist organizations created consumption needs related to the movement and its ideology. It is not difficult to observe the patterns and manner of presenting motifs on the examples of this type of clothing; they are a sign of concessions to a certain universality of visual stimuli appealing to young people (see illustration below).

Jihad motifs on clothing



Source: producer's website [<https://plus.google.com/115752447286669315337/about>]

Technological progress, conditioning the change in the way of communication of terrorist groups, is not indifferent not only regarding the research interest in the changes that high technology causes in the functioning of modern societies. The participation of terrorist groups in shaping narratives in new media translates, as already mentioned, into a description of global reality, primarily because the Internet has become a source of information also used to shape the message formulated by traditional media.

The modern world is not only in the face of communication challenges related to functioning in this new security environment. The war of the 21st and the following centuries will be mainly in cyberspace, which terrorists are increasingly using for their purposes. The head of the Office of Transformation of the Armed Forces (USA), justifying the need to undertake actions for the implementation of transformation processes, emphasizes in the report on the application of network-centric methods of warfare that technological evolution from the industrial to information period requires other sources of strength. While in the industrial era the combat force resulted from material resources (in

the sense of the size of the army and equipment), currently it comes from the exchange of information, access to information and speed of response. In his opinion, therefore, in the new theory of war, the network-centric war, not only the tools change, but also the way of conducting war and the sources from which the power comes from (DoD Office of Force Transformation, 2005, p. i).

This transfer of a significant part of the struggle, both on the “state vs. state” and on the “state vs. non-state actor” front, into the purely informational space, makes it impossible to treat issues related to communication of terrorist groups only in terms of content and form.

The use of new media by contemporary terrorist groups carries with it threats that have become part of the world around us. Radicalization and recruitment to terrorist organizations do not take place or take place less and less in the form of personal contacts. The networks, both virtual, online and social, change the way in which the world around us operates. They make direct communication not only unnecessary; it even becomes a threat to be avoided.

An excellent illustration of a similar, though not related to the fight for a global caliphate, is the terrorist attack of Anders Breivik, which took place in July 2012 in Norway. The assassin confessed the anti-immigrant ideology, directed mostly against the representatives of the Muslim minority, but at the same time, he used the tools found on the internet thanks to the people taking part in the global jihad. This free spread of the ideology of violence, but also a ready provision for its use is the price we pay for free and universally accessible new media, especially the Internet.

What, then, is the growing popularity of jihad, not only among the representatives of Muslim minorities, or in countries with indigenous religion and culture, but also in European countries? Can this phenomenon be classified as a kind of fashion: for violence, for adventure, for ultimate experiences?

It seems that such a conclusion is not completely unlikely. Raised in circumstances of stability and peace, 70 years after the end of the last great armed conflict, we seem to forget that in war there is nothing romantic. In the pages of adventure and action books, war appears to be extremely hygienic, filled with heroism and blood brotherhood. One can find the following descriptions only in very few of them:

„[Soldiers’] faces are covered with dust, sand, tar, gun lubricant, tobacco spittle and sewer water from the town. No one’s showered or changed out of the bulky chemical-protection suits they’ve been wearing for ten days. [...] Their filthy faces seem to make their teeth shine even whiter [...]” (Wright, 2011).

Also, a few words about why and how one uses the chemical suit:

„Marine instructors had scared everyone by talking about nerve gases that, as they put it, will “make you dance the funky chicken until you die”; blistering agents that will make your skin “burst up like Jiffy Pop”; and the risks of suffocating in your gas mask if you vomit. “If it’s chunky,” an instructor had said, “you won’t be able to clear it through the drain tube of your mask. You’ll have to swallow it or risk choking on it” (Wright, 2011).

The armed conflict described in this way does not seem captivating – yet many young people raised in a nonviolent Europe are attempting to join the Islamic State units operating in Syria, where chemical weapons are one of the most feared tools of warfare. Perhaps it is not only the power of jihad ideology or the effectiveness of its propaganda: maybe the world is facing potential war, in which on one side there will be people who have nothing to lose and on the other those who are unable to imagine how much they have to lose.

Hence the reflection on jihad is not enough. Communication exists in social contexts and without thorough self-diagnosis, we will not be able to understand how jihad could ever have become a fashion. Fashion is something that according to the Oxford Living English Dictionary is “a popular or the latest style of clothing, hair, decoration, or behaviour.” This popularity comes from somewhere; it is a response to a need. Becoming aware of the fact that there is a need for the bloody narrative of modern jihad is present in our society may be the beginning of understanding how to counteract the communication of terrorist groups and prevent the resulting radicalization and recruitment.

Chapter 11

Digital technologies for the protection of cultural heritage in the 21st century

Katarzyna Góralczyk and Katarzyna Zielińska

We must respond, by showing that exchange and dialogue between cultures is the driving force for all. We must respond by showing that diversity has always been and remains today a strength for all societies. We must respond by standing up against forces of fragmentation, by refusing to be divided into ‘us’ and ‘them.’ We must respond by claiming our cultural heritage as the commonwealth of all humanity.

Irina Bokova, Director-General of UNESCO
(#Unite4Heritage, 2015)

Abstract

The following paper aims to present the scope of the threat that modern terrorism presents towards the historical heritage of humanity, as well as to recognize chosen technologies that may to some degree contribute to mitigating this threat. Introducing virtual modeling as well as online displaying of the historical objects that are either already destroyed or are threatened by conflicts around the world, it presents new ways to take the marks of the past into the future.

A variety of global conflicts have accompanied humankind for centuries, thus being an element of social life and international relations. The intensity of their occurrence in subsequent epochs varied and their character, methods, and

techniques of plating were continually evolving. Even in today's dynamically changing international environment, conflicts on the world arena are also subject to constant change. The nature and intensity of the conflict, and its methods are continually changing.

The leading cause of world conflicts are no longer the desire to gain new territories or having more slaves as cheap workers, but today's causes stem from religious, ethnic or ideological differences between nations. It is also crucial to note that the frequency of conflict has changed. The number of internal conflicts has increased many times during the last centuries. At the same time, the number of international conflicts has decreased. Modern wars, globalization and modern technologies, and constant access to information are far from the regular armed activities of the early 20th century.

Analyzing the current conflicts against the background of the early 20th century ones, we can point out a variety of common elements such as regular armed activities, guerrilla warfare or broader criminal activity (Kaldor, 2013). Among the differences, we can mention actors participating in conflicts (especially non-state actors), their goals, high level of acts of aggression against non-combatants, and lastly, methods of obtaining financial resources to conduct conflicts. The acts of pillaging, smuggling and trade carried out on the black market determine the prolongation of the conflict and the systematic destruction of the area affected by it. That is why historical objects become one of the main and the most desired spoils of conflict nowadays. Moreover, very often they are used as a means of payment for obtaining additional financial resources. And yet, on the other hand they are very often destroyed for ideological and religious reasons.

The destruction and pillaging of cultural heritage sites during global conflicts and crises is not a new concept. The authors who described the achievements of prominent historical leaders often greatly described the level of destruction caused by wars on cities such as Carthage, Jerusalem or Rome. These acts, carried out by the attacking armies, were the result of specific and clear rules of conducting warfare activities. The leader who won had the right to plunder, destroy or set fire to the defeated city. Along with the development of the law of war, the practice of greater protection for material objects has also increased. Initially, voices calling for the need to protect sacred places (as a temple and cemetery) resulted from fear of the wrath of the deity who inhabited these places. Then the first principles of the practice of protecting cultural goods and objects were created. People have started paying more attention to artistic objects (moveable and immovable) and their value. These rules based on the principles of reciprocity, proportionality, and humanity, have become the cornerstone of the Hague branch of International Humanitarian Law on Armed Conflicts, which is binding on the warring parties today.

An integral part of any global armed conflicts is death, pain, and ruthlessness in the actions of the warring sites. The warring sites are circumventing the regulations of the International Humanitarian Law of Armed Conflicts established by the international community, very often both sides of the conflict are not respecting the rules (Timeline, 2012–2018). Our cultural heritage in the face of the enormous tragedy should be ready to deal with many more challenges. However, this heritage, created and built up by previous generations, is a testimony to the achievements and culture of the nation. It is an element of world culture, with scientific, social, historical and aesthetic values. Future societies also must take care of them, protect them and respect them in such a way that future generations can learn about the world and their origins. To destroy our cultural heritage is like pulling the soul out of the nation, to deprive it of the identity and individuality, and to weaken it and in the end, annihilate it. Most of all, acts of destructions, which the international community has witnessed, show how significant this problem is. The best known should at least be mentioned:

- the destruction of Dubrovnik during the siege of Serbian troops in 1991 and 1992 (Dubrovnik was besieged by the Serbian army from July, 19, 1991 to January 1992, and 68% of the Old Town buildings out of 824 were destroyed. Former Yugoslav vice admiral Miodrag Jokić was sentenced to seven years' imprisonment in 2004 for his attack on Croatian Dubrovnik in 1991);
- the destruction of Buddha statues in Bamiyan (Afghanistan) by the Taliban in 2001 (in fundamental Islam it is forbidden to present images of Allah).

A few years later in 2007 in Pakistan, the Taliban tried to do this in the Swatu Valley near Djhanabad (Jagielski, 2007). In 1992, the National Museum in Kabul was plundered, where 35,000 coins were stolen together with a treasure from Kundzuk (Gańczak, 2018). In 2008, one of the Buddha statues in Bamiyan (Afghanistan) was damaged by NATO troops (Geller, 2008). In 1990, Museum in Kuwait was plundered by Iraqi troops (at that time, the Iraqi Government claimed that the action was necessary under the First Protocol to the Hague Convention, as a part of its duty to protect cultural heritage in the occupied territory; most of the objects were returned, but some were placed on the art market). They destroyed and plundered many works of art, books, manuscripts, and other cultural objects. Also, the National Museum in Cairo was looted almost at the same time (eight priceless objects were lost, including a wooden statuette of King Tutanchamon covered by gold form the 18th dynasty (Egypt: Bezcenne skarby, 2011).

The fighting of ISIS since 2010 in Iraq and Syria, where there are remains of Mesopotamia, and the Republic and the Roman Empire, and the Ottoman

Empire, showed people the danger of destruction on one of the most important of the world's cultural sites. The level and extent of destruction carried out by ISIS members are unprecedented in modern world history and even unimaginable in its consequences. It is impossible to indicate all the damage done at that time; however, it is worth to indicate a few of them. Many historical objects were destroyed as a result of street fights, bombardments, mechanical damages, pillaging, improper transport or storage and in acts of pure vandalism. UNESCO defines deliberate, conscious and premeditated destruction of cultural goods as a "violation of the laws and customs of war" as a war crime. Article VI of the Statute of the International Military Court defines the theft of public or private property as a war crime, the senseless destruction of settlements, towns or villages or a desolation not motivated by a need of war (Charter of the International Military Court, 1945). However, it does not help to prevent ISIS fighters from further destruction. ISIS is fully aware of acts committed and the threat that these acts of destruction pose all over the world. To draw media and people's attention, they documented and posted their acts online. They proclaim that art is idolatrous and offensive to God. As a result, paintings, sculptures, mosaics, monuments, and buildings were victims of fanatical and religious fighters. However, at the same time, ISIS recognizes the value of historical buildings and sells on the black market artifacts acquired as a result of pillaging or illegal excavations.

The policy of destroying culture pursued by ISIS members has led to irreparable damage to the heritage of Syria and Iraq. More than 2900-year-old ziggurat of the ancient city of Nimrud in northern Iraq was destroyed (Egipt: Bezcenne skarby, 2011). In addition to building damages caused by fighting, cities also become victims of illegal excavations and smuggling carried out by ISIS (revenues from the sales on the black market are among the three main sources of financing for Islamist militants, alongside oil and human trafficking). In Iraq, the fighters destroyed many monuments in the Nineveh Museum in Mosul (Ross, 2015), in Nimrud they have blown up the Nabu Temple (ISIS blows up Temple, 2016). Also, Damascus's Old Town was destroyed, as a Tetraylon and a Roman amphitheater in Palmiry (Dean, 2017) and the palace of Assyrian King Ashurnasirpal in Nimrud were blown up in 2015 (Danti et al., 2015, pp. 1–4) the same as the Umajad Mosque in Aleppo (the Mosque, together with the 45-meter high Minaret, collapsed as a result of the fighting of Syrian insurgents with forces loyal to President Bashar-I Assad). Also in Syria, many places were destroyed, for example Al-Madina suke (Karouny, 2012), Krak des Chevaliers (Darke, 2014) and Shiite's Jawad Husseiniyal Mosque (Hafiz, 2014). The Sunni Mausoleum of Ahmed al Rifai (2014) and the Mosque of Al Arbain in the center

of Tikrit were also destroyed. A variety of objects of the Christian religion were destroyed in this part of the world. As an example, one can focus on the oldest Christian Monastery of St. Elijah in Iraq, which was utterly ruined (Mendoza et al., 2016).

The principle of protection of and also respect for cultural goods during armed conflicts are regulated by the Convention for the Protection of Cultural Goods in the Event of Armed Conflicts (The Hague Convention of 1954). This document was prepared and signed after World War II in 1954. According to this document, countries accepted the responsibility to respect the goods located on their territories and those of the countries which are parties to this Convention. They shall, therefore, refrain from using the goods, and their immediate environment, as means of protection for purposes which could expose them to destruction or damage from any hostile activities. Countries and parties have also banned acts of theft, robbery, misappropriation, and vandalism. They ordered to prevent them and to cause them to stop, as well as not to use props on moving objects. In the Second Protocol of the Convention, the international community made it very clear that any person who deliberately uses a cultural asset to enhance the military action, causes widespread destruction of misappropriation, theft or destruction of historical sites, thus commits a crime and should be prosecuted under the law (article 25 of the Hague Convention of 1954). Given the constant devastation and destruction of the world heritage in ancient Mesopotamia, the Hague Convention is entirely inadequate, and its provisions no longer correspond to the revised form of military action. The UN Security Council, in the Resolution 2199 of 2015, unequivocally condemns the deliberate or accidental destruction of historic buildings for the reason that it is exceptionally powerless to destroy monuments. The Council is also aware that individuals and group associated with Al Qaeda generate revenue from the smuggling and pillaging of monuments form archeological sites, libraries, museums, and other places, thereby raising funds for recruitment activities and the organization of terrorist attacks. They also reaffirm and maintain their decision in Resolution 1843 to oblige all countries to take action to stop smuggling, illegal trade and export of historical items from Iraq. The Security Council also called on all organizations to support their activities and assist in the implementation of the resolution (UNSC Resolution 2199). By prohibiting trade in Syria's monuments, this resolution extends to 2003 with number 1483 on Iraq and condemns any deliberate or accidental destruction of cultural heritage. The resolution also confirms that the objects acquired as a result of trade and smuggling are a source of financing for the recruitment and organizational and operational processes of group and individuals associated with Al Qaida to carry out further terrorist attacks. The resolution also obliges

countries to cooperate and to take all necessary measures to stop the trade of Iraqi and Syrian artifacts, religious, historical or archeological and other objects of cultural and scientific importance to the cultural heritage of the area. Thus, UNESCO, INTERPOL and other organizations and citizens were obliged to be vigilant and to pay attention to the origin of historical buildings from the ancient Mesopotamia.

The conflict in Iraq and Syria continues, so the international community is watching social network and communication channels with concern, documenting the new and succeeding publications by ISIS fighters, as well as by those taking action to document the level of damage. In times of armed conflict in Syria and Iraq, where large areas of territory are cut off from the rest of the world and new technologies are lacking in permanent contact, internet communication, satellites and electronics are often the only tools to provide the opportunity to document and support measures to protect and respect cultural goods.

A key action for the damage inventory is the documentation of damage by satellite communication aerial photography and by drones. The photographs taken in this way allow us to track current activities in historical areas and archeological sites (UNESCO Director-General condemns, 2017). Comparisons made thanks to satellite or aerial photographs are often the only document that allows for documentation and chronology of events.

International cooperation between institutions, organizations, services, associations of researchers and collectors is a fundamental factor for any action. Publishing stolen objects on public lists or databases has in many cases saved those objects and allowed their return to the places from which they were robbed. Such databases are e.g. the Red List, created by ICOM (ICOM, 2018) and has been published since 2000. The Red List contains lists of stolen and cataloged objects of recognized institutions (e.g. museums). They do not provide a base for all objects that have been stolen from the area. These databases assist border authorities, police and auction houses in detecting illegally acquired objects. They have recovered thousands of artifacts from Syria, Iraq and Mali (Red Lists, 2018). Another important database is the INTERPOL Stolen Works of Art Database (Database, 2018), which is primarily dedicated to law enforcement agencies but also to other entities or individuals with appropriate powers and competencies.

The most crucial tool in this situation is the database of national legal acts maintained and made publicly available by UNESCO, which provides knowledge and other tools for the legal status of individual countries in the field of cultural heritage protection. The documentation of damaged and stolen historical buildings can also be found on Facebook profiles, like, for example, “Archeology in Syria”, which documented the destruction that took places in Syria. This page

is particularly valuable for photographs and documents of different objects in the „before and after” system. That helps and shows the highest scale of destruction.

The documentation of the losses is undoubtedly the first action that should be taken in order to protect and preserve the cultural heritage of all of the nations and countries. The reconstruction and renewal follow. Often, damage or destruction of historic buildings is irreversible and cannot be repaired. In this case, the digitalization of documents in cultural places is very helpful. After putting pictures into the system, people around the whole world can have free access to them via the Internet. This digital technology makes it possible, in the first place, to preserve them and make them available to the public. This form ages a fundamental task for museum institutions. The constant development of communication and digital technologies has opened a new chapter in communication between the museum and the visitors (the audience). Preserved digital presentation of objects, often in 3D technology, combined with scientific information describing the object, constitutes full information needed by the recipient. Thanks to the free access to the digitalized objects, the visitor, who is in a different country, can use the presented and preserved objects. The documentation of individual historic buildings has led to the creation of virtual museums. By scanning objects in 3D form and posting the whole collections on the website, it is possible to visit and get to know objects without leaving home (Louvre Online Tours, 2018). New virtual museums are often an addition to physical ones, and they are a newly developed form of promotion or encouragement for people to visit the museum headquarters. However, in a situation of armed conflict and irreversible damage, such a new form of digital museums are the only form of information and education for people nowadays and future generations (Chiodi, 2007).

The development of digital and information technologies allows not only for the preservation and dissemination of damaged, stolen cultural heritage. It also allows for a form of a replacement by three-dimensional objects printed in 3D on the basis of a digital model. This technique can be used to complement spatial objects such as Palmira, destroyed by ISIS fighters (Smith, 2018).

It may seem that the world of the new way of communication, technology development, digitalization and globalization allows for a quick flow of information, materials and tools to protect and prevent the destruction of historic buildings. Members of international organizations, the staff of institutions, services, researchers and specialists shall endeavor to preserve all that is left of previous generations in order to pass it on to future generations. Creation of international legal framework, people’s will, and the technological developments that support it cannot save the world’s heritage from human fanaticism, hatred and the desire for profit as long as they are under threat and at risk of destruction.

Undoubtedly, the available technology and computerization of many human undertakings allow for much quicker and effective cooperation of services, help in recovering and saving historic places. Cooperation of law enforcement authorities through the publication of lists of treated monuments, joint exercises, and exchange of their own experiences are the key for this process. If it is done successfully, future generations will be able to say that we have protected their heritage for them and have saved their cultural legacy.

Chapter 12

Success Factors of Islamic State Propaganda

Wojciech Szewko

Abstract

The extent of progress achieved by modern terrorist organizations is to a significant degree dependent of their effective information and propaganda strategies. The following paper is an attempt to showcase the propaganda tools and methods used by the Islamic State as an example of a successful campaign supporting the operational activities of a terrorist organization.

A significant number of current analyses dedicated to the propaganda of the Islamic State (IS) and its influence on the “radicalization” of Muslims in Western European countries, including the recruitment of Muslims in Africa and Asia, concentrates on forms of its narration. Those forms include multithread influence through social networks, as well as varied forms: info-graphics, multimedia presentations, high-quality film editing and reproducing forms of popular video games in attack scenes.

Accordingly, proposed forms of counteracting are founded on similar assumptions – cutting off communication channels, closing accounts on social networks (Wolf, 2018), creating programmes (Lacroix, 2018) to prevent “radicalization”, and developing countermeasure programmes for parents to enable the recognition of “radicalization” among the youth. Proposals for IS propaganda prevention measures are usually limited to several simple actions (as, for example, the French plan for radicalization combating), which restrict access to radical messages but do not refer to their content.

In the case of the Islamic State, it is the message content itself that has contributed to its success when competing with other jihad organizations for recruits, financing, and the support on the local and international level. It is the communication content which is unique and which differentiates IS from other radical Muslim groups such as the Afghan Taliban, the Somali Al-Shabab, the Syrian Hayat Tahrir al-Sham, and finally, the Al-Kaida. Furthermore, the purpose of IS was, and still is, confronting its views with the views of the above groups and in that way intercepting their followers.

Islamic State's propaganda success stems in fact from its theological and political organizational model, its vision of political, economic and social relations and the adaptation of information channels and forms of transmission to propagate their vision. Moreover, the very notion of IS's "radicalism" or "radicalization" is inherently faulty because it implies that the Islamic State promotes actions substantially more radical than those supported by, for example, Afghan or Pakistani Taliban. In actuality, however, Islamic State has proved on many occasions that its views are much more moderate than the opinions of those groups, e.g. concerning the issue of women's education. For example, in 2015, IS published a series of photos showcasing schools for women and university in Mosul, contrasting with the Taliban, which conducted operations set on destroying schools for women (via twitter account @Daeshness, currently unavailable).

In Aqidah (an Islamic term meaning "creed") explaining the grounds of faith of Islamic State, Abu Umar al-Baghdadi, then the leader of IS, stated: „Our belief in faith is the middle path, between Khawarij who are Ghuluw (excessive in the matters of religion) and between Ahlu al-Irjaa who are separate faith from actions" (Sheikh Abu Umar al-Baghdadi, 2015). The ideology of the Islamic State, also in its understanding, does not deviate fundamentally from visions promoted by Salafi Jihadi Movement (Al-Muhājir, 2007, pp. 147–152). That means that it was not "radicalism" which was the essence of the Islamic State's success.

Caliphate

The first unique aspect giving the Islamic State a propaganda advantage over any other jihadist groups is the proclamation of the caliphate. The caliphate was to represent the crowning of the IS' success in territorial expansion, in administration formation, and in the implementation of the basic principles of sharia law. It was the very proclamation of caliphate which enabled the qualitative change, the change with which other jihadist groups were not able to compete. The Islamic State justified its decision in the following manner:

“Here the flag of the Islamic State, the flag of tawhīd (monotheism), rises and flutters. Its shade covers land from Aleppo to Diyala. Beneath it, the walls of the tawāghīt (rulers claiming the rights of Allah) have been demolished, their flags have fallen, and their borders have been destroyed. Their soldiers are either killed, imprisoned, or defeated. The Muslims are honored. The kuffār (infidels) are disgraced. Ahlus- Sunnah (the Sunnis) are masters and are esteemed. The people of bid’ah (heresy) are humiliated. The hudūd (sharia penalties) are implemented – the hudūd of Allah – all of them. The frontlines are defended. Crosses and graves are demolished. Prisoners are released by the edge of the sword. The people in the lands of the State move about for their livelihood and journeys, feeling safe regarding their lives and wealth. Wulāt (plural of wālī or “governors”) and judges have been appointed. Jizyah (a tax imposed on infidels) has been enforced. Fay’ (money that was taken from the infidels without battle) and zakat (obligatory alms) have been collected. Courts have been established to resolve disputes and complaints. Evil has been removed. Lessons and classes have been held in the masājid (mosques) and, by the grace of Allah, the religion has become completely for Allah. There only remained one matter, a wājib kifā’ī (collective obligation) that the ummah sins by abandoning. It is a forgotten obligation. The ummah has not tasted honor since they lost it. It is a dream that lives in the depths of every Muslim believer. It is a hope that flutters in the heart of every mujāhid muwahhid (monotheist). It is the khilāfah (caliphate). It is the khilāfah – the abandoned obligation of the era” (Al-Muhājir, 2007, pp. 147–152).

Proclaiming the caliphate, the Islamic State did not need to promote it. It took advantage of the success of a longtime promotion action of the caliphate concept among Muslim society all over the world; the promotion activities carried out by Hizb-ut-Tahrir (HT) organization. The organization was established in 1953 by Taqiuddin an-Nabhani al-Filastyni as a political movement which disavows nationalism, capitalism, and socialism as concepts alien to Islam. Instead, the organization seeks to bring about the return of the Caliphate that ruled Muslims, following the death of the Prophet Muhammad under the four “righteous Caliphs” (Rauert, 2005, p. 28). The organization advocates political change through the destruction of the existing state apparatus and the construction of a new Islamic state.

In the 2000s, the organization became a global scale movement, active and popular also in the West (Jane’s Terrorism, 2009). During the “Big change of the

World towards Khilafah” conference in Jakarta, Indonesia, a crucial time for the establishment of the Islamic State, the organization gathered over 130 thousand followers (Around 130,000 Muslims, 2013).

In this way, by proclaiming caliphate, the Islamic State responded to the demand of hundreds of thousands of Muslims around the world who were already convinced by HT to the concept of the restoration of the caliphate and the abolition of current state structures, the caliphate is very well defined in research materials and publications by Hizb ut-Tahrir. Moreover, a subversion of existing state structures as non-Islamic, including monarchy (The Ruling System, 2002), strengthened the revolutionary effect of Salafi’s postulate of spiritual renewal and the purification of Islam from compromise inflections (Wiktorowicz, 2006, p. 209).

For the Islamic State, it was enough to prove that the caliphate was proclaimed properly and possesses all attributes described in HT materials and that it corresponds to characteristics known from historical records of the governance of first rightful caliphs. In its core programme document constituting the caliphate ISIS proves that its establishment is “Allah’s promise”:

“Allah has promised those who have believed among you and done righteous deeds that He will surely grant them succession [to authority] upon the earth just as He granted it to those before them and that He will surely establish for them [therein] their religion which He has preferred for them and that He will surely substitute for them, after their fear, security, [for] they worship Me, not associating anything with Me. However, whoever disbelieves after that – then those are defiantly disobedient” (Quran, An-Nur (The light), [24:55]).

However, according to the authors of the declaration, the authority alone is not sufficient for claiming the rights to be the actual caliph legitimized by the Quran. The caliph needs to have “the ability of creation, reforming, removing oppression, the dissemination of justice, bringing peace and calmness. Only by meeting these conditions, the succession which Allah has mentioned to the angels can take place. Without it, the authority would be nothing more than monarchy, domination, and control, supported by destruction, corruption, oppression, submission, fear, and decadence of human being and its reduction to the level of animals. This is the reality of succession, which has been created for us by Allah. It is not simple monarchy, submission, domination, and control” (This is the promise, 2014, p. 1).

Moreover, the inevitability of caliphate, i.e. the fact that caliphate is not an option for the Muslim community but an obligation, arises from the most popular among the creators of ISIS interpretation of the Quran authored by Al-Qurtubi:

“This ayat (verse) is sound evidence for having a leader and a khalif who is obeyed so that he will be a focus for the cohesion of society, and the rulings of the khalifate will be carried out. None of the Imams of the Community disagree about the obligatory nature of having such a leader, except for what is related from al-Aamm (lit. the Deaf), who lived up to the meaning of his name and was indeed deaf to the Shari’a, and those who take his position who say that the khalifate is permitted rather than mandatory if the Community undertakes all their obligations on their own without the need for a ruler to enforce them” (Belwey, Tafsir, 2003, p. 203).

What follows is that caliphate is an obligatory and inevitable phase of the political action of the Muslim community. It is a historical necessity, even if any other form of governance can fulfill all assumptions of Sharia law. Moreover, caliphate can only be legitimized as sacrum if it realizes specific aims and achieves them by the implementation of strictly defined measures. Any departure from these conditions excludes further Quranic legitimacy of governance and automatically demands its rejection and eradication.

A separate aspect and at the same time the weakest factor in the propaganda use of the proclamation of the caliphate was the caliph himself, until recently a leader of a small organization, neither having a substantial degree of war charisma nor ideological recognition in the Jihadist world. The argumentation for appointing Abu Bakr Al-Baghdadi as the caliph was deduced indirectly. Firstly, Abu Mohammed Adnani, the spokesman for ISIS, stated in an audio-recorded declaration widely spread through the Internet, that neither does he know the biography of the caliph nor the criteria according to which he was selected for this position, also adding that “he meets all criteria demanded by scholars” and, what is more, named him “a man of jihad, sheikh, scholar, worker, believer, imam, eminent reformer, descendant of the prophet’s home-dwellers” (Walid, 2014). The original Arabic sources while discussing the qualifications of a candidate fit to be a caliph enumerate the following: generosity, righteousness, courage, and excellent knowledge of religion and the world. The first historical caliph Abu Bakr, as well as his three successors, fulfilled these characteristics and consequently deserved the name of “Rightly-Guided Caliphs” (ar. *Al-Khulafa-ur-Rashidun*) (Afsarrudin, 2014).

Thus, the first constitutive element is the possession of characteristics or virtues which should necessarily be proved for legitimization. The second constituent element is a consultation mechanism: shura. Shura means mutual consultations and is defined as “the collective effort for seeking objective truth” (Hasan, 1984, p. 21). We find in the Quran not just an authorization but an obligation for its use in the decision process of selecting a caliph:

“So by mercy from Allah, [O Muhammad], you were lenient with them. And if you had been rude [in speech] and harsh in heart, they would have disbanded from you. So pardon them and ask forgiveness for them and consult them in the matter. And when you have decided, then rely upon Allah. Indeed, Allah loves those who rely [upon Him]” (Quran, Al-Imran, (The family of Imran) [3:159]).

The Prophet himself has also used shura consultation mechanism. Abu Huraira indicates: „I have never seen a person who would consult his companions more often than the emissary of Allah does.” Historically, shura has been used to some extent even for the selection of the “Rightly-Guided Caliphs.” Abu Bakr, delegating caliphate to Omar, used election shura. He has not issued any written statement on the delegation of the caliphate to Omar, but consulted this with his trusted advisors who backed his choice unanimously (Suood, 2001, p. 133). That means that the use of shura for the legitimization of a caliph’s rule has religious character arising from the canon of faith, from its explanations (hadiths) as well as being a historical tradition (usus) in elections of consecutive caliphs.

The constitutive declaration for the Islamic State’s caliphate states:

“The Islamic State represented by its authorities, consisting of its leaders and board members (shura), decided to establish Islamic Caliphate (Khilafah) as a place of meeting for governor (Khalifa) for Muslims and vowed their loyalty to a sheikh, fighter, scholar, who practises what preaches to a faithful, leader, fighter, reinstated, descendant of Prophet’s family, slave of Allah, Ibrāhīm Ibn ‘Awwād Ibn Ibrāhīm Ibn ‘Alī Ibn Muhammad al-Badrī al-Hāshimī al-Husaynī al-Qurashī, according to his family name, as-Sāmurrā’ī, according to his birthplace and al-Baghdādī from place of preach and living. He accepted the vow of submission (ba’yah). Therefore he is imam and caliph for all Muslims” (This is the Promise, 2014).

The above document indicates the consultations of shura and scholars as well as pointing out all attributes that were to characterize the “Rightly-Guided Caliphs.” As a result, it was implied that the selection of Al Baghdadi as a rightful caliph had a strong legal and theological basis.

From those kinds of sources IS derives a thesis that imamah (leadership) is equally religious and political. IS claims that in contemporary times secularism separated religion from state and sharia from law system, considering the Quran a book of prayers (hymns) and declamation rather than the text of governance, law, and its implementation. Those Muslims, recognized by ISIS as apostates,

attempted to satisfy the governing tyrants (The concept, 2014). Moreover, people of today do not understand that imamah in its religious aspect cannot be adequately constituted before “people of truth” form a proper political imamah over the earth and people.

If a person of such ummah (community) tries to accept “a limited freedom in the profession of faith under the rule of infidel tyrants (ar. tawaghit), or seeks for protection against them in regard to the will of fulfillment of religious needs, he acts as if jumping from frying pan into fire. This leads to the integration of both aspects of authority – political and religious when we try to define the imamah passed on to Ibrahim, mentioned in verse (2:124) and there is no doubt that sharia includes both meanings” (The concept, 2014).

Finally, Adani – the undisputable author of the declaration “Here is the promise of Allah” and likely the author of the idea of the proclamation of the caliphate – is calling all Muslims to join the caliphate. According to the quoted interpretations, it is for them a religious obligation from the moment of the proclamation of caliphate:

“Come forth, O Muslims, to the land of the Caliphate. For you to be a shepherd over a flock of sheep in the land of Islam is better for you than to be an obeyed leader in the land of disbelief. Here, tawhīd (monotheism) is actualized. Here, walā’ and barā’ are embodied. Here, there is jihād for the cause of Allah. There is no paganism here nor any idols, no ethnic partisanship nor nationalism, no pagan democracy nor infidel secularism. There is no difference here between Arab and not Arab, nor between black and white. Here, the American is the brother of the Arab, the African is the brother of the European, and the Easterner is the brother of the Westerner. There is commanding of good and forbiddance of evil. Here, Allah’s Sharia is implemented. Here, by Allah’s grace, the religion is entirely for Allah. Here, there is an open declaration of tawhīd. Here is the land of Islam. Here is the land of the Caliphate” (al-Furqān Media, 2015).

Prophecy

An essential part of IS ideology, finding a later reflection in propaganda, was a reference to an apocalyptic prophecy in a hadith describing some of the events of the Malahim (what is sometimes referred to as Armageddon in English), where

the most significant battle between Muslims and the crusaders (the West/the enemy) takes place.

There are several elements of the prophecy adopted as crucial by the IS propaganda. Firstly, the place itself – Dābiq – is an area in Northern Syria. Occupation and control over this territory were to fulfill the underlying assumptions of the prophecy – the location of an apocalyptic battle controlled by Muslims. Hence the name of Dabiq – ISIS’ Propaganda Magazine. There are references in propaganda materials to the “The Dābiq Appointment” e. g.:

“So do not rejoice, o America. You will continue to assemble your forces and that of your crusader allies until you step into the arena of Dābiq, wherein you will be crushed and defeated. This is the promise of Allah; indeed Allah does not fail in His promise” (Say to those, 2014).

A video message published by wilayah Niniwa “The Dābiq Appointment” (New video, 2015), shows the final battle with armies in the West including IS tanks advancing toward Rome, etc.

Conquering the Dābiq by the Turkish army in October 2016 was a hard hit to the propaganda of caliphate. Also, Aamaq, the central news agency of IS, is called after a town adjoining Dābiq. According to hadith, „the Hour will not be established until the Romans land at al-A’maq or Dābiq (two places near each other in the northern countryside of Halab). Then an army from al-Madinah of the best people on the earth at that time will leave for them” (Sahih Musli, Book 41).

Huddud

A critical element of IS legitimization is proving that this state is led strictly according to the rules defined by the Quran and hadiths, and at the same time rejects fiqh (jurisprudence) in compromising versions and interpretations. So again, IS did not need to do much in the area of the promotion of values. The literal understanding of the Quran and hadiths, a rejection of any compromises with the values of the Western world were promoted through years in Salafist and Wahabbist mosques around the world. During the preaching, the followers were called to comply with fundamental values, to reject hypocrisy, which is distinctive to “moderate” interpretations, and to act according to the provisions of the Quran.

Thus, the Islamic State, implementing several basic rules and promoting the fact of their realization, responded to the demand of a multimillion population

of people subjected to Salafist indoctrination all over the world, especially in Western Europe. Al-Adnani, the spokesman of IS, has been speaking about those values, pointing out the measures of victory which already took place, because for the first time in modern history IS realized something that other organizations just proposed.

“We achieved victory the day we declared walā’ and barā’, crushed the idols, proclaimed tawhīd in every masjid, street, and place, stoned the adulterer, killed the sorcerer, amputated the hand of the thief, flogged the drunkard, and returned virtue to the Muslims’ women through hijab. We achieved victory the day we broke the ballot boxes and appointed a caliph through ammunition boxes and by striking necks. We achieved victory the day we established prayer, gave zakāh, ordered the good, and forbade the evil” (al-Furqān Media, 2015).

In every town taken by IS troops during the territorial expansion of the caliphate, the administrative structure for collecting and distributing zakat was immediately implemented. IS propaganda was publicizing photos taken during certain operations and presented info-graphs with statistical data (Collecting Zakat, 2015). Similarly, the execution of penalties, envisaged in the Quran for certain crimes, such as theft, adultery, spreading depravity on earth (treated as thuggery), was implemented. For example, „the woman and the man guilty of adultery or fornication – flog each of them with a hundred stripes” (Quran, An Nur [24:2]). The Islamic State tried to document all of its public executions – flogging, adulterers, decapitations, cutting off arms – not to shock with violence, but to provide proof that it realizes the Quran’s provisions accurately and literally. The purpose of this was an indication of the purity of worship, placed in opposition to its distortion in those Muslim countries where huddud is not applied.

Reprisal (kisah)

From the beginning of the military intervention by the US-led coalition, the Islamic State has presented itself as an executor of the Quranic rule of reprisal – kisah performed on behalf of the attacked and bombed population. “And if you punish, then punish them with the like of that with which you were afflicted” (Quran, An Nahl [16:126]).

It was and still is one of the essential elements of IS’ propaganda, especially when shrinking territory did not allow developing other elements. Every act

of violence in the West, every terrorist attack, including the attacks on 15th November in Paris, was advertised in IS' propaganda as a reprisal for military operations and bombing conducted by the coalition. The movie "Healing the Believers Chests" can serve as a showcase (Healing, 2015). It presents the execution of a Jordanian pilot who was burnt alive for taking part in air raids on Raqqa. An implicit IS' message, intended for recruitment, was to indicate that only IS is capable of shooting down a coalition airplane and of taking revenge on the enemy inaccessible to other military groups. Similarly, the attacks in Western Europe are a case in point.

The essential elements standing behind the successes of Islamic State's propaganda are at the same time the factors influencing its potential failure. Questioning the legitimization of caliphate proclamation by jihadist ideologists constrained the flow of fighters to IS and prevented the Somali Al Shabab, an Islamic Maghreb Al-Khaida groups and Syrian Nusra (and its consecutive emanations) from joining IS. Losing territory, including the area connected with the apocalyptic prophecy, undermines the theological legitimization of caliphate. Shrinking territory makes it de facto impossible to realize an actual state governed by sharia and limits the abilities to postulate state – and this makes IS not different from other groups – just posing changes without abilities to implement them. Similarly, limitations in military capabilities reduce IS attractiveness for migrants from Western Europe, whom the role of conquerors and soldiers of globnetal caliphate would suit very well, but not the part of pursued guerillas.

Sums distributed by the Zakah Center (Sums distributed, 2016)



Bibliography

- „Archeology in Syria” Facebook fanpage, source: <https://web.facebook.com/Archaeology.in.Syria/> [accessed 18 August 2018].
- (Mini)Słownik BBN: propozycje nowych terminów z dziedziny bezpieczeństwa (eng. National Security Bureau’s (Mini)Dictionary: proposals for the new terms in the field of security) (2015), source: <http://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html> [accessed 20 September 2018].
- #Unite4Heritage campaign launched by UNESCO Director-General in Baghdad, 28 March 2015, źródło: <http://whc.unesco.org/en/news/1254> [accessed 20 August 2018].
- About the cPPP (2016, July), European Cyber Security Organization, source: <https://ecs-org.eu/cppp> [accessed 18 July 2018].
- Active Shooter – How to Respond. (2008). Washington DC: U.S. Department of Homeland Security, p. 2. source: https://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf [accessed 19 July 2018].
- Active Shooter How to Respond, DHS.gov, (2008), source: https://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf [accessed 15 July 2018].
- Active Shooter Incidents in the United States in 2016 and 2017, the Advanced Law Enforcement Rapid Response Training (ALERRT) Center at Texas State University and the Federal Bureau of Investigation, U.S. Department of Justice, Washington, D.C. 2018.
- Advertisement of clothing with Jihadi motifs, source: producer’s website <https://plus.google.com/115752447286669315337/about> [accessed 25 August 2018]
- Afsarrudin A. (2014), *The Pretender-Caliph and Islamic History: The Truth about Abu Bakr al-Baghdadi*, ABC Religion and Ethics, 16th July 2014, source: <http://www.abc.net.au/religion/articles/2014/07/16/4047157.htm> [accessed 27 August 2018]
- Aggarwal Neil K. (2010), *How are Suicide Bombers Analysed in Mental Health Discourse? A Critical Anthropological Reading*, “Asian Journal of Social Science”. Vol. 38, No. 3, 2010.
- Al-Adnānī al-Shāmī, A.M. (2014), *This Is the Promise Of God*, audio record, of 29 June 2014, source: <https://azelin.files.wordpress.com/2014/06/shaykh-abc5ab-mue1b8a5ammad-al-e28098adnc481nc4ab-al-shc481mc4ab-22this-is-the-promise-of-god22.mp3>,

- transcript source: <https://azelin.files.wordpress.com/2014/06/shaykh-abc5ab-mue1b8a5ammad-al-e28098adnc481nc4ab-al-shc481mc4ab-22this-is-the-promise-of-god22-en.pdf> [accessed 22 August 2018].
- al-Furqān Media presents a new audio message from the Islamic State's Shaykh Abū Muḥammad al 'Adnānī al-Shāmī: "So They Kill and Are Killed"* (2015), source: <https://jihadology.net/2015/03/12/al-furqan-media-presents-a-new-audio-message-from-the-islamic-states-shaykh-abu-mu%E1%B8%A5ammad-al-adnani-al-shami-so-they-kill-and-are-killed/>, transcript source: <https://khilafahtimes.wordpress.com/2017/08/21/so-they-kill-and-are-killed/> [accessed 22 August 2018].
- Al-Muhājir A.H. (2007), *Qul mūtū bi-ghayz ikum*, Muassasat al-Furqān, 5 May 2007, transcript in Majmu'.
- Animated propaganda cartoon depicting the Hamas – Fatah conflict, using inspirations from the Walt Disney film „The Lion King”* (2007), source: Memri TV materials, source: <https://www.youtube.com/watch?v=3RxtBBSZ5js> [accessed 25 August 2018].
- Archetti C. (2015)., *Terrorism, Communication and New Media: Explaining Radicalization in the Digital Age*, "Perspectives On Terrorism", vol. 9, no. 1.
- Arenstein S., 1986. *The KGB and Soviet Disinformation*, and: *Sovieticus: American Perceptions and Soviet Realities* (review), SAIS Rev. 6, <https://doi.org/10.1353/sais.1986.0061>, [accessed 25 August 2018].
- Around 130,000 Muslims have attended the biggest Khilafah conference in Islamic history in Bung Karno stadium in Jakarta, Indonesia*, 3 June 2013, source: <http://www.hizb.org.uk/real-change/around-130000-muslims-have-attended-the-biggest-khilafah-conference-in-islamic-history-in-bung-karno-stadium-in-jakarta-indonesia/> [accessed 22 August 2018].
- Belwey A. H., Tafsir al-Qurtubi, *Classical-Commentary of the Holy Quran*, Dar AI Taqwa Ltd. 2003.
- Berger J. (2015). *How terrorists recruit online (and how to stop it)*, Brookings. source: <https://www.brookings.edu/blog/markaz/2015/11/09/how-terrorists-recruit-online-and-how-to-stop-it/> [accessed 30 July 2018].
- Bew J. (2014), *The Real Origins of Realpolitik*, "The National Interest", source: <https://nationalinterest.org/article/the-real-origins-realpolitik-9933> [accessed 20 September 2018].
- Biała Księga Bezpieczeństwa Narodowego RP* (2013), (eng. White Book of the National Security of the Republic of Poland), source: <http://www.bbn.gov.pl/download/1/20897/WhiteBookNationalSecurityPL2013.pdf>, Warsaw BBN [accessed 20 September 2018].
- Bjelopera, J., Bagalman, E., Caldwell, S., Finklea, K. and McCallion, G. (2013). *Public Mass Shootings in the United States: Selected Implications for Federal Public Health and Safety Policy*. Congressional Research Service.
- Blair J. Pete, & Schweit K. W. (2014). *A Study of Active Shooter Incidents, 2000 – 2013*. Texas State University and Federal Bureau of Investigation, U.S. Department of Justice, Washington D.C. 2014.

- Bonchek M. (2016), *How to Build a Strategic Narrative*, „Harv. Bus. Rev”, source: <https://hbr.org/2016/03/how-to-build-a-strategic-narrative> [accessed 23 July 2018].
- Byman D. (2017), *Beyond Iraq and Syria: ISIS' ability to conduct attacks abroad*, Brookings, source: <https://www.brookings.edu/testimonies/beyond-iraq-and-syria-isis-ability-to-conduct-attacks-abroad/> [accessed 23 July 2018].
- Castells M. (2005), *The Network Society: from Knowledge to Policy* [in:] Castells M., Cardoso G. (ed.), *The Network Society From Knowledge to Policy*, John Hopkins Center for Transatlantic Relations, Washington.
- Castells, M. (2010). *The rise of the network society*, 2nd ed. Cambridge MA: Wiley-Blackwell.
- Certifications (2018), Global Information Assurance Certification, source: <https://www.giac.org/certifications> [accessed 5 July 2018].
- Charter of the International Military Court*, London 8 August 1945, https://mswia.gov.pl/ftp/OCK/dokumenty_Prawo_MPH/1945_8_VIII_Porozumienie_miedzynarodowe.pdf [accessed 17 August 2018].
- Chatfield A., Reddick C. and Brajawidagda U. (2015), *Tweeting propaganda, radicalization and recruitment: Islamic state supporters multi-sided Twitter networks*, Research Online, source: <http://ro.uow.edu.au/eispapers/5029/> [accessed 18 July 2018].
- Chiodi S. (2007), *Iraq Project: the Virtual Museum of Baghdad*, source: https://www.researchgate.net/publication/29686276_Iraq_Project_the_Virtual_Museum_of_Baghdad [18 August 2018].
- Collecting Zakat in Falluja*, source: www.justpaste.it/zakat_falluja [archived, currently unavailable, accessed 11 January 2015].
- Corner E., Gill, P. (2015), *A False Dichotomy? Mental Illness and Lone-Actor Terrorism*, „Law and Human Behavior”, Vol. 39, No. 1, 2015.
- Crime in the U.S.* (2016), Federal Bureau of Investigation, source: <https://ucr.fbi.gov/crime-in-the-u.s/2016> [accessed 6 July 2018].
- Cronin A. K., Ludes J. M. (ed.) (2004), *Attacking Terrorism. Elements of a Grand Strategy*, Georgetown: Georgetown University Press.
- Cybersecurity Certifications | Information Security Certifications | (ISC)²* (2018), International Info System Security Certification Consortium, source: <https://www.isc2.org/Certifications> [accessed 3 July 2018].
- Cybersecurity Insurance* (30 June 2016), U.S. Department of Homeland Security, source: <https://www.dhs.gov/cybersecurity-insurance> [accessed 13 July 2018].
- Danti M., Branting S., Paulette T., Cuneo A. (2015), *Report on the Destruction of the Northwest Palace at Nimrud*, source: http://www.asor-syrianheritage.org/wp-content/uploads/2015/05/ASOR_CHI_Nimrud_Report.pdf [accessed 18 August 2018].
- Darczewska J. (2015), *The devil is in the details. Information warfare in the light of Russia's military doctrine*, Warsaw: OSW, source: https://www.osw.waw.pl/sites/default/files/pw_50_ang_the-devil-is-in_net.pdf, [accessed 20 September 2018].
- Darke D. (2014), *How Syria's ancient treasures are being smashed*, source: <https://www.bbc.com/news/magazine-28191181> [accessed 17 August 2018]

- Database, INTERPOL (2018), source: <https://www.interpol.int/Crime-areas/Works-of-art/Database> [accessed 18 August 2018].
- Dean S. (2017), *ISIS blows up the Tetrapylon and Roman Amphitheatre in the ancient city of Palmyra after recapturing it from the Syrian Army*, source: <http://www.dailymail.co.uk/news/article-4139568/ISIS-blows-Tetrapylon-Roman-Amphitheatre-Palmyra.html> [accessed 17 August 2018].
- Dearden L. (2014), *What causes people to commit mass murder?*, The Independent, source: <https://www.independent.co.uk/news/science/what-causes-people-to-commit-mass-murder-9402791.html> [accessed 18 August 2018].
- Deen T. (2014), *Despite 13-Year Deadlock, UN Makes Headway Fighting Terrorism*, <http://www.ipsnews.net/2014/01/despite-13-year-deadlock-u-n-makes-headway-fighting-terrorism/> [accessed 15 August 2018].
- Denning D. E. (2014), *Framework and principles for active cyber defense*, „Computers & Security”, 40, <http://doi.org/10.1016/j.cose.2013.11.004> [accessed 18 July 2018].
- Detsch J., *Islamic State adds smartphone app to its communications arsenal*, The Christian Science Monitor, 3 December 2015, source: <https://www.csmonitor.com/World/Passcode/2015/1203/Islamic-State-adds-smartphone-app-to-its-communications-arsenal> [accessed 30 September 2018].
- Diamond E., *The Media Show: The Changing Face of the News, 1985–1990*, MIT Press Cambridge, 1991.
- Doktryna cyberbezpieczeństwa RP* (2015), (eng. Cybersecurity Doctrine of the Republic of Poland), source: <https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf> [accessed 20 September 2018].
- Dorn, M. (2016), *20 Active Shooter and Active Killer Prevention Strategies*, Global CTI, source: <http://gcti.com/20-active-shooter-and-active-killer-prevention-strategies/> [accessed 18 July 2018].
- ECSO Public Session*, 20 June 2018, source: <https://ecs-org.eu/press-releases/ecso-public-session> [accessed 18 July 2018].
- Egelman S., Harbach M., & Peer E. (2017). *Behavior Ever Follows Intention?*, Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems – CHI 16, 5357–5261, source: <http://doi.org/10.1145/2858036.2858265> [accessed 18 July 2018].
- Egipt: Bezcenne skarby skradziono w Kairze w czasie rewolucji* (2011), Polska the Times, source: <https://polskatimes.pl/egipt-bezcenne-skarby-skradziono-w-kairze-w-czasie-rewolucji/ar/369193> [accessed 17 August 2018].
- Fake: US Sells Ukraine Defective Javelins*, 2018, source: StopFake.org [accessed 18 July 2018].
- Feldman J. (2016), *New psychological study finds traits common to ,active shooters’*, Journalist’s Resource, source: <https://journalistsresource.org/studies/government/criminal-justice/role-psychological-traits-mass-shootings> [accessed 25 July 2018].
- Francescani C. (2016, April 26), *Ransomware Hackers Hold U.S. Police Departments Hostage*, source: <https://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746> [accessed 18 July 2018].
- Frei D., Sicherheit (1977), *Grundfragen der Weltpolitik*, Stuttgart: Verlag W. Kohlhammers.

- Fukuyama F. (1992), *The End of the history and the last man*, New York: Free Press.
- Galeotti M. (2016), *Opinion | Putin Is Waging Information Warfare. Here's How to Fight Back*, N. Y. Times, source: <https://www.nytimes.com/2016/12/14/opinion/putin-is-waging-information-warfare-heres-how-to-fight-back.html> [accessed 25 July 2018].
- Galeotti M. (2017), *Controlling Chaos: How Russia manages its political war in Europe*, ECRF EU, source: https://www.ecrf.eu/publications/summary/controlling_chaos_how_russia_manages_its_political_war_in_europe [accessed 25 July 2018].
- Gambetto D., Hertog S. (2016), *Engineers of Jihad: The Curious Connection between Violent Extremism and Education*, Princeton University Press.
- Gańczak F. (2018), *Złote zniwa*, Newsweek, source: <https://www.newsweek.pl/swiat/skarby-starozytnosci-na-europejskich-rynkach/zk59tkv> [accessed 17 August 2018].
- Ganor B. (2002) *Defining Terrorism*, „Media Asia”, 29:3, 123–133, DOI: 10.1080/01296612.2002.11726675.
- Geller A. (2008), *NATO wysadziło posąg Buddy w Afganistanie*, Dziennik Gazeta Prawna, source: <http://wiadomosci.dziennik.pl/swiat/artykuly/75027,nato-wysadzilo-posag-buddy-w-afganistanie.html> [accessed 17 August 2018].
- Gitlin T. (1980), *The Whole World is Watching: Mass Media in the Making & Unmaking of the New Left*, Berkeley, University of California Press.
- Goban-Klas T., Sienkiewicz P. (1999), *Spółeczeństwo informacyjne: szanse, zagrożenia, wyzwania* (eng. Information Society: Opportunities, Threats, Challenges), Kraków: Wydawnictwo Fundacji Postępu Telekomunikacji.
- Goldschmidt, M. (2018, March 8), *Social Engineering is the new norm in hacking*, source: <https://www.cso.com.au/article/634433/social-engineering-new-norm-hacking/> [accessed 22 July 2018].
- Goodman T. (2018), *10 Signs of an Active Shooter – Alamom*, Alamom Consulting, Inc., source: <http://alamom.com/about-us/blog/10-signs-active-shooter-alamom/> [accessed 23 July 2018].
- Gorman R. F., *Great Debates at the United Nations: An Encyclopedia of Fifty Key Issues 1945–2000*, Santa Barbara, CA 2001.
- Gratian M., Bandi S., Cukier M., Dykstra J., & Ginther, A. (2017), *Correlating human traits and cyber security behavior intentions* „Computers & Security”, 73, source: <http://doi.org/10.1016/j.cose.2017.11.015> [accessed 23 July 2018].
- Grinberg D. (1994), *Ruch anarchistyczny w Europie Zachodniej 1870–1914* (eng. Anarchist movement in Western Europe 1870–1914), Warsaw: PWN Publishing House.
- Hafiz Y. (2014), *ISIS Destroys Shiite Mosques And Shrines In Iraq, Dangerously Fracturing Country*, source: https://www.huffingtonpost.com/2014/07/07/isis-destroys-shiite-mosque_n_5564373.html? [accessed 17 August 2018].
- Hallahan K., Holtzhausen D., Ruler B. van, Verčič D., Sriramesh K. (2007), *Defining Strategic Communication*, „Int. J. Strateg. Commun.”, 1, 3–35, source: <https://doi.org/10.1080/15531180701285244> [accessed 22 July 2018].
- Hasan A., *The Doctrine of 'Ijma' in Islam*, The Islamic Research Institute, Islamabad, Pakistan, 1984.

- Healing the believers' chests* (2015), source: <https://inspirationfromzion.com/2015/02/07/healing-the-believers-chests/> [accessed 27 August 2018].
- Hellman M., Wagnsson, C. (2017), *How can European states respond to Russian information warfare? An analytical framework*, *Eur. Secur.* 26, 153–170. <https://doi.org/10.1080/09662839.2017.1294162>
- Himma, K. E., & Dittrich, D. (2005). Active Response to Computer Intrusions. *SSRN Electronic Journal*, 664–681. <http://doi.org/10.2139/ssrn.790585> [accessed 22 July 2018].
- Hizb ut-Tabriz*, Jane's Terrorism and Insurgency Center, October 26, 2009.
- Hoffman B. (1999), *Oblicza terroryzmu* (English edition: Inside Terrorism), Warsaw: Bertelsmann Media.
- Hunter E. and Pernik P. (April 2015), *The Challenges of Hybrid Warfare*, ICDS,, source: <https://icds.ee/the-challenges-of-hybrid-warfare/> [accessed 20 September 2018].
- ICOM – International Council of Museums, source: <http://www.icom.co.jp/world/>. [accessed 17 August 2018].
- Information Sharing*, 18 May 2018, Department of Homeland Security, source: <https://www.dhs.gov/topic/cybersecurity-information-sharing> [accessed 16 July 2018].
- Intergovernmental Panel on Climate Change*, source: <http://www.ipcc.ch/> [accessed 25 July 2018].
- International Association of Privacy Professionals* (2018), International Association of Privacy Professionals, source: <https://iapp.org/certify/> [accessed 5 July 2018].
- ISIS blows up Temple of Nabu in Nimrud* (2016), source: <https://www.apollo-magazine.com/isis-blows-up-temple-of-nabu-in-nimrud/> [accessed 17 August 2018].
- Jagielski W. (2007), *Pakistańskim talibom nie udało się zniszczyć skalnego posagu Buddy*, „Gazeta Wyborcza”, source: <http://wyborcza.pl/1,86669,4486293.html> [17 August 2018].
- James N., (2015), *Is Violent Crime in the United States Increasing?*, Report Number: R44259, Congressional Research Service, source: <https://fas.org/sgp/crs/misc/R44259.pdf> [accessed 18 July 2018].
- Jenkins B. M. (1976), *International Terrorism: A New Mode of Conflict* (in:) „International Terrorism and World Security”, Carlton D., Schaerf C. (ed.), Lawrence, Mass.: Harvard University Press.
- Johnson R. (2018), *Hybrid War and Its Countermeasures: A Critique of the Literature* „Small Wars Insur.”, 29, 141–163, source: <https://doi.org/10.1080/09592318.2018.1404770> [accessed 18 July 2018].
- Jytte Klausen (2015), *Tweeting the Jibad: Social Media Networks of Western Foreign Fighters in Syria and Iraq*, *Studies in Conflict & Terrorism*, 38:1, 1–22, DOI: 10.1080/1057610X.2014.974948 [accessed 20 July 2018].
- Kaldor M. (2013), *In defence of new wars*, „Stability. International Journal of Security & Defence”, source: <https://www.stabilityjournal.org/articles/10.5334/sta.at/> [accessed 16 August 2018].

- Kaldor M., 2013, *In defence of new wars*, „Stability. International Journal of Security & Defence”, source: <https://www.stabilityjournal.org/articles/10.5334/sta.at/> [accessed 16 August 2018].
- Kania J., Kramer M. (2011), *Collective Impact*, „Stanf. Soc. Innov. Rev.”, 9(1).
- Karouny M. (2012), *Large part of ancient souk in Syria's Aleppo in ashes: activists*, source: <https://www.reuters.com/article/us-syria-crisis-idUSBRE88J0X720120930> [accessed 18 August 2018].
- King P., (2008), *Is the Taliban an insurgent or terrorist organisation? Video interview with Ahmed Rashid*, „NATO Review”, NATO, source: www.nato.int/docu/review/2008/04/ap_cost/en/index.htm [accessed 22 September 2018].
- Klausen J. (2015), *Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq*, „Studies in Conflict & Terrorism”, 38(1).
- Krombholz K., Hobel H., Huber M., & Weippl E. (2015), *Advanced Social Engineering Attacks*, „Journal of Information Security and Applications”, 22.
- Krouse W., Richardson D. (2015), *Mass Murder with Firearms: Incidents and Victims, 1999–2013*, Report Number: R44126, Congressional Research Service, source: <https://fas.org/sgp/crs/misc/R44126.pdf> [accessed 18 July 2018].
- Kulik, T. (2018, January 29), *Why The Active Cyber Defense Certainty Act Is A Bad Idea*, source: <https://abovethelaw.com/2018/01/why-the-active-cyber-defense-certainty-act-is-a-bad-idea/> [accessed 14 July 2018].
- Kurlantzick J. (2007), *Charm Offensive*, New Haven: Yale University Press.
- Lacroix F. (2018), *Edouard Philippe dévoile 60 mesures contre la radicalisation*, Les Echos, source: https://www.lesechos.fr/23/02/2018/lesechos.fr/0301339433473_edouard-philippe-devoile-60-mesures-contre-la-radicalisation.htm [accessed 22 August 2018].
- Laqueur W. (1986), *Reflections on Terrorism*, Foreign Affairs, Fall 1986, vol. 65, No. 1.
- Lee R. (2015), *The Sliding Scale of Cyber Security*, SANS Institute, source: <https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240> [accessed 12 July 2018].
- Lindley-French J. (2014), *NATO's Post-2014 Strategic Narrative*, NATO Def. Coll. 11.
- Lindros K., Tittel E. (2016, May 4), *What is cyber insurance and why you need it*, source: <https://www.cio.com/article/3065655/cyber-attacks-espionage/what-is-cyber-insurance-and-why-you-need-it.html> [accessed 18 July 2018].
- Cyber Risk Cyber Secure* (2016), Lloyds, London, U.K.
- Closing the Gap: Insuring your business against evolving cyber threats* (2017), Lloyds, KPMG, & DAC Beachcraft, source: <https://www.lloyds.com/about-lloyds/what-lloyds-insures/cyber/cyber-risk-insight/closing-the-gap> [accessed 18 July 2018].
- Louvre Museum Online Tours* (2018), source: <https://www.louvre.fr/en/visites-en-ligne> [accessed 18 August 2018].
- Marshall R.D., Bryant R.A., Amsel L., Eun Jung Suh, Cook J.M., Neria Y. (May 2007), *The psychology of ongoing threat: Relative risk appraisal, the September 11 attacks*,

- and terrorism-related fears*, „American Psychologist” 62, no. 4, PsycARTICLES, EBSCOhost [accessed 29 July 2018].
- Marthoz J.-P., *Terrorism and the Media A Handbook for Journalists*, source: <http://unesdoc.unesco.org/images/0024/002470/247074E.pdf> [accessed 30 September 2018].
- Economic Impact of Cyber Crime-No Slowing Down*, McAfee, & Center for Strategic and International Studies (2018), source: <https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf> [accessed 20 July 2018].
- Mendoza M., Alleruzzo M. Janssen B. (2016), *Oldest Christian monastery in Iraq is razed*, source: <https://eu.usatoday.com/story/news/world/2016/01/20/oldest-christian-monastery-iraq-razed-isil/79075182/> [accessed 17 August 2018].
- Moore, J. (2018). *Md. Gov. Hogan on Capital Gazette shooting | WTOP*, source: <https://wtop.com/maryland/2018/07/we-should-have-been-able-to-stop-him-md-gov-hogan-on-suspected-newspaper-gunmans-threats/> [Accessed 20 July 2018].
- Morgan S. (ed.). (2017), *2017 Cybercrime Report*, Cybersecurity Ventures, source: <https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf> [accessed 21 July 2018].
- Morton R., Hiltz M.A., (ed.) (2008), *Serial Murder: Multi-Disciplinary Perspective for Investigators* Federal Bureau of Investigation, source: <https://www.fbi.gov/stats-services/publications/serial-murder> [accessed 22 July 2018].
- Nelson P. S., Scott, J. L. (1992), *Terrorism and the Media – an empirical analysis*, „Defence Economics”, 3(4).
- New video message from The Islamic State: “The Dābiq Appointment – Wilāyat Nīnawā”*, 11 December 2015, source: <https://jihadology.net/2015/12/11/new-video-message-from-the-islamic-state-the-dabiq-appointment-wilayat-ninawa/> [accessed 27 August 2018].
- Nichol J. (2009), *Russia-Georgia Conflict in August 2008: Context and Implications for U.S. Interests*, CRS Wahington, source: <https://fas.org/sgp/crs/row/RL34618.pdf> [accessed 11 November 2018].
- Nye J. S. (2004), *Soft Power and American Foreign Policy*, „Political Science Quarterly”, Vol. 119, No. 2.
- Ochrona dóbr kultury według konwencji podpisanej w Hadze 14 maja 1954 roku* (eng. Protection of cultural assets according to the Hague Convention of May 14th, 1954), source: http://www.unesco.pl/fileadmin/user_upload/pdf/Haga.pdf/ [accessed 17 August 2018].
- Orehek E., Fishman S., Dechesne M., Doosje B, Kruglanski A. W., Cole A. P. ; Saddler B., Jackson T. (2010), *Need for Closure and the Social Response to Terrorism*, „Basic and Applied Social Psychology”, 32:4, 279–290, DOI: 10.1080/01973533.2010.519196.
- Overill R.E. (2004), *Reacting to cyber intrusions: the technical, legal and ethical dilemmas*, „Journal of Financial Crime”, 11(2), source: <http://doi.org/10.1108/13590790410809095> [accessed 13 July 2018].
- Partnership for Protection* (2003), InfraGard, source: <https://www.infragard.org/> [accessed 19 July 2018].

- Perešin A. (2007), *Mass Media and Terrorism*, „Medijska istraživanja: znanstveno-stručni časopis za novinarstvo i medije” 1(2007).
- Preliminary Semiannual Uniform Crime Report January–June, 2017* (2017), Federal Bureau of Investigation, source: <https://ucr.fbi.gov/crime-in-the-u.s/2017> [accessed 6 July 2018].
- Projekt „Doktryny bezpieczeństwa informacyjnego RP (2015), (eng. Project of the Information Security Doctrine of the Republic of Poland), source: https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf [accessed 20 September 2018].
- Propaganda material by ISIS after Paris attacks as reported by NYT* (November 2015), source: <http://www.nytimes.com/video/world/100000004166589/isis-video-appears-to-show-assailants.html> [accessed 05 August 2018].
- Puyvelde D. Van (2015), *Hybrid war: does it even exist?*, source: <http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm> [accessed 22 September 2018].
- Quran: Al-Imran (The family of Imran) [3:159]; An Nahl (16:126); An Nur (The Light (24:2), (24:55).
- Rapoport D. C. (2004), *The Four Waves of Modern Terrorism* [in:] Kurth Cronin A., Ludes J.M. (ed.), *Attacking Terrorism. Elements of a Grand Strategy*, Georgetown Press.
- Rapoport D. C., *The Four Waves of Rebel Terror and September 11*, *Anthropoetics* 8, no. 1 (Spring/Summer 2002), source: <http://www.anthropoetics.ucla.edu/ap0801/terror.htm> [accessed 15 August 2018].
- Rauert T. (Fall 2005), *The Next Threat from Central Asia*, „Journal of International Security Affairs”, No. 9.
- Red Lists* (2018), ICOM, source: <http://icom.museum/en/activities/heritage-protection/red-lists/> [accessed 17 August 2018].
- Reitan E. (2010), *Defining Terrorism for Public Policy Purposes: The Group-Target Definition*, „Journal of Moral Philosophy”, vol. 7, no. 2, July 2010, EBSCOhost, doi:10.1163/174552409X12574076813513.
- Richards D. (2014). *The Twitter jihad: ISIS insurgents in Iraq, Syria using social media to recruit fighters, promote violence*, ABC News, source: <http://www.abc.net.au/news/2014-06-20/isis-using-social-media-to-recruit-fighters-promote-violence/5540474> [accessed 20 July 2018].
- Roselle L., Miskimmon A., O’Loughlin B. (2014), *Strategic narrative: A new means to understand soft power*, „Media War Confl.” 7, 70–84, source: <https://doi.org/10.1177/1750635213516696> [accessed 21 July 2018].
- Ross P. (2015), *ISIS Destroys 3,000-Year-Old Mosul Museum Artifacts With Sledgehammer, Pickaxes*, source: <https://www.ibtimes.com/isis-destroys-3000-year-old-mosul-museum-artifacts-sledgehammer-pickaxes-video-1829270> [accessed 17 August 2018].
- Safety and Security for the Business Professional Traveling Abroad. Safety and Security for the Business Professional Traveling Abroad* (2016), Federal Bureau of Investigation, source: <https://www.fbi.gov/file-repository/business-travel-brochure.pdf/view> [accessed 10 July 2018].

- Sahih Muslim*, Book 41, Hadith 6924, source: <https://sunnah.com/muslim/54> [accessed 27 August 2018].
- Say To Those Who Disbelieve, You Will Be Overcome*, An Address by the Official Spokesman of the Islamic State The Mujāhid Shaykh Abū Muhammad al-Adnānī ash-Shāmī (2015), source: <https://jihadology.net/2015/10/13/new-audio-message-from-the-islamic-states-shaykh-abu-mu%E1%B8%A5ammad-al-adnani-al-shami-say-to-those-who-disbelieve/>, transcript source: https://archive.org/stream/SayToThoseWhoDisbelieveYouWillBeOvercome/say%20to%20those%20who%20disbelieve%20you%20will%20be%20overcome_djvu.txt [accessed 27 August 2018].
- Schildkraut J., Elsass J. (2016), *Mass Shootings: Media, Myths, and Realities*, ABC-CLIO, LLC, Westport, source: ProQuest Ebook Central [accessed 6 July 2018].
- Schildkraut J., Elsass J., Kimberly M. (2017), *Mass shootings and the media: why all events are not created equal*, „Journal of Crime and Justice”, 41:3, 223–243, source: DOI: 10.1080/0735648X.2017.1284689 [accessed 17 July 2018].
- Schultz, J. (2018). Pre-attack indicators: Do we finally have a profile on active shooters?. [online] PoliceOne. Available at: <https://www.policeone.com/active-shooter/articles/477019006-Pre-attack-indicators-Do-we-finally-have-a-profile-on-active-shooters/>
- Shane, S. (2018), *Facebook Removes More Accounts Tied to Russian ‘Troll Factory’*, N.Y. Times, source: <https://www.nytimes.com/2018/04/03/business/facebook-russian-trolls-removed.html> [accessed 25 July 2018].
- Sheikh Abu Umar al-Baghdadi explains the Aqeedah of IS* (2015), English translation, source: <https://www.youtube.com/watch?v=4E8GS7RQH3Q>; transcript at: <https://ansarkhilafah.wordpress.com/2015/05/19/the-aqidah-of-is/> [archived, currently unavailable, accessed 20 May 2015].
- Sheikh Abu Umar al-Baghdadi explains the Aqeedah of IS*, English translation, source (2015), source: <https://www.youtube.com/watch?v=4E8GS7RQH3Q>; transcript at: <https://ansarkhilafah.wordpress.com/2015/05/19/the-aqidah-of-is/> [accessed 20 May 2015, archived, currently unavailable].
- Silva J.R., Capellan J.A. (2018), *The media’s coverage of mass public shootings in America: fifty years of newsworthiness*, „International Journal of Comparative and Applied Criminal Justice”, source: DOI: 10.1080/01924036.2018.1437458 [accessed 25 July 2018].
- Silver J., Simons, A., Craun, S. (2018), *A Study of the Pre-Attack Behaviors of Active Shooters in the United States Between 2000 – 2013*, Federal Bureau of Investigation, U.S. Department of Justice, Washington, D.C. 20535.
- Silverman H., DiGiacomo J. Simon D. (2018), *Five dead in shooting at Capital Gazette in Annapolis, Maryland*, CNN.com, source: <https://edition.cnn.com/2018/06/28/us/annapolis-maryland-newsroom-shooting/index.html> [accessed 20 July 2018].
- Skuse A., Gillespie M., Power G., (ed.) (2011), *Drama for development: cultural translation and social change*, SAGE, Thousand Oaks, Calif.

- Smith R. (2018), *3D-printing is helping to restore the world's destroyed heritage sites*, source: <https://www.weforum.org/agenda/2018/04/3d-modelling-is-helping-to-restore-the-worlds-destroyed-heritage-sites/> [accessed 18 August 2018].
- Spaaïj R., *The Enigma of Lone Wolf Terrorism: An Assessment*, „Studies in Conflict & Terrorism”, vol. 33, no. 9, Sept. 2010, EBSCOhost, doi:10.1080/1057610X.2010.501426 [accessed 18 July 2018].
- Spicer, B. (2015), *Using Situational Awareness to Identify Pre-Attack Indicators*, „Campus Safety Magazine”, source: https://www.campussafetymagazine.com/safety/using_situational_awareness_to_identify_pre_attack_indicators/ [accessed 16 July 2018].
- Steinbach M. (2016), *ISIL Online: Countering Terrorist Radicalization and Recruitment on the Internet and Social Media*, Federal Bureau of Investigation, source: <https://www.fbi.gov/news/testimony/isil-online-countering-terrorist-radicalization-and-recruitment-on-the-internet-and-social-media-> [accessed 7 July 2018].
- Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, adopted by Heads of State and Government at the NATO Summit in Lisbon 19–20 November 2010, source: https://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf [accessed 20 August 2018].
- Sums distributed by the Zakah center in the city of Raqqah and its countryside during August 2016*, Telegram application channel of Aamaq Agency [archived, currently unavailable, accessed 10 July 2016].
- Suood T. (2001), *Biographies of the Rightly-Guided Caliphs (from the works of Ibn Katheer; at-Tabari, and as-Suyooti)*, source: https://www.islamland.com/uploads/books/en_Biographies_of_the_Rightly-Guided_Caliphs.pdf [accessed 17 August 2018].
- Szafranski, R., 1995. A Theory of Information Warfare: Preparing for 2020. *Airpower J.* 9, 56–65.
- Teperik D., Senkiv G., Bertolin G., Kononova K., Dek A. (2018), *Virtual Russian world in the Baltics*, NATO Strat. 41.
- Thatcher M., *Speech to American Bar Association*, source: <https://www.margaretthatcher.org/document/106096> [accessed 30 September 2018].
- The concept of imamah* (2014), Dabiq No. 1, 5 July 2014.
- The Implementation of Network-Centric Warfare* (2005), DoD Office of Force Transformation, source: <http://handle.dtic.mil/100.2/ADA446831> [accessed 20 August 2018].
- The North Atlantic Treaty*, Washington D.C. 4 April 1949, source: https://www.nato.int/cps/ie/natohq/official_texts_17120.htm [accessed 20 September 2018].
- The Ruling System in Islam* (2002), Hizb ut Tahrir, 5th edition, Khilafah Publications, London.
- The use of the Internet for terrorist purposes* (2012), UNODC, Vienna, source: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf [accessed 11 November 2018].

- This Is the Promise of Allah – declaration of proclamation of the Islamic State* (2014), English version, source: http://myreader.toile-libre.org/uploads/My_53b039f00cb03.pdf [archived, currently unavailable, accessed 4 August 2014].
- Thomas, T. (2004), *Russia's Reflexive Control Theory and the Military*, „J. Slav. Mil. Stud.” 17, source: <https://doi.org/10.1080/13518040490450529> [accessed 19 July 2018].
- Timeline of Syrian Chemical Weapons Activity, 2012–2018*, source: <https://www.armscontrol.org/factsheets/Timeline-of-Syrian-Chemical-Weapons-Activity> [accessed 20 August 2018].
- Tocqueville A. de, (2000), *Democracy in America*, Chicago: University of Chicago Press.
- Treverton G. F., Jones S. G. (2005), *Measuring National Power*, Santa Monica: Rand Corporation.
- U.S. Code*, source: <https://www.law.cornell.edu/uscode/text> [accessed 20 July 2018].
- U.S. Mass Shootings, all years (2013–2018)*, source: <https://www.massshootingtracker.org/data/all> [Accessed 6 July 2018].
- UNESCO Database of National Cultural Heritage Laws*, UNESCO, source: <http://www.unesco.org/culture/natlaws/> [accessed 18 August 2018].
- UNESCO Director-General condemns destruction of the Tetracylon and severe damage to the Theatre in Palmyra* (2017), UNESCO World Heritage site, source: <https://whc.unesco.org/en/news/1620/> [accessed 17 August 2018].
- United Nations Security Council Resolution 2199 (2015)*, UNESCO, source: <http://unesdoc.unesco.org/images/0023/002321/232164e.pdf> [accessed 17 August 2018].
- Automated Indicator Sharing (AIS) Fact Sheet* (2015), United States Computer Emergency Readiness Team, source https://www.us-cert.gov/sites/default/files/ais_files/AIS_fact_sheet.pdf [accessed 17 July 2018].
- Victor D. (2018), *Mass Shooters Are All Different. Except for One Thing: Most Are Men*, *Nytimes.com*, source: <https://www.nytimes.com/2018/02/17/us/mass-murderers.html> [accessed 17 July 2018].
- Vintiadis E. (2018), *Mass Shooting and the Myth of the Violent Mentally Ill*, „Psychology Today”, source: <https://www.psychologytoday.com/us/blog/minding-the-mind/201802/mass-shooting-and-the-myth-the-violent-mentally-ill> [accessed 17 July 2018].
- Walid, A. (2014), *Profile: Mysterious 'Caliph' Abu Bakr Al-Baghdadi*, Middle East Monitor, 1st July 2014, source: <https://www.middleeastmonitor.com/20140701-profile-mysterious-caliph-abu-bakr-al-baghdadi/> [accessed 27 August 2018].
- Weimann G. (2004), *www.terror.net. How Modern Terrorism Uses the Internet* (special report United States Institute of Peace), source: <http://www.usip.org/publications/wwwterrornet-how-modern-terrorism-uses-the-internet> [accessed 25 August 2018].
- Wiktorowicz Q. (2006), *Anatomy of the Salafi Movement*, „Studies in Conflict & Terrorism”, 29.
- Wojciechowski S. (2017), *Reasons of Contemporary Terrorism. An Analysis of Main Determinants*, „Radicalism and Terrorism in the 21st Century: Implications for Security”, Peter Lang AG.

- Wolf N. (2018), *Twitter suspends 235,000 accounts in six months for promoting terrorism*, The Guardian, source: <https://www.theguardian.com/technology/2016/aug/18/twitter-suspends-accounts-terrorism-links-isis> [accessed 22 August 2018].
- Wright E. (2011), *Generation Kill*, e-book, New York: Transworld Digital.
- Zuijdewijn J., Baker M. (2016), *Analysing Personal Characteristics of Lone-Actor Terrorists: Research Findings and Recommendations*, „Perspectives on Terrorism”, Vol. 10, No. 2.

Authors' notes

Quinn Harty is a sophomore at the University of Denver in Colorado majoring in International Studies and concentrating in International Security. He is a summer intern for the Terrorism Research Institute at Collegium Civitas and is absolutely thrilled to be able to spend his summer working in a field that really interests him. He hopes you find his ideas interesting.

Bianca Canal is a student at the University of Texas at Austin. She studies Philosophy, Government and American History focusing on the American Identity and how it is shaped by the government. She is working at the Terrorism Research Center in Poland to broaden her perspective in international relations and further understand the increase in terrorist activity, a phenomenon that largely shapes world politics and America's global agenda. Bianca enjoys swing dancing, outdoor activities and live music in her favorite city, Austin, Texas. Upon returning to the United States, she plans to explore careers in dance, theatre and education.

Nicole Wojtkiewicz is an undergraduate student at The University of South Carolina with an expected graduation date of May 2019. She is a Political Science and Criminal Justice double major with career interests in Law and Counter Intelligence. Nicole is an intern at the Terrorism Research Center within Collegium Civitas in Warsaw, Poland, for the summer of 2018. Her current internship project is on "Security and Society in the Information Age" with a focus on modern recruitment tactics. Nicole was eager to spend her summer in Poland due to the fact that her parents both emigrated from Poland and the majority of her family still resides there. During her time at school Nicole is the Director of Outreach for Women in Business and works for a Criminal Defense law firm.

Casey Guthrie is an undergraduate student at Michigan State University. She has an anticipated graduation date of May 2020. Her Major is Criminal Justice and her Minor is Security Management. Her career interests include law enforcement and counterintelligence. She is an intern at the Terrorism Research Center at Collegium Civitas in Warsaw, Poland. Her current project involves a research paper about security and society in the information age, with a focus on preventing mass shootings and active shooters.

Abigail Kuchek is about to start her third year at the University of Texas at Austin. She is majoring in Politics, Philosophy, and Economics and earning a certificate in Human Rights and Social Justice. Abby spent the last year researching global development indices networks at UT Innovations for peace and development and will be a 2018–19 Next Generation Scholar at the Robert Strauss Center for International Security and Law. She is also passionate about interpersonal violence advocacy and volunteers with UT Voices Against Violence and Interpersonal Violence Peer Support. Off campus, she spends her time painting, writing, and taste testing Austin's vegan ice cream offerings.

Hazal Bulut is an undergraduate student at Michigan State University, majoring in Criminal Justice. She has an anticipated graduation date in May 2020. Hazal is an intern for the summer of 2018 at the Terrorism Research Center at Collegium Civitas Warsaw, Poland. Her career interests include criminal profiling, crime scene investigation and counterintelligence.

Charles Schmidt is an undergraduate student at The Pennsylvania University. His Major Focus is Security Risk Analysis with a Minor Focus in Criminal Justice. He is a summer 2018 intern at the Terrorism Research Center within Collegium Civitas University in Warsaw, Poland. Topics of interest include Counter-Terrorism, Policing and Intelligence.

Jacob M. Schmitt is a Summer Research Intern with the Terrorism Research Center, a think tank hosted by Collegium Civitas University in Warsaw, Poland. Jake is an undergraduate Global Security Studies candidate at the University of Wisconsin-Milwaukee with a focus on Russia, Eastern Europe and Central Asia. Jake has researched the implications of nuclear arms in international relations and threats to global civil aviation from illicit arms sales.

Krzysztof Liedel, Ph.D., specialises in security management, is a lawyer, an expert in the field of international terrorism and combating it, and an expert in

information analysis, especially in the area of decision analysis. He is a trainee at the National Counterterrorism Center in the USA, the former head of the Department of Terrorist Prevention, Department of Public Security of the Ministry of Internal Affairs and Administration, former director of the Department of Homeland Security of the National Security Bureau. He is the head of the Institute for Information Analysis at Collegium Civitas, Director of the Center for Research on Terrorism CC. Lecturer at Collegium Civitas and Warsaw University. Author and co-author of many publications on international terrorism and fights against it, as well as on information analysis.

Paulina Piasecka, PhD, is an expert in the area of international terrorism and cybersecurity. She is a former senior expert in the Counter-terrorism unit of the Ministry of Interior and Administration of the Republic of Poland, and head of the unit for Non-Military Security (Department of Legal and Non-Military Affairs) at National Security Bureau, Poland. Dr Piasecka was a participant of the US State Department “International Visitor Leadership Program” in the area of cybersecurity. She is Deputy Director of the Terrorism Studies Centre at Collegium Civitas, Deputy Head of Information Analysis Institute at Collegium Civitas, and a lecturer at Collegium Civitas. She is a co-author and editor of publications on cybersecurity, information analysis, and international terrorism and counterterrorism.

Katarzyna Góralczyk, Ph.D., alumna of the Faculty of History of the Church of the Pontifical University of John Paul II in Krakow (2005); Postgraduate Study of Diplomacy and International Relations at the Jagiellonian University in Krakow (2006); the Postgraduate Study of Information Safety in the National Defence Academy in Warsaw (2007). She was awarded PhD title in 2012 at The National Security Department of the National Defence Academy in Warsaw after defending the thesis on “The protection of cultural goods by the Polish Military Contingent in the international stability operations in Iraq (2003–2008)”. Her research concentrates mainly on the international humanitarian law of armed conflicts with a particular focus on the protection of cultural heritage during armed conflicts and the cultural and social security. Since 2009 the Chairman of the Board of the Science and Culture Foundation, which realises a variety of cultural and educational projects in Malopolska. She is also a member of the commission and team for the Propagation of Humanitarian Law functioning by the main board of the Polish Red Cross in Warsaw and its branch in Krakow. A member of the Blue Shield in Krakow as well as a specialist in the Centre for Research on Terrorism Collegium Civitas.

Katarzyna Zielińska, PhD, historian, political scientist, educator. Head of the Education and Dissemination Department of the Polish Aviation Museum in Krakow. Author of many articles on the history and political parties in the United States of America, local government and museum education. In the years 2012–2018, she prepared and led many educational and cultural events and projects, such as Malopolski AirShow or Aerosabat 2016. Over last few years she has conducted and organized educational activities for various audiences, including interdisciplinary and intercultural activities, such as workshop Fly High (2015), Eskadrylla Niepodległej (2017) or workshops on 100 years of Boeing planes (2013), which were realized with funds from either the Boeing concern or the Ministry of Culture and National Heritage. In 2017, in cooperation with the Science and Culture Foundation, she conducted a series of educational classes – Muzoflight. In 2013–2018 she held classes for the high school students at the Czyzyńska Academy of Self-Government.

Wojciech Szewko, PhD, former Polish Deputy Minister of Science, is a lecturer at the Terrorism Research Centre, Collegium Civitas, assistant professor at Institute of Homeland Security, UTH, and the president of Foundation of International Cooperation and Development. He is an expert on Islamic Jihad (ideology, organisation, tactics), international terrorism, and international relations in the Middle East and Asia. Dr Szewko speaks five languages (with various level of proficiency). Previously, Dr Szewko served as a lecturer at Warsaw University, Academy of Defense, Academy of Humanities and as an expert with the National Center for Security Studies. Dr Szewko served as the president of the Polish Chinese Foundation for Communication and Cooperation. He was an advisor to the Prime Minister and the Head of the Office of Ministers and also served as Deputy Minister of Science (2003–2004).

It is our pleasure to present this unique publication – composed of papers written by talented young American students – participants in the Summer School Program “Security and Society in the Information Age” and by experts cooperating with the Terrorism Research Center at Collegium Civitas University in Warsaw, Poland.

This book is the result of the internship program held in summer of 2018 at the Terrorism Research Center which is one of the leading think-tanks in Poland with renowned experts participating in projects conducted by the Center. The main thematic focus of the internship was the changing paradigm in security. The interns looked at such important issues as cybersecurity, the prevention of mass shootings and active shooter situations through education and awareness programs, radicalization and recruitment to terrorist organizations, the role of the mass media in shaping public opinion on terrorism, the condition of democracy in the age of fake news, the evolution of modern terrorism and many more.

We hope you will find the book interesting and valuable and we cordially invite you to learn more about “Security and Society in the Information Age” programming at www.securityandsociety.org.

ISBN 978-83-61067-90-0



9 788361 067900