8-2018

Spreading Propaganda in Cyberspace: Comparing Cyber-Resource Usage of Al Qaeda and ISIS

cyberterrorism, Al Qaeda, ISIS, propaganda, cyber-resources, cyber-technologies, multiple correspondence analysis

Follow this and additional works at: <https://vc.bridgew.edu/ijcic>

Part of the [Criminology Commons](#), [Criminology and Criminal Justice Commons](#), [Information Security Commons](#), and the [Social Control, Law, Crime, and Deviance Commons](#)

Recommended Citation

Choi, Kyung-shick; Lee, Claire Seungeun; and Cadigan, Robert (2018) Spreading Propaganda in Cyberspace: Comparing Cyber-Resource Usage of Al Qaeda and ISIS, *International Journal of Cybersecurity Intelligence & Cybercrime*: 1(1), 21-39. <https://www.doi.org/10.52306/01010418ZDCD5438>

This item is available as part of Virtual Commons, the open-access institutional repository of Bridgewater State University, Bridgewater, Massachusetts.

Copyright © 8-2018 Kyung-shick Choi, Claire Seungeun Lee, and Robert Cadigan

K. Choi, C.S. Lee, & R. Cardigan. (2018). *International Journal of Cybersecurity Intelligence and Cybercrime*, 1 (1), 21-39.

Spreading Propaganda in Cyberspace: Comparing Cyber-Resource Usage of Al Qaeda and ISIS

Kyung-shick Choi, Boston University and Bridgewater State University, U.S.A

Claire Seungeun Lee*, Inha University, South Korea

Robert Cadigan, Boston University, U.S.A

Key Words: cyberterrorism, Al Qaeda, ISIS, propaganda, cyber-resources, cyber-technologies, multiple correspondence analysis

Abstract:

Terrorists in cyberspace are increasingly utilizing social media to promote their ideologies, recruit new members, and justify terrorist attacks and actions. This study explores the ways in which types of social media, message contents, and motives for spreading propaganda take shape in cyberspace. In order to empirically test these relations, we created a dataset with annual terrorism reports from 2011 to 2016. In our global cyberterrorism dataset, we used and connected cyber-resources (Facebook, online forum, Twitter mentions, websites, and YouTube videos) and legal documents of individual cases that were mentioned in the reports. The data suggest that ISIS and Al Qaeda utilize different platforms, and utilize platforms differently. The results show that YouTube videos were used primarily for propagating certain ideologies and for recruiting members for Al Qaeda and ISIS. Al Qaeda-affiliated cyberterrorists used YouTube videos as both individual sources and embedded sources for Facebook and Twitter, whereas ISIS-affiliated cyberterrorists predominantly used YouTube videos and Twitter posts.

Introduction

In April, 2015, Ardit Ferizi – a citizen of Kosovo and the known leader of Kosovo’s Hacker’s Security – posted on his Twitter account, @Th3Dir3ctorY, “Getting to Know Kosovar Hacker’s Security Crew plus an Exclusive Interview with Th3Dir3ctorY,” complete with a link providing access to the information (United States of America v. Ardit Ferizi, 2015: 6). On April 26-27, 2015, he exchanged tweets and confirmed that, “Yes brother/Im muslim al britani” (United States of America v. Ardit Ferizi, 2015: 10). He continuously posted ISIS videos and provided an ISIS recruiter and leader with the personal information of 1,351 U.S. military members so that it could be used as a “hit list.” Given these unlawful actions, he was charged with providing material support to the Islamic State of Iraq and Syria (ISIS, hereafter). Ferizi was arrested in Malaysia, where he was accessing the Internet to

*Corresponding author

Claire Seungeun Lee, Ph.D., Assistant Professor of Sociology, Department of Chinese Studies, College of Humanities, Inha-ro 100, Inha University, Nam-gu, Incheon, South Korea, 22212

Email: clairelee@inha.ac.kr, drclaireselee@gmail.com

Reproduction, posting, transmission or other distribution or use of the article or any material therein, in any medium as permitted by written agreement of the International Journal of Cybersecurity Intelligence and Cybercrime, requires credit to the Journal as follows: “This Article originally appeared in International Journal of Cybersecurity Intelligence and Cybercrime (IJCIC), [year] Vol. #, Iss. #, pp. 00-00” and notify the Journal of such publication.

© 2018 IJCIC 2578-3289/2018/08

further his cyberterrorist agenda, and was extradited to the United States to face prosecution. Ferizi pleaded guilty and was sentenced to 25 years in prison.

Terrorist organizations and individuals like Ferizi have developed extensive capacities for disseminating propaganda, recruiting members, and communicating support to terrorist organizational structures and operations. While documents such as *The Minimanual of the Urban Guerilla* (Marighella, 1969) and the 1977 edition of *The IRA Green Book* (Coogan, 2002) continue to offer practical guidance, the scope and sophistication of current activities could not have been predicted by their authors. Counterterrorism focuses on the capacity of cyberterrorists to employ sophisticated techniques to attack a nation's critical infrastructure. However, terrorists also routinely use advanced technology to facilitate and coordinate daily activities and conduct conventional attacks.

Cyberterror – a term coined by Barry Collin in the 1980s – has received heightened attention in recent years from the media (Tafoya, 2011; Weimann, 2004a). Academia, on the other hand, has been scattered in terms of its scope, detail, and focus. That is, while some studies have focused on the threats and vulnerabilities of cyberattacks (Conway, 2005; Weimann, 2004a), others have discussed social media and Internet involvement in cyberterrorism (Aly, Macdonald, Jarvis, & Chen, 2017; Archetti, 2013; 2015; Conway, 2017; Gendron, 2017; Mair, 2017; Rudner, 2017). Moreover, some research on cyberterrorism focuses on how the Internet and cyberspace are used for terrorism funding, recruiting, and propaganda (Aly, 2017; Crilley, 2001; Denning, 2010; Gill, Corner, Conway, Thornton, Bloom, & Horgan, 2017; Jacobson, 2010; Liang, 2015; Ranstorp, 2007; Thomas, 2003; Weimann, 2004a; 2004b; 2006). Since few empirical and descriptive studies exist on how terrorists use cyberspace for propaganda (Archetti, 2013; Conway, 2017; Zelin, 2013), most scholarly work employ textual and/or narrative analyses (Aly, 2017). Such a void in the literature remains largely true even today (Conway, 2005), and in particular, a limited number of studies which use longitudinal data exist due to difficulties in acquiring and saving relevant data.

In this paper, we focus on the aspect of cyberterrorism in relation to terrorist use of cyber-technologies/resources. We extend our approach of using different cyber-resources from Conway (2005)'s initial study on examining cyberterrorist websites by focusing on other types of cyber-resources – such as online and social media platforms – in addition to cyberterrorist websites within the analysis. Methodologically, we use a systematic approach with a unique and longitudinal dataset.

The current study is designed to identify trends and patterns of cyberterrorism in propaganda by using a multiple correspondence analysis. In particular, this research explores whether or not organizations – specifically Al Qaeda and its affiliates and ISIS – differ in their usage of cyber-resources in organizing activities and operations. The focus is on cyber-resources used in managing the organization of its membership and supporting conventional tactics such as bombing, hijacking, arson, assault, kidnapping, and hostage taking (Jenkins, 2006). The propaganda focus is analytically distinct, but often overlaps in organizational practice with recruitment and financing. That is, propaganda mobilizes potential recruits in a population, while also encouraging financial donations to the cause. To examine how, and in what ways, Al Qaeda and ISIS use different cyber-resources for disseminating propaganda, we created a dataset on cyberterrorism propaganda that uses English to convey terrorism-related messages. The “global cyberterrorism dataset” is based on multiple years of annual Terrorism Reports (2011 – 2016) and connects cyber-resources with legal documents to individual cases that were mentioned in the reports.

Until recently, the area of cyberterrorism and/or terrorist attacks in cyberspace have been discussed in security studies and political science inquiries (e.g. Weinberg, Pedahzur, & Hirsch-Hoefler, 2004;

Weinmann, 2005a; 2005b) more so than any other discipline, including criminology. Using information and communication technology or cyber-resources for recruitment and propaganda was discussed in the criminology literature, but most of them were looking at violent organizations (e.g. gangs) or extremist groups (e.g. Corb, 2011; Décary-Héту & Morselli, 2011; Decker & Pyrooz, 2011; Pyrooz, Decker, & Moule, 2015; Sela-Shayovitz, 2012).

From a criminological perspective, approaches to cyberterrorism are still lacking methodologically speaking, empirical testing in understanding cyberterror through these theoretical grounds – with a particular interest in perpetrators – has yet to be developed. An exception is documented within the area of politically-stimulated and/or state-centered cyberattacks, not cyberterrorism. In this thread, previous studies have focused on the subcultures of hackers and cyber-attackers with a claim that cyberterrorism is ideologically shaped and geared in a political manner (Britz, 2010; Holt, 2009; 2012; Holt, Kilger, Chiang, & Yang, 2017; Yar, 2013).

Linking empirical testing to criminological theories complements existing knowledge and offers guidance to both scholarship and policy sectors. By using our global cyberterrorism dataset, an integrated theoretical framework, which combines Cloward and Ohlin's (1960) subcultural theory with Cornish and Clarke's (1985) rational choice theory, was adopted. This theory is apropos in analyzing twenty-first century terrorist organizations focusing on the ways in which specific types of cyber-capability influence the operational functions of terrorist organizations (propaganda) and the situations in which terrorist acts occur.

An integrated framework: Applying subcultural theory and rational choice theory to cyberterrorism

By definition, terrorist organizations traditionally reject the culturally accepted means of accomplishing socially approved goals and, in the case of some domestic terrorist organizations, offer variant interpretations of those goals (c.f. Schmidt, 2012). Terrorism in cyberspace is a criminal activity with organized actions and those who have shared group identity. Groups such as Al Qaeda and ISIS, as well as others rooted in Salafi jihadism, reject the opportunity structures and goals of economic success in the Western world and challenge the legitimacy of governments in Muslim majority nations (Armbrorst, 2013; Dar & Hamid, 2016). To successfully accomplish their means of terrorism, they damage both themselves and others by using violent behaviors, armed forces, ideology, and radicalization. On the other hand, terrorist groups and individuals in cyberspace have maintained the basic premise of conventional terrorism while heightening the level of engagement with technology and cyber-capabilities to support their terrorist acts. These features of cyberterror are explicated by two theoretical perspectives – subcultural theory and rational choice theory. In order to examine the use of cyber-resources in cyberterrorists' propaganda actions, subcultural theory and rational choice theory are applied to cyberterrorism.

Subcultural Theory

Those espousing terrorism can be seen as constituting either a subculture or a counterculture within their own societies. The basic premise of the subcultural theory is that individuals conform to the norms and behaviors of their subculture when they cannot meet or exceed the goals of the dominant culture (Cohen, 1955). Subcultural theory can help not only in understanding the circumstances under which terrorist actions are likely, but also the form with which such actions will take. Two classes of determinants are: (1) the situation and (2) the actor's frame of reference (Cohen, 1955; Downes, 1966).

These two factors play a significant role in better understanding the subculture of ideology-based distinct terrorist groups and/or individuals in cyberspace.

The situation component is where the subculture distinctively occurs. This comprises of the physical location, resources available, and social organizations (Cohen, 1955; Downes, 1966). While various state actors have the capacity to marshal extensive cyber-resources for distributed denial of service attacks (DDoS) and systems hacking, non-state actors tend to focus on the use of resources in propaganda, recruitment, organizational communication, and financial management (United Nations Office on Drugs and Crime, 2012). For cyberterrorism, locations become less relevant than conventional terrorism, while resources that are often associated with particular terrorist organizations are highly embedded in subcultural traits. Despite the lack of documentation in cyberterrorists' subculture, terrorists' clear-cut affiliations exist. However, we can derive implications from works on subcultural characteristics of hackers and cyberattackers, who are not always terrorists but could have a similar level of capacities for technological facilitations for carrying out terrorism, or victimization of cyberattacks (Holt et al., 2017). An actor's frame of reference can be understood as the set of assumptions that guide members' understanding of their larger culture and place in it. For example, Al Qaeda has labelled the world as being comprised of near enemies – apostate Muslim countries and far enemies – Western democracies (Armstrong, 2015; Ibrahim, 2007; U.S Department of State Diplomacy in Action, 2012;). ISIS has cast its concerns in apocalyptic language (McCants, 2015; Tucker, 2014). While direct victims of such terrorist attacks are not the main targets (Schmidt, 2012), the symbolic significance of violent victimization in Muslim majority countries differ between Al Qaeda and ISIS.

In order to establish the caliphate, ISIS has engaged in ruthless violence including beheading, burning hostages alive, rape, and physical deformation for committing criminal offenses in territories they control (Tucker, 2014). Terrorists' frames of reference and different situational factors lead them to prioritize opportunities for action differently and evaluate actions according to different criteria than Al Qaeda. Al Qaeda in the Arabian Peninsula (AQAP), for example, has vehemently protested beheadings despite some reports in anti-jihadist sources (Jihad Watch, 2008).

In the cyber-realm, terrorist groups use the Internet for recruiting and mobilizing participants, fundraising, and planning for attacks (Ogun, 2012; Thomas, 2003). In particular, Al Qaeda and ISIS use a similar but distinct cyber-strategy to engage in cyberterrorism. On the one hand, Jihadist groups use websites, discussion forums, and social media to propagate their messages and outsource propaganda by using online magazines (Gendron, 2017). Dabiq "glorifies" those who have died fighting for the "cause." Examples of this glorification can be seen in how they build schools for ISIS children, and care for the elderly who have lost children who fight for the ISIS cause. This is done in an effort to recruit those who wish to be part of the great deeds for which they perceive ISIS to be fighting. While ISIS also uses social media to gain credibility and legitimacy (Farwell, 2014), its hacking attacks target both civilians in Western democracies and its counterpart terrorist groups such as Al Qaeda (Nance & Sampson, 2017). According to Pisoiu's (2015) research, which uses subcultural theory on jihadi and right-wing radicalization in Germany, cyberterrorists utilize distinct subcultures for radicalizing terror actions while maintaining mainstream tools and styles. That is, terrorists in cyberspace often have this dual strategy in keeping with subcultural traits. Al Qaeda and ISIS, with an ambition of reaching broader audience members and targets, exploit the mainstream media (Farwell, 2014), while utilizing social media and other cyber-resources. Taken together, subcultural differences within each terrorist affiliation in relation to cyber-resources and cyber-capabilities are documented in terrorists' involvement in cyberspace.

Rational Choice theory

The premise of the rational choice theory is that an offender commits a specific crime to serve a specific purpose (Cornish & Clarke, 1986; Guerette, 2010). Situational tactics have been adopted to reduce criminal opportunity and risks: (1) methods which increase or decrease the amount of effort criminals engage in; (2) methods to increase or decrease the risk for criminals; and (3) methods used to increase or decrease the rewards of certain crimes (Guerette, 2010).

While terrorist activities in cyberspace are grounded in specific organizational and subcultural contexts, rational choice theory suggests that the use of technology will also depend on a group's calculation of efforts needed, as well as the risks and benefits associated with the chosen type of attack (Guerette, 2010).

These three components, which are consistently discussed in rational choice theory, can be applied to cyberterrorists' engagement of cyber-resources. These factors play an instrumental role in cyberterrorists' decision to select the best cyber-resource for the right time and place to achieve their goals. To manage a reduced risk and obtain a high and easy reward, motivated perpetrators use cyber-resources to propagate, deliver messages, and attack targets in cyberspace. Cyber-resources are used as a result of choices that were made rationally. The first component of rational choice theory, risk, is reduced by conducting terrorism in cyberspace. In turn, utilizing cyber-resources is a low-risk strategy available to motivated perpetrators who plan to engage in cyberterrorism. In other words, as an offender encounters a higher level of perceived risk of terrorist activity, the likelihood of achieving the goal will be reduced to reflect the potential costs involved (Guerette, 2010). A technically competent individual(s) can use these resources in such a way that they maximize contact with targets who exhibit low self-protective behavior while maintaining distance from those targets who exhibit high self-protective behavior.

The second component, effort, is recognized by technological facilitation (posting and uploading technology-facilitated resources and circulating propaganda) and a less risky presence. For cyberterrorists, an easy access to potential targets online means no limit to their physical presence. Through the use of Internet resources, terrorists are now able to directly upload unedited videos of their attacks for mass audiences (Jenkins, 2006). This enables any user on the Internet to see the atrocities terrorists are committing. Without effective deterrent agencies to prevent these videos and images from surfacing, terrorists rationally choose to upload them to their websites, or other social media platforms because the risk of facing charges is minimal.

The third component, rewards, is also important for any deviant behavior vis-à-vis cyberterrorism. Terrorists' motivations for getting better rewards by using disruptive self-protective behavior (e.g., hiding real identities and fabricating physical locations of technological facilities, etc.) may improve their reputation in the subcultural group. At the same time, claiming responsibilities for terrorist actions in cyberspace is a critical step not only for proliferating their attacks but also for gaining potential rewards and building reputations.

These three tenets of rational choice theory in cyberterrorism – risk, effort, and rewards – are effective if terrorists' technological facilitation of cyber-resources and their deliberate contents are well tied with spreading propaganda. Also, the reasons and motivations for why terrorist groups and individuals use particular tools are also important. A further explanation of subcultural differences and similarities of cyberterrorist actions and rational choices in our global cyberterrorism dataset will be discussed in the next section of this study.

Data and methodology

We used multiple data sources and methodologies to explore how cyberterrorists were organized, recruited members, and motivated themselves to perpetrate terrorist attacks in cyberspace. While much can be gained from ideology-based terrorism studies and datasets, research focusing on cyberterrorism is limited (Capellan, 2014). Given the scarcity of comprehensive cyberterrorism datasets, it is imperative that collection be done to create one that can be operationalized in current and future inquiries.

Data sources

This research combined multiple data sources into its primary dataset. The first set of data is derived from existing annual terrorism reports from 2011 to 2016 (U.S. Department of State, 2011; 2012; 2013; 2014; 2015b; 2016). The data includes a list of all terrorist attacks, case descriptions, nationality of victims and terrorists, agencies, sanctions, types of attack, arrest dates, terrorist groups, and any major personal information. These multiyear reports are useful in that they highlight the patterns of both terrorism and cyberterrorism behaviors. However, as the focus of the reports is more on terror rather than on cyberterror, it is imperative that we collect additional information to make this analysis as complete and encompassing as possible.

In order to obtain more data on the aspects of cyberterror, we gathered both social media and court documents that strengthen the details of various cyberterrorism cases. Social media postings (Facebook, online forums, Twitter mentions, websites, and YouTube videos) as well as news media articles which were mentioned in each case were collected for further analysis. Additionally, the court documents of each case indicating the sanction, year of sanction, and reasons for such decisions were collected.

Data collection

At Phase I of data collection, the major variables were manually recorded from the annual terrorism reports (2011 to 2016) and entered into a database. At the second stage of data collection, we identified further information on the available cases from both legal documents and social media.

In order to understand how al Qaeda and ISIS terrorist groups in cyberspace spread propaganda, we needed to identify affiliations of each terrorist/suspect and classify these cyberterrorists into the two groups: Al Qaeda and ISIS. Table 1 presents a list of cyberterrorists based on their apostate ideology.

Byman (2014, p. 438) notes that, “there is little work on terrorist alliances, and what work there is suggests that these alliances are rare, with an exception of Bapat and Bond’s work (2012).” Identifying groups for each actor is the core step of this research. In doing so, we drew multiple academic and media sources for categorizing actors into groups. Cyberterrorist groups with Al Qaeda have actors who are clearly associated with Al Qaeda (Byman, 2014). However, ISIS cyberterrorist groups are relatively difficult to track, and the internal dynamics of ISIS-cyberterrorist groups are still developing (National Counterterrorism Center, n.d. a; b; c; d; Roggio, 2011).

Data analysis

Measures and descriptions of variables / sample characteristics A total of 79 cases were identified from terrorism reports for the 5-year duration between 2011 and 2016. In the global cyberterrorism da-

Table 1. Affiliations of cyberterrorists in the Global Cyberterrorism Dataset

Al Qaeda-affiliated groups	ISIS-affiliated groups
Al Qaeda	Abu Sayyaf militants (jihadist)
Al Qaeda in the Arabian Peninsula (AQAP)	Ansar Bayt al Maqdis militants
Al Qaeda in the Islamic Maghreb (AQIM)	Free Sunni Brigade Haqqani Network
Al Nusra Front (al-Qaeda in Syria)	ISIS
Al-Shabaab	(Imarat Kavkaz) Jemaah Anshorut Tauhid
Al Qaeda in South Asia	Jund al-Khilafah (ISIS affiliate)
Colleen LaRose	Martin Couture-Rouleau
MHA “the librarian”	Unidentified Lone Wolf (IS Supporter/pro-ISIS account)
Unidentified Lone Wolf (Al Qaeda supporter)	Sinai Province Group

Note: Arranged by alphabetical order of Al Qaeda-affiliated groups.
Sources: Bacchi, 2014; DW, 2009; Jones, 2014; Khan, 2015; Mapping Militant Organization, 2016;
National Counterterrorism Center, n.d. a; b; c; d; Olsen, n.d.; Reuters, 2012; 2016; Spiegel Online, 2012;
Stratfor, n.d.; U.S. Department of State, 2015a.

taset, we have three types of variables: (1) case-related variables; (2) terrorist suspect’s characteristics; and (3) victim’s characteristics. The focus of this study is on the association between the type, content, and motive of cyberterrorists disseminating propaganda. The main variables (type, content, and motive) of this study are illustrated below, with type of cyber-resources having five categories: YouTube video (coded 1), website (coded 2), Twitter post (coded 3), online forum (coded 4), and Facebook post (coded 5). Content of propaganda messages have the following categories: attack threats, beheading, bombing (including suicide bombing, car bomb, bomb plan and construction), execution, shooting, seize control, terrorist literature, and recruitment. Motive has nine categories: documentation (documenting actions), fear and threat (creating fear and threat), incitement, justification (justifying actions), pride, promotion (promoting terrorism), ransom, recruitment, and support. Date, month, and year, as well as the number of cases, are also part of the case-related variables.

For the sociodemographic characteristics of terrorist suspects and victims for each cyberterrorism case there are age, gender, number of suspect/victim, and national origin of suspect/victim. The genders of the suspects were coded as (1) male, (2) female, and (3) male and female. Victim genders were coded as male (1), and male and female (2).

Both suspects and victims were predominantly male. Male victims accounted for 79.3% of total victims, while male suspects consisted of 94.6% of total suspects. The victim sample consisted of 20.7% mixed gender dynamics. The overall age of suspects was younger than victims (suspects were 29.6 years old on average, whereas victims’ average age was 39.5 years). For suspects, we matched legal documents to their cyberterror case for sanctioned months.

The national origins of cyberterror suspects and victims varied. Terrorists, especially those who are related to al Qaeda, targeted western democracies (Armstrong, 2015; Ibrahim, 2007; U.S. Department of State Diplomacy in Action, 2012). This was also reflected in our global cyberterror dataset. Sixteen victimized cases of cyberterror were unspecified. As a result, we followed the direction of previous studies (Armstrong, 2015; Ibrahim, 2007; U.S. Department of State Diplomacy in Action, 2012), and coded them as “western democracies.” Victim nationalities totaled 23 countries with one unspecified group: Cameroon, Canada, Croatia, Egypt, Ethiopia, France, Germany, India, Indonesia, Iraq, Israel, Japan, Jordon, Lebanon, Libya, Philippines, Russia, Spain, Syria, Uganda, United Kingdom, United States, Yemen, and western democracies. The nation of suspects totaled 27 countries with one unspecified group: Afghanistan, Algeria, Australia, Bangladesh, Cameroon, Canada, Egypt, France, Germany, India, Indonesia, Iraq, Israel, Lebanon, Libya, Mali, Morocco, Nigeria, Philippines, Roma-

nia, Russia, Somalia, Spain, Syria, United Kingdom, United States, Yemen, and western democracies. Table 2 presents summary statistics for the variables.

Table 2. Summary statistics for the Global Cyberterrorism Dataset, 2011 to 2015

Variable	Description	<i>n</i>	<i>M</i>	<i>SD</i>
<i>Case-related variables</i>				
Case	Cyberterrorism case	78	1.7	0.46
Type	Type of cyber-resources	78	3.7	1.42
Content	Content of propaganda	78	5.6	3.05
Date	Date of case	77	47.8	26.6
Month	Month of case	77	6.0	3.6
Year	Year of case	78	2014	1.2
<i>Terrorist suspect's characteristics</i>				
AgeSuspect	Suspect's age	29	29.6	11.0
GenderSuspect	Suspect's gender	55	Male (94.6%)	0.2
NumSuspect	Number of perpetrators involved	36	1.1	0.3
Nation of suspect	Nation of suspect	78	18.8	8.9
Sanction	Sanctioned months	10	169.5	64.1
<i>Victim's characteristics</i>				
Age of victim	Victim's age	11	39.5	12.3
Gender of victim	Victim's gender	29	Male (79.3%)	0.4
NumVictim	Number of victims involved	35	7.3	10.9
Nation of victim	Nation of victim	78	16.3	8.3

M = mean, *SD* = standard deviation

Multiple correspondence analysis

Multiple correspondence analysis (MCA), which is an extended version of correspondence analysis (CA), is an effective method to explore the pattern of relations of more than two categorical dependent variables (Abdi & Valentin, 2007). We can interpret MCA results on the basis of closeness between different variables. However, it is counted as important when vicinities between points from the same set (i.e., rows with rows, columns with columns) occur (Abdi & Valentin, 2007).

Both MCA and CA are used in criminology studies to identify associations among mafia activities, and countries (Calderoni, Berlusconi, Garofalo, Giommoni, & Sarno, 2016). Some of these studies explore how a mafia group is limited to or beyond national boundaries (Varese, 2012). Like these previous studies, this inquiry of global cyberterrorism propaganda is essentially an organized crime. Some of the cyberterror attacks are thoughtfully organized, whereas others are loosely organized but have common ideologies or agendas which are likely to belong to one terrorist group or another. In this analysis, we extend the use of MCA into analysis of terrorist propaganda activity.

Results

Trend of cyberterrorism: Al Qaeda and ISIS

With the technological advancements, terrorists increasingly use not only their weapons and strategies on the ground, they are also using technologies and cyber-resources for disseminating ideas and coordinating actions (Aly, 2017; Crilley, 2001; Denning, 2010; Gill et al., 2017; Jacobson, 2010; Liang,

Fig. 1. Terrorist Cyber-Activities: Al Qaeda and ISIS

2015; Ranstorp, 2007; Thomas, 2003; Weimann, 2004a; 2004b; 2006). Al Qaeda and ISIS use different cyber-resources and modes of activity related to terrorism in cyberspace. A significant change of players in cyberterrorism is documented in Figure 1. While cyberterrorism by Al Qaeda has been distributed well from 2011 to 2015, most of the cyberterrorism activities by ISIS were highly concentrated in 2014 and 2015 (96.4% of all ISIS cyberterror cases in the dataset) and evenly distributed (n=27). Al Qaeda and its franchises have actively engaged with cyberterrorism during the entire study period. ISIS, on the other hand, became predominantly active from April 2014 to August 2015. This could also be related to Al Qaeda's rejection of ISIS as not being representative of Al Qaeda's beliefs/modus operandi/objectives, and their efforts to distance themselves from associating with ISIS. For most of its existence, ISIS was strongly linked to operations inside Iraq and became involved in Syria in the spring of 2013 – they only began attacking other rebel groups in August of 2013 (Glenn, 2016). Increased support from within Syria and success of overtaking towns and cities provided renewed confidence for ISIS as an independent organization, thereby increasing attractiveness to join as an increasingly effective and far-reaching terrorist organization. Greater successes by ISIS created increased presence across social media platforms.

With such substantial differences in the timing of cyberterrorism incidents by Al Qaeda and ISIS, we turn our attention to whether or not they use cyber-resources differently. As Rudner (2017: 10) suggested, "Al Qaeda has deemed the Internet a great medium for spreading the call of Jihad and following the news of the mujahideen (Islamic warriors) (Rudner, 2017: 10)." Table 3 shows Al Qaeda's frequent use of websites and YouTube videos, along with ISIS' repeated use of YouTube videos and

Twitter posts. YouTube was commonly identified as an effective medium of disseminating propaganda by both groups.

Table 3. Type of cyber-resources: Al Qaeda and ISIS

	Al Qaeda		ISIS	
	Frequency	Percent	Frequency	Percent
Facebook Post	2	9.1	9	16.1
Online Forum	2	9.1	2	3.6
Twitter Post	2	9.1	15	26.8
Website	8	36.4	6	10.7
YouTube Video	8	36.4	24	42.9
Total	22	100.0	56	100.0

Cyber-resources documenting cyberterror actions show that Al Qaeda and ISIS disseminate different content for propaganda. Beheading is the most frequently used content (23.2%) for ISIS, followed by terrorist literatures (21.4%), whereas threatening has occurred the most for Al Qaeda's cyberterror attacks (36.4%).

Table 4. Content of online terrorist materials: Al Qaeda and ISIS

	Al Qaeda		ISIS	
	Frequency	Percent	Frequency	Percent
Beheading	-	-	13	23.2
Bombing	2	9.1	9	16.1
Control	1	4.5	3	5.4
Execution	1	4.5	3	5.4
Recruitment	4	18.2	4	7.1
Shooting	-	-	4	7.1
Terrorist Literature	6	27.3	12	21.4
Threat	8	36.4	8	14.3
Total	22	100.0	56	100.0

Note: * respectively refers to a group-specific propaganda
(Al Qaeda literature for Al Qaeda and ISIS ideology for ISIS)

Consistent with the trend of timing, tools, and content of these two groups in cyberattacks, the reason and motives behind cyberterrorism for Al Qaeda and ISIS seem different. Promoting certain ideologies (31.8%) is the main motive for Al Qaeda-affiliated suspects, whereas creating fear and threat (37.9%) is the principle motive for ISIS-affiliated actors to conduct such actions.

Similar to ISIS, Al Qaeda also finds importance in generating fear and threat using cyberattacks across the world. Justifying and supporting their actions (19.0%, respectively) is the second most frequently observed motive for ISIS.

MCA: Propaganda by Al Qaeda vs ISIS

MCA allows us to create a link between variables (i.e., type, content, and motive) to further understand the dynamics of cyberterror actions by Al Qaeda and ISIS. Figure 2 and Figure 3 represent the relationship between cyber-resource usage and motivations by two main terrorist groups.

Table 5. Motives behind cyberterror: Al Qaeda and ISIS

	Al Qaeda		ISIS	
	Frequency	Percent	Frequency	Percent
Documentation	1	4.6	2	3.4
Fear and threat	4	18.2	22	37.9
Incitement	-	-	1	1.7
Justification	3	13.6	11	19.0
Pride	1	4.5	1	1.7
Promotion	7	31.8	2	3.4
Ransom	1	4.5	4	6.9
Recruitment	4	18.2	4	6.9
Support	1	4.5	11	19.0
Total	23	100.0	56	100.0

Fig. 2. and Fig 3. Type, Content, and Motive of Propaganda by Al Qaeda (left) and ISIS (right)

Propaganda by Al Qaeda and ISIS show different characteristics by type, content, and motive. Al Qaeda utilized Twitter to post bombing cases, whereas YouTube was used to primarily disseminate propaganda messages regarding executions. Moreover, while terrorist literatures were disseminated and promoted through websites by Al Qaeda groups, ISIS used Twitter, online forums, and websites to support and promote their ideologies. Twitter and online forums were also employed to show bombings and justify ISIS terrorist actions.

Al Qaeda predominantly used cyber-resources to promote its ideologies, while ISIS used cyber-resources to primarily create fear and justify their cyberterror actions. For example, on December

29, 2012, Al-Malahem Media associated with Al-Qaeda in the Arabian Peninsula posted a message on a militant website offering money to people who could kill US soldiers in Yemen and/or kill the US Ambassador in Yemen (Al-Qaeda in the Arabian Peninsula, December 29, 2012). Al-Qaeda forces situated in the Arabian Peninsula used a website to promote their terrorist ideologies. Lawal Babafemi, a Nigerian suspect affiliated with Al-Qaeda in the Arabian Peninsula, was sanctioned to serve 180 months as he “was in charge of editing and publishing articles on online INSPIRE AQ magazine, was forerunner in campaigning and recruiting online, [and] was paid \$9,000 for it” (Lawal Babafemi, Al-Qaeda in the Arabian Peninsula, September 27, 2013). Collen LaRose, who was sentenced to serve 150 months, “had multiple emails and YouTube accounts and website which published jihadist literature and videos” (Collen LaRose, undated).

In contrast, ISIS focused on dramatic acts of terrorism. The group posted a 4-minute video titled, “A Message to America,” showing US journalist James Foley kneeling in an orange jumpsuit reading a message scripted by ISIS. This was followed by “Jihadi John,” who read another message addressing the United States. Following that message, the film cut back to a headless corpse of James Foley (ISIS, August 19, 2014). On August 29, 2014, Ansar Bayt al-Maqdis militants, known for being linked to ISIS, posted a video on Twitter of them beheading four Egyptians they accused of providing intelligence to Israel that resulted in three of their militants being killed (Ansar Bayt al-Maqdis militants, August 29, 2014).

Discussion

This paper investigated both Al Qaeda and ISIS’ use of cyber-resources to disseminate propaganda messages. A new way of examining terrorism in today’s technologically advanced era is using cyber-resources to explore cyberterrorism. This is supported by rational choice principles, which suggest that perpetrators engage in terrorist behaviors that increase their criminal rewards while decreasing the amount of effort it takes to diminish the risks associated with their actions (Guerette, 2010).

Classifying these cyberterrorist suspects into two groups is a quintessential element of this research. Our global cyberterrorism database presents different suspects based on their affiliations with Al Qaeda and ISIS. With regards to the subcultures of each group, these two terrorist groups have different formations, development, ideologies, and uses of cyber-resources. On one hand, in the global cyberterrorism dataset, we have nine suspects those who are affiliated with Al Qaeda: Al Qaeda, Al Qaeda in the Arabian Peninsula (AQAP), Al Qaeda in the Islamic Maghreb (AQIM), Al Nusra Front (Al Qaeda in Syria), Al-Shabaab, Al Qaeda in South Asia, Colleen LaRose, MHA “the librarian,” and an unidentified Lone Wolf (Al Qaeda supporter). While most of these suspects are from regional branches of Al Qaeda, individual actors who are related to Al Qaeda were also found in the cyberterror cases from 2011 to 2016. Contrary to this, cyberterror suspects who are associated with ISIS included Abu Sayyaf militants (jihadist), Ansar Bayt al Maqdis militants, Free Sunni Brigade Haqqani Network, ISIS, (Imarat Kavkaz) Jemaah Anshorut Tauhid, Jund al-Khilafah (ISIS affiliate), Martin Couture-Rouleau, an unidentified Lone Wolf (IS Supporter/pro-ISIS account), and the Sinai Province Group.

According to subcultural theory principles, while these two groups share ideologies, religion, and culture within their affiliation, they also utilize similar patterns of cyber-resources. First, both Al-Qaeda and ISIS found YouTube videos to be the most effective tool in disseminating threatening messages. However, according to our data and analysis, while Al-Qaeda largely relied on the use of websites, ISIS used Twitter posts to spread their videos and/or broadcast their activities more than other cyber-

resources. Disseminating these videos and messages are rationalized choices for ISIS cyberattackers. In doing so, they not only show solidarity toward their organization, but also justify their behavior because those who were put at a higher risk and ultimately died, did not make a rational choice.

Conclusion

Building on the emerging literature on propaganda research in global cyberterrorism (Crilley, 2001; Vatis, 2001; Thomas, 2003; Weimann, 2004b; 2006; Liang 2015; Ranstorp, 2007; Stenersen, 2008; Denning, 2010; Jacobsen, 2010) and arguably the first empirical study of propaganda research using MCA in global cyberterrorism, this paper analyzed how Al Qaeda and ISIS use cyber-resources in their propaganda processes. In doing so, we have constructed a global cyberterror dataset by combining both cyber-resources (Facebook, online forums, Twitter mentions, websites, and YouTube videos) and legal documents to individual cases that were mentioned in reports.

The results of this paper show that cyberattack strategies of Al Qaeda and ISIS have a different configuration. YouTube videos were predominantly used for propagating certain ideologies and for recruiting members for both Al Qaeda and ISIS. However, there was an isomophoric pattern in the number of suspects who were subscribed to al Qaeda and ISIS ideologies, respectively. Al Qaeda-affiliated cyberterrorists used YouTube videos as both individual sources and embedded sources through Facebook and Twitter, whereas ISIS used Twitter accounts to show their successes and victories by disseminating messages and videos of beheadings and bombings.

This paper is not without limitations. It is important to note that our data sources, which were compiled from Global Terrorism Reports, media reports, and court cases, may not capture a whole picture and may only offer some part of the terrorists' cyber-activities. However, our data show a similar pattern to what Berger and Morgan's study (2015) has presented. Thus, future research should use a longer period of multiple sources for further investigation and incorporate other large databases such as the National Consortium for the Study of Terrorism and Responses to Terrorism's Global Terrorism Database (START, n.d.) into our dataset.

The findings of this study lead us to present the following policy implications. Preventive measures on cyberterrorist attacks are important and better examined at the federal, state, and local levels (Choi, 2015: 290-291). With regards to investigations, law enforcement organizations need to better equip themselves with technological advancements, while also considering international cooperation between agencies at different levels inside and outside their own national boundaries. Second, given that cyberterrorism uses social media to target civilians who have access to the Internet, it is imperative that citizens are trained to recognize potential risks and know how best to report and detect cyberterror actions. While public awareness programs and campaigns for citizens are important and require effective tools to recognize the different types, characteristics, and issues within cyberterrorism, major online platforms, such as Facebook, Twitter, and YouTube, must consider strengthening their ability to identify and report posts and videos that contain cyberterrorism contents.

As terrorism in cyberspace is likely to be furthered with technological advancements, future research agendas and efforts need to be made to document and analyze these different cyberterrorism activities in other languages. Acknowledging the limitations of the language-accessibility in our global cyberterrorism dataset is important, as our dataset only includes English materials. Incorporating other languages within the database is beneficial given the wide target audience and vast victim pool related to non-English languages. Although cyberterror activities in local and regional languages are

also important, such actions have a local, yet limited effort to reach potential audiences. As the geographical boundary of cyberterrorism is beyond boundaries of nation-states, policing and sanctions for suspects and criminals involved in such cases are ultimately difficult to capture. Thus, a comprehensive and collective effort on legally bounded measures for cyberterror activities should be considered. In this regard, we suggest legal aspects of cyberterrorism with sanctioned cases be studied further in future research agendas. Both convictions of suspects and the legal foundations of potential and existing cyberterror are important measures for us to understand. In the future, socio-demographic variables of victims and terrorists, as well as case variables in this global cyberterror dataset, should also be examined. The potential linkage between different terrorist groups should also be further examined in future cyberterrorism research.

References

- Abdi, H. & Valentin, D. (2007). *Multiple Correspondence Analysis*. In N. Salkind (ed.), *Encyclopedia of Measurement and Statistics* (pp. 651–657). Thousand Oaks: Sage.
- Aly, A. (2017). Brothers, believers, brave mujahideen: Focusing attention on the audience of violent Jihadist preachers. *Studies in Conflict & Terrorism*, 40(1), 62–76.
- Aly, A., Macdonald, S., Jarvis, L., & Chen, T. M. (2017). Introduction to the special issue: Terrorist online propaganda and radicalization. *Studies in Conflict & Terrorism*, 40(1), 1–9.
- Archetti, C. (2013). *Understanding terrorism in the age of global media: A communication approach*. Basingstoke: Palgrave Macmillan.
- Archetti, C. (2015). Terrorism, communication and new media: Explaining radicalization in the digital age. *Perspectives on Terrorism*, 9(1), 49–59.
- Armbrorst, A. (2013). *Jihadi violence: A study of al-Qaeda's media*. Berlin: Duncker and Humblot.
- Armstrong, K. (2015). *Fields of blood: Religion and the history of violence*. New York: Anchor Books.
- Bacchi, U. (2014, October 21). Canada: Isis 'lone wolf' killer martin couture rouleau mows down soldiers with car. *IB Times*. Retrieved from <http://www.ibtimes.co.uk/canada-isis-lone-wolf-killer-martin-couture-rouleau-mows-down-soldiers-car-1471023>.
- Bapat, N. A. & Bond, K. D. (2012). Alliances between militant groups. *British Journal of Political Science* 42(4): 793–824.
- BBC Monitoring (2016, May 12). Sinai Province: Egypt's most dangerous group. *BBC*. Retrieved from <http://www.bbc.com/news/world-middle-east-25882504>.
- Berger, J. & Stern, J. M. (2015). *ISIS: The state of terror*. New York: HarperCollins.
- Britz, M. T. (2010). *Terrorism and technology: Operationalizing cyberterrorism and identifying concepts*. In T. J. Holt (ed.), *Crime On-Line: Correlates, causes, and context* (pp. 193–220). Raleigh: Carolina Academic Press.
- Byman, D. (2014). Buddies or burdens? Understanding the Al Qaeda relationship with its affiliate organizations. *Security Studies*, 23, 431–470.
- Calderoni, F., Berlusconi, G., Garofalo, L., Giommoni, L., & Sarno, F. (2016). The Italian mafias in the world: A systematic assessment of the mobility of criminal groups. *European Journal of Criminology*, 13(4), 413–433.
- Capellan, J. A. (2015). Lone wolf terrorist or deranged shooter? A study of ideological active shooter events in the United States, 1970–2014. *Studies in Conflict & Terrorism*, 38(6), 395–413.
- Choi, K. (2015). *Cybercriminology and digital investigation*. El Paso: LFB Scholarly Publishing LLC.
- Cloward, R. A. & Ohlin, L. E. (1960). *Delinquency and opportunity: A theory of delinquent gangs*. Glencoe: The Free Press.
- Cohen, A. K. (1955). *Delinquent boys: The culture of the gang*. Glencoe: The Free Press.
- Coogan, T. P. (2002). *The IRA*. New York: St. Martins Press.

- Corb, A. (2011). *Into the minds of Mayhem: White supremacy, recruitment and the Internet*. Presented at Google Ideas conference, Dublin, Ireland.
- Conway, M. (2005). *Terrorist web sites: Their contents, functioning, and effectiveness*. In P. Seib (ed.), *Media and conflict in the twenty-first century* (pp. 185-215). New York: Palgrave Macmillan.
- Conway, M. (2017). Determining the role of the Internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism*, 40(1), 77–98.
- Cornish, D. B. & Clarke, V. G. (1986). *The Reasoning criminal: Rational choice perspectives on offending*. New York: Springer-Verlag.
- Crilley, K. (2001). *Information warfare: New battle fields Terrorists, propaganda and the Internet*. Aslib Proceedings. MCB UP Ltd.
- Décary-Hétu, D. & Morselli, C. (2011). Gang presence in social network sites. *International Journal of Cyber Criminology*, 5(2), 876–890.
- Decker, S. & Pyrooz, D. (2011). Gangs, terrorism, and radicalization. *Perspectives on Radicalization and Involvement in Terrorism*, 4(4), 151–166.
- Denning, D. E. (2010) *Terror's web: How the internet is transforming terrorism*. In Y. Jewkes & M. Yar (Eds.), *Handbook of Internet Crime* (pp. 194–213). Devon: Willan Publishing.
- Downes, D. M. (1966). *The Delinquent solution*. New York: The Free Press and London, Collier-Macmillan.
- DW (2009, October 2). German authorities arrest suspected al Qaeda members. DW. Retrieved from <http://www.dw.com/en/german-authorities-arrest-suspected-al-qaeda-member/a-4753384>.
- Dutta, S., Geiger, T., & Lanvin, B. (2015) (eds.). *The global information technology report 2015: ICTs for inclusive growth*. Geneva: World Economic Forum. Retrieved from http://www3.weforum.org/docs/WEF_Global_IT_Report.2015.pdf.
- Farwell, J. P. (2014). The media strategy. *Survival: Global Politics and Strategy* 56(4): 49–55.
- Glenn, C. (2016). *Timeline: Rise and spread of the Islamic State*. Washington, D.C.: Wilson Center. Retrieved from <https://www.wilsoncenter.org/article/timeline-rise-and-spread-the-islamic-state>.
- Gendron, A. (2017). The call to Jihad: Charismatic preachers and the Internet. *Studies in Conflict & Terrorism*, 40(1), 44–61.
- Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., & Horgan, J. (2017). Terrorist use of the Internet by the Numbers: Quantifying behaviors, patterns, and processes. *Criminology & Public Policy*, 16(1), 99–117.
- Guerette, R. T. (2010). *Understanding Crime Displacement: A Guide for Community Development Practitioners*. Local Initiatives Support Corporation (LISC), Crime Safety Initiatives (CSI) and the Metlife Foundation.
- Holt, T. J. (2009). *The attack dynamics of political and religiously motivated hackers*. In T. Saadawi & L. Jordan (eds.), *Cyber Infrastructure Protection*. New York: Strategic Studies Institute, (pp. 161–183).

- Holt, T. J. (2012). Exploring the intersections of technology, crime and terror. *Terrorism and Political Violence*, 24, 337–354.
- Holt, T. J., Kilger, M., Chiang, L., & Yang, C.-S. (2017). Exploring the correlates of individual willingness to engage in ideologically motivated cyberattacks. *Deviant Behavior*, 38(3), 356–373.
- Ibrahim, R. (2007). *The Al Qaeda reader: The essential texts of Osama Bin Laden's terrorist organization*. New York: Broadway Books.
- Jacobson, M. (2010). Terrorist financing and the Internet. *Studies in Conflict & Terrorism*, 33(4), 353–363.
- Jenkins, H. (2006). *Convergence Culture: Where old and new media collide*. New York and London: New York University Press.
- Jones, S. G. (2014). *A Persistent Threat: The Evolution of al Qaeda and Other Salafi Jihadists*. Santa Monica: The RAND Corporation. Retrieved from http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR637/RAND_RR637.pdf.
- Khan, M. (2015). France: Timeline of terrorist attacks. January 7. *IB Times*. Retrieved from <http://www.ibtimes.co.uk/france-timeline-terrorist-attacks-1482413>.
- Liang, C. S. (2015). Cyber Jihad: understanding and countering Islamic State propaganda. GSCP Policy Paper 2.
- Mair, D. (2017). #Westgate: A Case Study: How Al-Shabaab used Twitter during an ongoing attack. *Studies in Conflict & Terrorism*, 40(1), 24–43.
- Mapping Militant Organization (2016, August 26). Boko Haram. Retrieved from <http://web.stanford.edu/group/mappingmilitants/cgi-bin/groups/view/553?highlight=boko+haram>.
- Marighella (1969). The Minimanual of the urban guerilla. Retrieved from <https://www.marxists.org/archive/marighella-carlos/1969/06/minimanual-urban-guerrilla/>.
- McCants, W. (2015). *The ISIS Apocalypse: The history, strategy and the doomsday vision of the Islamic State*. New York: St Martins.
- Nance, M. & Sampson, C. (2017). *Hacking ISIS: How to destroy the cyber Jihad*. New York: Skyhorse.
- National Counterterrorism Center (n.d.)a. Abu Sayyaf. Retrieved from <https://www.nctc.gov/site/groups/abu.sayyaf.html>.
- National Counterterrorism Center (NCTC) (n.d.)b. Al-Nusrah Front. *Counterterrorism Guide*. Retrieved from <https://www.nctc.gov/site/groups.html>.
- National Counterterrorism Center (NCTC) (n.d.)c. Ansar Bayt al Maqdis. Retrieved from https://www.nctc.gov/site/groups/ansar_bayt_al_maqdis.html.
- National Counterterrorism Center (NCTC) (n.d.)d. Haqqani Group - al Qaeda linkage. Retrieved from https://www.nctc.gov/docs/2014_worldwide_threats_to_the_homeland.pdf.
- Olsen, M. G. (2014, September 17). Worldwide threats to the homeland. National Counterterrorism Center (NCTC). Retrieved from https://www.nctc.gov/docs/2014_worldwide_threats_to_the_homeland.pdf.

- Ogun, M. H. (2012). Terrorist use of Internet: Possible suggestions to prevent the usage for terrorist purposes. *Journal of Applied Security Research*, 7(2), 203–217.
- Pyrooz, D. C., Decker, S. H. & Moule, R. K. (2015) Criminal and routine activities in online settings: Gangs, offenders, and the Internet. *Justice Quarterly*, 32(3), 471–499.
- Ranstorp, M. (2007). *The virtual sanctuary of al-Qaeda and terrorism in an age of globalization*. In J. Eriksson & G. Giacomello (Eds.), *International relations and security in the digital age* (pp. 31–56). London and New York: Routledge.
- Reuters (2012, March 27). Spain arrests Qaeda suspect for inciting attacks. *Reuters*. Retrieved from <http://www.reuters.com/article/us-spain-qaeda-idUSBRE82Q0UH20120327>.
- Reuters (2016). Colleen Larose – admitted contacts with al Qaeda operative. *Reuters*. Retrieved from <http://www.reuters.com/article/us-usa-jihadjane-idUSBREA050PC20140106>.
- Rudner, M. (2017). ‘Electronic Jihad’: The Internet as Al Qaeda’s catalyst for global terror. *Studies in Conflict & Terrorism*, 40(1), 10–23.
- Schmidt, A. (2012). The revised academic consensus definition of terrorism. Retrieved from <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/schmid-terrorism-definition/html>.
- Sela-Shayovitz, R. (2012). Gangs and the web: Gang members’ online behavior. *Journal of Contemporary Criminal Justice* 28(4): 389–405.
- Sieber, U. (2010). *Instruments of international law: Against terrorist use of the Internet*. In M. Wade & A. Malievic (Eds.), *A war on terror?: The European stance on a new threat, changing laws and human rights implications* (pp. 171–219). New York: Springer.
- Spiegel Online (2012, March 22). Promoting Terror Online: Al-Qaida ‘Media Warrior’ Gets Five Years. Retrieved from <http://www.spiegel.de/international/germany/suspected-al-qaida-propagandist-convicted-in-germany-a-823072.html>.
- Stenersen, A (2008). The Internet: A virtual training camp?. *Terrorism and Political Violence* 20(2): 215–233.
- Stratfor (n.d.). Free Sunnis of Baalbek. Retrieved from <https://www.stratfor.com/situation-report/iraq-free-sunnis-baalbek-brigade-pledges-allegiance-militant-leader>.
- Tafoya, W. L. (2011). Cyber Terror. The Federal Bureau of Investigation. Retrieved from <https://leb.fbi.gov/2011/november/cyber-terror>.
- Thomas, T. L. (2003). Al Qaeda and the Internet: The danger of “cyberplanning”. *Parameters*, Spring, 112–123.
- Tucker, C. (2014). The Islamic State: Origins, goals, and future implications. July 13. The Eurasia Brief. Available at: https://eurasiacenter.org/publications/ISIS_Briefing_Colin_Tucker.pdf (accessed January 9, 2017).
- Varese, F. (2012). How Mafias take advantage of globalization. *British Journal of Criminology*, 52(2), 235–253.
- Vatis, M. A. (2001). *Cyber attacks during the war on terrorism: A predictive analysis*. Hanover: Institute for Security, Dartmouth College.
- Weinberg, L., Pedahzur, A., & Hirsch-Hoefler, F. (2004). The challenges of conceptualizing terrorism. *Terrorism & Political Violence*, 16(4), 777–794.

- Weimann, G. (2004a). Cyberterrorism: How real is the threat? United States Institute of Peace Special Report. Retrieved from <http://www.usip.org/sites/default/files/sr119.pdf> (accessed January 9, 2017).
- Weimann, G. (2004b). *www. terror. net: How modern terrorism uses the Internet*. Diane Publishing.
- Weimann, G. (2005). Cyberterrorism: The sum of all fears?. *Studies in Conflict & Terrorism*, 28(2), 129–149.
- Weimann, G. (2006). *Terror on the Internet: The new arena, the new challenges*. US Institute of Peace Press.
- U.S. Department of State Diplomacy in Action (2012). Retrieved from <https://www.state.gov/>.
- U.S. Department of State (2011). *Country reports on terrorism on 2010*. Washington, D.C.: Department of State.
- U.S. Department of State (2012). *Country reports on terrorism on 2011*. Washington, D.C.: Department of State.
- U.S. Department of State (2013). *Country reports on terrorism on 2012*. Washington, D.C.: Department of State.
- U.S. Department of State (2014). *Country reports on terrorism on 2013*. Washington, D.C.: Department of State.
- U.S. Department of State (2015a). *Country reports on terrorism on 2014*. Washington, D.C.: Department of State.
- U.S. Department of State (2015b). *Country reports: Middle East and North Africa overview*. Country reports on terrorism 2015. Retrieved from <https://www.state.gov/j/ct/rls/crt/2015/257517.htm>.
- U.S. Department of State (2016). *Country reports on terrorism on 2015*. Washington, D.C.: Department of State.
- United States of America v. Ardit Ferizi a/k/a Th3Dir3ctorY (2015, October 6). No. 1: 15-MJ-515. United States District Court for the Eastern District of Virginia.
- United Nations Office on Drugs and Crime (2012). *The use of the Internet for terrorist purposes*. New York: United Nations.
- Yar, M. (2013). *Cybercrime and Society*. The second edition. London: Sage.
- Zelin, A. Y. (2013, December 19). Foreign Jihadists in Syria: Tracking recruitment networks. *The Washington Institute for Near East Policy*. Retrieved from <http://www.washingtoninstitute.org/policy-analysis/view/foreign-jihadists-in-syria-tracking-recruitment-networks>.