MAPPING GLOBAL CYBERTERROR NETWORKS

An Empirical Study of Al-Qaeda and ISIS Cyberterrorism

Journal of Contemporary Criminal Justice

Post-Print (Accepted Manuscript)

Claire Seungeun Lee* [a], Kyung-Shick Choi [b], Ryan Shandler [c] & Chris Kayser [d]

[a] University of Massachusetts Lowell

[b] Boston University

[c] University of Haifa

[d] Cybercrime Analytics Inc.

Cite as: Lee, C., Choi, K.S., Shandler, R., Kayser, C. (Forthcoming) "Mapping Global Cyberterror Networks: An Empirical Study of Al-Qaeda and ISIS Cyberterrorism Events". *Journal of Contemporary Criminal Justice.*

* claire_lee@uml.edu

Abstract

This current study explores the internal dynamics and networks of terrorist groups in cyberspace—in particular, Al-Qaeda and ISIS. Using a "Global Cyberterrorism Dataset" that features data on cyberterror attacks between 2011 and 2016, this research analyzes these two terrorist groups through the lens of a cyber-conflict theory that integrates conflict theory with Jaishankar's space transition theory. Through a network analysis methodology, we examine the invisible relations and connections between the national origins and target countries of cyberterror attacks. The analysis focuses on the networks of national origins of terrorists and victims; network structures of Al-Qaeda and ISIS actors; and clustering networks of Al-Qaeda and ISIS cyberterrorists. Results indicate that terror in cyberspace is ubiquitous, more flexible than traditional terrorism, and that cyberattacks mostly occurred within the countries of origin. We conclude by discussing the complex features of cyberterror networks and identify some of the geo-strategic implications of the divergent cyber strategies adopted by Al-Qaeda and ISIS.

Keywords: Cyberterrorism, Al-Qaeda, ISIS, social network analysis, cyber-conflict theory, space transition theory

Introduction

In the aftermath of the 9/11 terror attacks, a surge of academic research in the field of terrorism has contributed to a deep understanding of how conventional kinetic terrorism is organized, facilitated, and propagated (Abrahms, 2019; Duyvesteyn, 2004; Neumann & Smith, 2007). Yet terrorism is subject to the same global forces and developments as the rest of the world, and advances in technology have beckoned forth a new threat of cyberterrorism. The ubiquity and anonymity of cyberspace has enabled terror organizations to access new methods in designing traditional or complex attacks. The cyber component of cyberterrorism relates to both the networked structure of modern terror organizations that are able to more efficiently disseminate and communicate information, and also the wielding of cyber weapons that allows for anonymous transnational attacks against newly vulnerable targets.

While research on technology-facilitated terrorism has increased (Archetti, 2013; Mair, 2017; Rudner, 2017), only a handful of papers have incorporated empirical analyses of cyberterrorism (Gross, Canetti, & Vashdi, 2016; Gross, Canetti, & Vashdi, 2017; Canetti, Gross, Waismel-Manor, Levanon, & Cohen, 2017; Qvortrup, 2015). This paper attempts to add to the dearth of empirical research into cyberterrorism (Conway, 2005; Conway, 2017; Holt, Stonhouse, Freilich, & Chermak, 2019; Zelin, 2013), by conducting a systematic analysis of the relationship between actors and victims in cyberterrorism, resulting from increased use of technology and cyberspace to plan, execute, monitor, and evaluate the results of their attacks. Developing an understanding of the relationship between offenders and victims in cyberterrorism cases would contribute a great deal to the criminological literature, and also to policymakers, national security officials, and the wider public. To do this, we introduce a novel "Global Cyberterrorism Dataset" that provides comprehensive data on dozens of cyberterror attacks attributed to Al-Qaeda and ISIS between 2011 and 2016.

For the purposes of this analysis, we define cyberterrorism as a computer-based attack, or threat thereof, that is intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological (Lachow, 2009). This relatively broad definition builds on Dorothy Denning's seminal understanding of cyberterrorism as the "convergence of terrorism and

cyberspace" (Denning, 2000). We adopt a definition that views cyberterrorism as pertaining to acts that use cyberspace as a means of attack, as well as those that view it as the target of the attack. In light of the heated debate over the scope and definition of cyberterrorism (Luiijf, 2014), we adopt a broad operationalization of the phenomenon, rejecting more modern variants that suggest that cyberterrorism must cause physical destruction (Egloff, 2020; Lachow, 2009). As such, our expansive construal of the phrase includes the use of cyber networks by terror organizations to disseminate political messages, for recruitment, fundraising, and more.

This current study explores the internal dynamics and networks of terrorist groups in cyberspace—in particular, Al-Qaeda and ISIS. Specifically, this paper illuminates how the national origins and sources of terrorists and victims are interrelated to one another by looking through the prism of cyberterror attacks launched by these two terror groups. Using the uniquely constructed dataset—"global cyberterrorism dataset"—that includes annual data from Terrorism Reports from 2011 to 2016 (US Department of State, 2012; 2013; 2014; 2015; 2016; 2017), and legal and media resources, this study aims to contribute an understanding of the relationships and dynamics between Al-Qaeda and ISIS terrorists, their victims, and the increased reach on a local and global basis afforded terrorists who take advantage of advancements in cyberspace. We focus our analysis on Al-Qaeda and ISIS for several reasons. First, these two organizations are ranked among the top eight deadliest terror organizations, and of those on the list, are the only organizations with a global mission and transnational capabilities (LaFree and Dugan, 2016). Just as importantly, Al-Qaeda and ISIS are listed as among the five wealthiest terror organizations, offering the resources to develop expensive cyber assets (Zehoral, 2018). Second, Al-Qaeda and ISIS possess highly sophisticated and developed cyber strategies. Al-Qaeda has been quietly investing in cyber-jihad capabilities for more than 20 years, while much commentary has been dedicated to ISIS' mastery of social networks and digital communication to engage in outreach and prepare for attacks (Ogun, 2015; Sardarnia and Safizadeh, 2019). Third, while both Al-Qaeda and ISIS have invested significant resources in developing cyber capabilities, they each possess a distinct cyber strategy that is distinguished on the propaganda focus and the prioritization of particular networks (Choi, Lee, & Cadigan, 2018). This divergence of strategy is not merely tactical, but relates to key differences in ideological doctrines (Arosoaie, 2015), which may in turn influence their (cyber)terror actions and recruitment strategies.

In order to understand why certain countries are victims and/or originating sources, this study proposes an explorative theory—"cyber-conflict theory"—that combines conflict theory with Jaishankar's (2007) space transition theory. Conflict theory, often criticized by its shortcomings—low empirical validity and ideological bias—does not adequately explicate terror in cyberspace. Because terrorism is an organized and ideological activity, propositions of space transition theory, which are rooted in conflict theory, can be applied to cyberterrorism to gain a better understanding of the ways in which terrorism occurs in cyberspace. Transposing conflict theory and space transition theory into cyberspace provides us our framework of "cyber-conflict theory" to empirically test why and how Al-Qaeda and ISIS have created distinct patterns of offender-and-victim relations in cyberterrorism, followed by a discussion of the data and research methods, and a presentation of the data analysis. Finally, this study concludes with a discussion of the research findings, limitations, future research agendas, and policy implications of the current study.

An Integrated Framework Of "Cyber-Conflict Theory": Conflict Theory And Space Transition Theory

To ground our findings in the existing literature on conflict behavior, we offer an integrated framework that combines traditional conflict theory with space transition theory. We then apply the new "cyber-conflict theory" to cyberterrorism to reinterpret conflict theory in cyberspace. Below

we offer a brief review of these two theories and describe how they apply in the realm of cyberspace.

Conflict theory in cyberterrorism

Conflict theory views crime as a function of the conflict that exists in society. Conflict theorists argue that criminology is generally too concerned with asking why people commit crimes and suggests that societal crime is predominantly caused by class conflict and inequality (Turk, 1969). The primary objective of social conflict theorists is to explain crime within economic and social contexts and to express the relationship between the nature of social class, crime, and social control. Thus, conflict theorists view crime as the outcome of class struggle. According to Marxian conflict theory, conventional terrorist acts, and by extension, cyberterrorist acts, are typically motivated by ideological beliefs that are supported by the actions of those who feel oppressed and unfairly disadvantaged (Marx, 1859).

This traditional conflictist view of crime can equally be applied to cyberterrorism, where values, ideologies and norms play an influential role. Recent studies tentatively suggest that individuals associated with terror organizations tend to come from underprivileged backgrounds and from countries that are highly religious and ideologized (Kreuger & Malečková, 2003; Sterman, 2015). Most cyberterror attacks are motivated by an all-encompassing ideology or religious belief as evidenced in the impetus of Al-Qaeda and ISIS. Ideological changes and technological advancements influence the ways in which cyberterrorism is propagated, organized, and occurs (Choi, Lee, & Cadigan, 2018).

This combination of ideology and technology means that terrorism in cyberspace, in the view of traditional conflict theory, could be attributed to a class struggle between different classes and ideologies, or an uneven world order, fueled by wealth, technology, ideology, and geopolitics. As the data shows, cyberterror attacks tend to occur most often against wealthy democratic nations raththaer n poorer and non-democratic nations, which can result in a reversal of roles of victims and offenders (Rozentsvaig, Kovalenko, & Gubareva, 2018). Terrorists who utilize cyber-resources to promote and propagate ideology and exercise power through global terrorism predominantly target western democracies that do not share the same views, ideologies, and political systems of the perpetrators.

Space transition theory for cyberterrorism

Space transition theory was developed to explain the conforming and non-conforming behavior of individuals as they transition from a physical space to cyberspace (Jaishankar, 2007). While this theoretical framework does not explicitly engage with conflict theory, this theory has clear roots in the conflictist tradition, as seen in a central tenet of the theory that expounds that "the conflict of norms and values of physical space with the norms and values of cyberspace may lead to cybercrimes". The view that differences in the norms and values of cyberspace associated with offenders' backgrounds are similar to the conflict theory's perspective of viewing the dominant system of social relations as a major cause of crime, and that offenders from different socio-economic status can become easily engaged in illegal acts to bring out social change.

Jaishankar (2007) presents seven propositions for explaining and supporting his argument. We can summarize the claims in relation to cyberspace as: (1) Offender's characteristics: Individuals who have repressed criminal behavior in the physical space have a propensity to commit cybercrime; (2) Disguisable/changeable identity: The nature of cyberspace—anonymity and flexibility of identity formation and absence of deterrence, gives offenders a choice to commit cybercrime; (3) Space convertibility: Offenders' criminal behavior in different spaces (physical and cyberspace) will transpose to other spaces; (4) Criminal opportunity with a low risk of detection:

The sporadic and spatio-temporal nature of cyberspace, creates a low risk of detection and provides offenders a means to escape; (5) Offenders' affiliations: Individuals who may have little or no connections in with others in their physical space, may unite in cyberspace to commit cybercrimes together; (6) Reduced threat to offenders: Individuals from closed society are more prone to commit cybercrimes in cyberspace than those from open society; and (7) Conflict of norms and values: A conflicted view of norms and values in physical space versus cyberspace may result in engaging in cybercrime (Jaishankar, 2007).

Three of the seven propositions of space transition theory – changeable identity of offenders, space convertibility, and criminal opportunity at a low risk of detection in cyberspace – can be directly applied to the phenomenon of cyberterrorism. The changeable identity of offenders' variable reflects the much talked about phenomenon of dissociative anonymity that describes the behavior of cyber users (Agustina, 2015; Suler, 2004). In a digital environment, users experience a lower deterrence factor due to a cognitive disinhibition effect prompted by physical separation from end-results. This is reflected in terrorist behavior since the dissociative anonymity reduces any deterrence from acting out destructive impulses that may be minimized in physical settings. The space convertibility factor simply suggests that criminal behavior in the physical world, or in this case terrorist behavior, is likely to manifest in cyberspace, absent any constraints. Since digital connectivity is growing globally, including among terror operatives, the theory essentially advocates that cyberterrorism is an inevitable evolution of conventional terrorism. The criminal opportunity of low risk of detection in cyberspace factor indicates how intermittent ventures into cyberspace, as well as its dynamic spatial-temporal character, combine to substantially lower the risk of capture and provide offenders with more chances to escape than conventional terror operatives.

While space transition theory puts emphasis on space convertibility between physical space and cyberspace for offenders, victims, and suspicious activities, traditional conflict theory gives us more insight into the importance of potentially conflicted views, values, ideologies, and norms specific to motives related to cyberterrorism. A further explanation of how the findings from the cyberterrorism dataset support the existence of this conflict-based cyberspace convertible theory (cyber-conflict theory) will be discussed in a later section of this paper.

Data and Methodology

Introducing the Global Cyberterrorism Dataset

In order to understand how the countries from which cyber terror attacks are launched are intertwined with dynamics of cyberterrorism, we created a "Global Cyberterrorism Dataset"[1] combining multiple sources of data on cyberterror attacks. The first set of data is derived from existing annual terrorist reports for the period 2011 – 2016 (US Department of State, 2012; 2013; 2014; 2015; 2016; 2017). These reports compiled records on all terrorist attacks, case descriptions, nation of victims and terrorists, agency, sanctions, type of attacks, arrest date, terrorist groups, along with major personal information. We linked this dataset with cyber-resources and social networking services (YouTube Videos, Twitter, Facebook, online forums, and websites) and major

[1] We acknowledge that there are existing excellent datasets on terrorism, in particular, the National Consortium for the Study of Terrorism and Responses to Terrorism's Global Terrorism Database is notable (National Consortium for the Study of Terrorism and Responses to Terrorism, 2020). While this is longitudinal and useful, the Database does not specifically focus on cyberterrorism.

historic events.[2] The major variables were manually recorded from the annual terrorism reports (2011 to 2016) and entered into a database in the first stage of data collection (Choi et al., 2018).

Table 1 presents the key variables in the dataset. Among 83 cases in our global cyber-terrorism dataset, 32.5 percent (n=27) are al-Qaeda cyberterrorism incidents, and 67.5 percent (n=56) are ISIS cyberterrorism cases. For both organizations, the vast majority of incidents were recorded in the final two years of the data range, reflecting a substantial acceleration of cyberterrorism from 2014 onward.

Table 1. Al-Qaeda and ISIS's cyberterror cases

Terrorist groups	**Al Qaeda**		**ISIS**	
	N	**%**	**N**	**%**
2012	4	14.8	1	1.8
2013	3	11.1	1	1.8
2014	9	33.3	27	48.2
2015	7	25.9	27	48.2
Total N	27	100.0	56	100.0

Table 2 and Table 3 present cyberterrorism cases of Al-Qaeda and ISIS in the dataset respectively. The country of origin of the victims most targeted by Al-Qaeda is the United States (n=7), followed by incidents where multiple targets were simultaneously targeted (n=5). Israel and Somalia were the only other cases where victims from a particular country were targeted multiple times. For ISIS, multiple simultaneous targets were most common, followed by Egypt, Syria and the United States.

Table 2. Al-Qaeda's cases: Countries of origin for victims and attackers

Victims (Targets)	**Number of victimizations**	**Attackers (Suspects)**	**Number of attacks**
United States	7	Israel	6
Multiple targets	5	Somalia	3
Israel	3	Nigeria	2
France	2	United Kingdom	2
Burundi	1	Yemen	2
Cameroon	1	Bangladesh	1
Ecuador	1	Cameroon	1
Germany	1	France	1
India	1	India	1
Iraq	1	Iraq	1

[2] While types and content of cyber-resources and social networking services in our dataset are important measures for cyberterrorism incidents, these do not factor in this current research. Thus, we provide relevant descriptions of these variables in the footnote only. A variable of *type of cyber-resources* was coded as Facebook post, online forum, Twitter post, Website, and YouTube video. *Content of cyber-resources* was coded as beheading, bombing, control, execution, recruitment, shooting, terrorist literature, and threat. *Motives of cyber-resources* was coded as documentation, fear and threat, incitement, justification, pride, promotion, ransom, recruitment, and support (see Choi et al., 2018).

Lebanon	1	Lebanon	1
Spain	1	Mali	1
Syria	1	Middle East	1
Uganda	1	Spain	1
		United States	1
		Unspecified sources	1

Notes: The order is based on the number of victimization/attacks from the largest to smallest in the dataset. All victims of the multiple targets were not always identified.

Table 3. ISIS's cases: Countries of origin for victims and attackers

Victims (Targets)	Number of victimizations	Attackers (Suspects)	Number of attacks
Multiple targets	13	Syria	14
Egypt	9	United States	9
France	4	Egypt	8
United States	4	Iraq	3
Iraq	3	Libya	3
Japan	3	Algeria	2
Germany	2	Australia	2
Jordan	2	Lebanon	2
Lebanon	2	Afghanistan	1
Syria	2	Canada	1
United Kingdom	2	France	1
Canada	1	Germany	1
Croatia	1	India	1
Ethiopia	1	Indonesia	1
Indonesia	1	Morocco	1
Israel	1	Philippines	1
Libya	1	Romania	1
Philippines	1	Russia	1
Russia	1	Spain	1
Spain	1	United Kingdom	1
Yemen	1	Unspecified source	1

Notes: The order is based on the number of victimization/attacks from the largest to smallest in the dataset.

Building on this foundation, we then added a second layer of data to augment the particulars of the terrorism incidents. This second layer of supplementary data was drawn from court documents and relevant news reports of the terrorism cases that were identified in the annual terrorism reports. While the multiyear terrorism reports (which have strong focuses on conventional terrorism rather than cyberterrorism) provide good data with which to track patterns of terrorism and cyberterrorism, it was imperative for us to collect additional information to allow for more robust analyses. For example, the secondary data sources enabled us to label the attacks according to the involvement of extended networks and affiliates of Al-Qaeda and ISIS. For this second stage,

all information from terrorist reports, legal documents, and social media were manually recorded and entered into the database

Identifying the perpetrator terror organization for each terror incident is an important step of this cyberterrorism research and a frequent challenge in terrorism research (Weimann, 2015). For the purpose of this dataset, we drew from multiple academic and media sources to categorize actors into our two groups—Al-Qaeda and ISIS (Byman, 2014; Council on Foreign Relations, 2008; 2016; Jocelyn, 2013; Kliegman, 2015; National Counterterrorism Center, 2014; Roggio, 2011; Yalibnan, 2014).

Social Network Analysis: Analysis Strategy

Our analysis strategy relies on the use of social network analysis. (Social) network analysis is widely used across disciplines of social and natural sciences such as sociology, criminology, political science and biology. It is used to explore invisible relations and connections between actors (Gaharwar, Shah & Gaharwar, 2015), co-offending networks among perpetrators (McGloin & Piquero, 2010; McGloin, Sullivan & Piquero, 2008; Reiss & Farrington, 1991; Sarnecki, 2001; Van Mastrigt & Farrington, 2009), street gangs (Grund & Denslet, 2012; Fleisher, 2006; McGloin, 2005; Papachristos, 2009), heroin distribution patterns (Natarajan, 2006), and organized crime syndicates (Campana &Varese, 2012; Klerks, 2001; McIllwain, 2004; Morselli, 2003; Morselli, 2009).

Social network analysis facilitates understanding of covert or illegal networks; thus, it is also a useful method to further understand hidden networks and dynamics of terrorism and cyberterrorism. Since the September 11 attacks, the social network analysis tools have been frequently applied to understand the nature and structures of terror organizations. In particular, a pioneering work by Krebs (2002) analyzed how the hijackers' networks that participated in the 9/11 attacks were linked by trust, tasks, finance and resources, and strategy and goals. Since then, multiple studies have utilized traditional criminal and terror network structures to analyze terrorism (Campana, 2016; Grund & Densley, 2015; Gunnell, Hiller & Blakeborough, 2016; Kelly & McCarthy-Jones, 2019; Mastrobuoni & Patacchini, 2012; Perliger & Pedahzur, 2011; Krebs, 2002). Various terrorist individuals and groups have been examined so far, including Al-Qaeda (e.g., Eilstrup-Sangiovanni & Jones, 2008; Enders & Su, 2007, Jackson, 2006), Neo-Jihadist Terror (Harris-Hogan, 2012), ego networks of five lone actor attacks in Australia (Bright, Whelan, & Harris-Hogan, 2020), Noordin Top's terrorist network in Southeast Asia (Roberts, 2011), the Jemaah Islamiyah cell for the 2002 Bali bombings (Koschade, 2007), and terrorists in the Malian conflict (Walther & Christopoulos, 2014).

Previous studies to examine (cyber)terrorism through the lens of social network analysis have typically focused on nodes (i.e., actors) and ties (e.g., activities, interaction, communication) in a network. Nodes relate to the number of actors, and their roles in a network. For ties, different activities and functionalities are measured – though the particular operationalization differs based on each research's aims. For example, the number of ties and how densely the networks are populated are a common metric (Kreb, 2002; Perliger & Pedazur, 2011). Activities are another common metric in measuring ties between actors, and can focus on organizational membership (Eilstrup-Sangiovanni & Jones, 2008), communication (Enders & Su, 2007; Jackson, 2006), and media and indictment (Kreb, 2002; Magouirk, Atran, & Sageman, 2008) were used as ties in a social network.

The reason why social network analysis can be effectively applied to cybercrime and cyberterrorism, is that they share a common network feature that allows us to observe how cyberattacks and cyber-actors are organized and mobilized in cyberspace. Key to the success of cyberterrorism is the ability for cyberterrorists to connect, share information, coordinate attacks, monitor results, and publicize their accomplishments in efforts to invoke fear, intimidation, and a

sense of victory. The Internet's global reach and relative anonymity can facilitate unrestricted communications for cyberterrorists to plan and execute the simplest, or most complicated cyber activities.

To conduct social network analysis, we used R and NodeXL to explore the relationships between the country of cyberterror targets and the country from which the cyberterror act was launched. We examined the vertex size to explore betweenness centrality, which refers to centrality with the shortest pathways between actors. We further employed a Harel-Koren graph to visualize the data in these analyses (Harel and Koren, 2000).

Results: Networks Of Terrorist-Victim Relations Of Al-Qaeda And ISIS

Detecting networks of national origins of terrorists and victims

Similar to conventional terrorists, cyberterrorists target countries and individuals whose views conflict with theirs. Cyberterror attacks by Al-Qaeda and ISIS are motivated by religious and political ideologies. Among 83 cases in our global cyberterrorism dataset, 32.5 percent (n=27) and 67.5 percent (n=56) of all cases are Al-Qaeda and ISIS cyberterrorism cases respectively. A total of 18 different countries were victimized (including multiple unspecified targets), while 29 distinct actors were involved in the attacks (including unspecified attackers). Figure 1 describes the connections between national origins of the cyberterrorists and targets/victims in the dataset. Colors of individual nodes in Figure 1 indicate frequencies of cyberterrorism involvement with actors. Darker colored nodes (i.e. red) indicate that they have a higher level of frequencies than lighter colored nodes (i.e. light yellow).

A common variable of the cyberterror activities of these two organizations is that the United States and other developed countries are the most frequent targets of Al-Qaeda and ISIS. This could be attributed to the United States' involvement in digitally and physically combating terror organizations in multiple geographic regions. Other countries that appeared in the dataset as either victims or origins (launching pads) of Al-Qaeda or ISIS cyberterror attacks included Cameroon, Canada, Egypt, France, Germany, India, Indonesia, Iraq, Israel, Philippines, Russia, Spain, Syria and the United Kingdom.

Countries such as Germany, Israel, France, Iraq, Spain, and Lebanon co-occurred as both victims and origins of Al-Qaeda and ISIS (see Table 1). These same victim-origin cases involve homegrown cyberterrorists for both Al-Qaeda and ISIS. Among these homegrown terrorists in cyberspace, some were radicalized due to high-risk social, economic, political or personal triggers, while others arguably acquired such knowledge due to religious heritage (Silber, Bhatt and Analysts, 2007). There are similar victim-terrorist cases involving ISIS that originated in Iraq and Lebanon. On July 5, 2014, ISIS leader Abu Bakr Al-Baghdadi posted a video on the internet of himself in the Great Mosque of al-Nuri in Iraq, telling all Muslims to wage jihad during Ramadan, while urging his people to follow his call to create their own caliphate (Atwan, 2015).

Focusing on attacks linked to Al-Qaeda, we observed that the United States, multiple targets, and Israel are the countries most frequently targets. Most of these attacks appeared to originate from the territories of Somalia, Middle East, Yemen, Nigeria, Bangladesh, and Israel. In addition, there were a number of Al-Qaeda related attacks where the origin of the attacks was in the same country as the target – such as in the United States, Israel, France, Iraq, Spain, and Lebanon. For attacks linked to ISIS, the most frequent targets include multiple targets, Egypt, and France. Countries such as Syria, United States, Egypt, France, Iraq, Libya, Germany, Lebanon, Canada, United Kingdom, Indonesia, the Philippines and Russia appeared to be both attackers and victims. Countries including Egypt, United States, Syria, Iraq, France, Lebanon, Canada, Indonesia, Spain, Russia, and the Philippines, had attacks inside the same nation for ISIS's cyberterrorism.

While France, Iraq, and Lebanon appear in both lists of Al-Qaeda and ISIS related attacks where the origin and target country are the same, the majority of the countries are different, and the overall number in the ISIS list is substantially larger. One interpretation of this data is that it may reflect divergent spheres of influence for these organizations – with ISIS holding sway over actors in more countries, but Al-Qaeda and ISIS sharing influence in certain countries where they are both active. An alternative explanation, though one that requires additional corroborating evidence, is the possibility of an intentional or unintentional division of resources between the ISIS and Al-Qaeda to refrain from concentrating their cyber assets in the same locations.

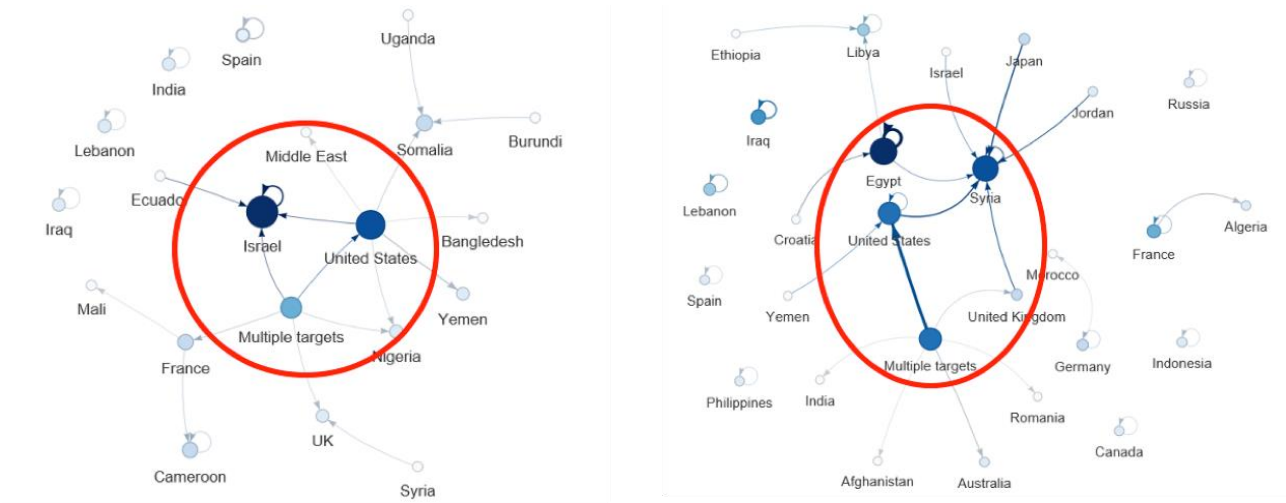
Looking closer at the data, we can see that Al-Qaeda and ISIS have slightly different patterns in the relationships between the origins of attackers and victims in our database. First, different actors exist for Al-Qaeda and ISIS. Some countries only appeared in the dataset of Al-Qaeda or ISIS. Cameroon and India appeared in Al-Qaeda's cases, while Canada, Indonesia, Libya, Philippines, and Russia appeared only in the ISIS cases.

Second, for both Al-Qaeda and ISIS, a number of attacks occurred inside the same country such as Iraq, Lebanon, and Spain where attackers and victims were inside the same countries. For example, among these homegrown terrorists in cyberspace, some were converted to Islam by faith and/or personal events, while others arguably acquired such knowledge by heritage.

Third, we did not observe overlapping countries of sole suspects and victims for Al-Qaeda and ISIS. For Al-Qaeda cases, Somalia, Nigeria, United Kingdom, Yemen, Bangladesh, Mali, and Middle East only appeared as countries of suspects, whereas Burundi, Ecuador, Germany, Syria, and Uganda appeared as countries of victims. For ISIS cases, Afghanistan, Algeria, Australia, India, Morocco, and Romania were countries of suspects only, whereas Croatia, Ethiopia, Israel, Japan, Jordan, and Yemen were countries of victims only. Additionally, we did not observe overlapping countries of sole suspects and victims for Al-Qaeda and ISIS. This may be attributable to the different ideologies and targets of Al-Qaeda and ISIS, except for activities related to their core targets.

Figure 1. Networks of national origins of cyberterror cases

Al-Qaeda **ISIS**



In-group Network Dynamics of Al-Qaeda and ISIS' Cyberterror Operations

Results of the network analysis for in-group networks for Al-Qaeda and ISIS are shown in Figure 2. Cyberterror incidents involving Al-Qaeda appear in blue, and ISIS appear in red. In order to present a comprehensive and comparative picture, we combined Al-Qaeda and ISIS together in the one same figure. According to this data, the United States is the most frequent target of cyberattacks by Al-Qaeda and ISIS, followed by unidentified targets. Our data also revealed that Hamas targeted Ecuador, Israel, an unidentified target, and the United States. The United States is also a frequent target of Al-Qaeda's affiliates. For example, the United States was targeted by regional al-Qaeda branches including Al-Qaeda in the Arabian Peninsula, Al-Qaeda in Southeast Asia, as well as major al-Qaeda players like Hamas and al-Shabaab.

Furthermore, unidentified targets sustained attacks by Hamas, al-Nursa, and Al-Qaeda in the Arabian Peninsula, an unidentified Al-Qaeda affiliate, and a lone wolf who claimed to be an Al-Qaeda entity. On June 16, 2011, Al-Qaeda publicized a hit-list of targets on a website that listed forty American businessmen, military personnel, and diplomats (Gustini, 2011). Al-Qaeda's threats of attacks, via their websites, created fear among targeted potential victims. In another example, we could identify the offender state when Al-Qaeda used a combination of videos and social media platforms originating in Bangladesh on May 3, 2015 to target a U.S.-origin blogger (Barry, 2015). Asim Umer, a leader of Al-Qaeda in South Asia, posted a 9-minute video announcing that followers of his group executed Avijit Roy, an atheist Bangladeshi-American blogger, and claimed to have conducted other attacks against writers and scholars who were against conservative Islam.

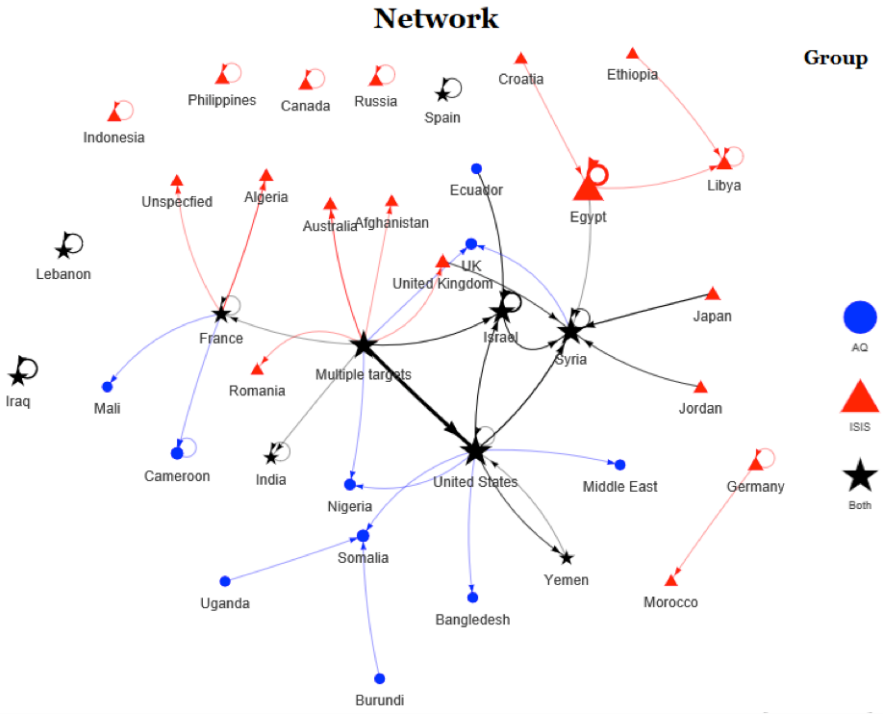
The dataset revealed that cyberterrorists tend to select targets within geographical proximity – a fact that is connected to the space transition theory within our cyber-conflict framework described in more detail below. Al-Nusra Front, which is one of the most prominent players in the Middle East, targeted Lebanon and Syria, and Al-Qaeda in South Asia targeted India, indicating a form of regionalism in cyberterror, which appeared to be a reoccurring pattern.

ISIS also relies upon various social media communications such as Twitter, Yahoo, and Facebook to broadcast acts of terrorism (Choi et al., 2018), and to a greater extent than Al-Qaeda, they tend to include graphic depictions of their heinous acts to spread fear around the world. Two prominent ISIS cases also involved Americans. The first occurred on August 19, 2014, when a 4-minute video with "A Message to America" showed James Foley, a U.S. journalist, kneeling in orange jumpsuit reading a message to America scripted by ISIS. After a brief break in the video, viewers were shown Foley's headless corpse. On November 16, 2014, ISIS released a video showing Jihadi John standing over the severed head of Peter Kassig, a captured U.S. citizen (Leaksource, 2014). Another video showed Jihadi John and others beheading 18 Syrian soldiers (Heavy, 2016). Similarly, ISIS-affiliated cyberterrorists based in Syria posted sensitized messages and videos on YouTube targeting the United States that exhibited characteristically violent behaviors. ISIS's messages were clear about their beliefs, their efforts against those who did not support their beliefs, and what ISIS would do to those who did not subscribe to their cause, or who were deprecating or disparaging of ISIS's efforts. Of note, our data revealed ISIS has a higher proportion of lone wolves than Al-Qaeda.

Both Al-Qaeda and ISIS cyberterrorist cases were highly focused on traditional targets such as Iraq compared to less conventional targets such as Egypt, India, Morocco, and the Philippines. In particular, unidentified ISIS players targeted the United Kingdom and the United States the most, followed by developed countries such as France, Germany, Israel, and Japan. One ISIS video posted on Twitter entitled, "A message of Blood for French Government", showed four ISIS militants standing over a French captive as he reads a prepared speech addressed to the French President, demanding France cease their airstrikes against ISIS. After a brief pause, viewers could see the captive's head placed in his lap.

Whereas traditional terrorism typically occurs in countries and regions near attackers due to spatiality issues, cyberterrorism can easily escape such physical boundaries, and can occur anywhere and anytime. However, our global cyberterrorism dataset refuted this intuitive expectation, with the global reach of cyberterror actors manifesting less than expected.

Figure 2. Networks of Al-Qaeda and ISIS cyberterror cases



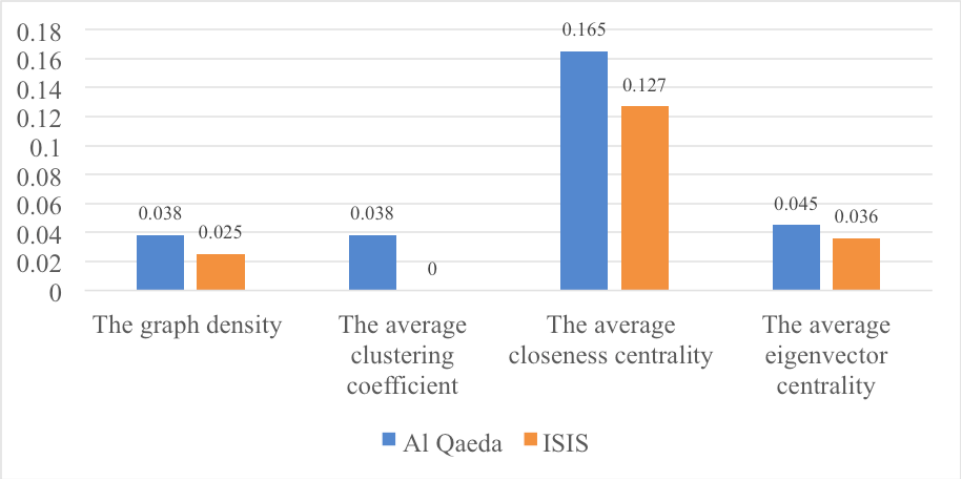
Clustering networks of Al-Qaeda and ISIS

Figure 3 shows network characteristics of actors involved in Al-Qaeda and ISIS-initiated and claimed cases. The graph density, which indicates how dense or sparse each graph is in relation to the number of actors involved in relevant cyberterror cases, was 0.038 and 0.025 respectfully. The density of the graph corresponds with the result of national origins and in-group structures, shown in Figure 1 and Figure 2, respectively. Put simply, more Al-Qaeda actors were closely involved in cyberterror cases than ISIS, whose networks tend to be more sparsely distributed in cyberterror cases.

In this clustering network analysis, the average clustering coefficient is one of the key measurements. It refers to differences between local measurements of how nodes are clustered in a graph and global measurements of such in an entire graph (Chalancon, Kruse, & Badu, 2013). This is used to understand "the degree to which the neighbors of a given node link to each other" (Barabási, 2016). The individual clustering for a node (Cli(g)) can be calculated as "the number of triangles connected to vertex i" that is divided by "the number of triples centered at i". The average clustering coefficient is calculated as ClAvg (g) = 1/n ∑i Cli(g).

The average clustering coefficient of Al-Qaeda was 0.038. While not high, it is significant when compared with ISIS's coefficient of 0.000. The latter implies that the ISIS cyberterror network had a relatively low level of interactions among the network structure (Park, Lim, & Park, 2015).

Figure 3. Characteristics of networks among Al-Qaeda and ISIS cyberterrorist actors



In this analysis, we used two centrality measures. Closeness centrality refers to a node's degree of closeness to all other nodes. A node located in the center and having a number of relations is likely to have a higher eigenvector closeness. The average closeness centrality of Al-Qaeda and ISIS actors was 0.165 and 0.127 respectively. Eigenvector centrality accounts for the significance of the neighboring nodes for degree centrality, which means how central and popular the node is. In other words, this measures "how good the network flow is and provides bounds on the diameter of a graph" (Zafarani, Abbasi, & Liu, 2014). The average eigenvector centrality of ISIS was 0.036 and 0.045 for Al-Qaeda actors.

These centrality measures in Figure 3 show a consistent result with the network structures that appeared in Figures 1 and 2. Results indicate that ISIS has a lower degree centrality, and a lower eigenvector centrality than Al-Qaeda, which signifies that ISIS has a larger number of actors in their network, and that actors are connected to a smaller number of nodes compared to Al-Qaeda. That is why the network structure appears to be sparser than Al-Qaeda's cyberterror network structure. In addition, a lower eigenvector centrality shows that key actors in the network of ISIS are less connected to one another as compared to Al-Qaeda.

Findings and Discussion

In this paper, we conducted a three-step analysis to detect networks of national origins of cyber-terrorists and victims, networks of actors in Al-Qaeda and ISIS, and clustered networks of Al-Qaeda and ISIS cyberterrorists. The findings allow us to analyze the offender-victim relations in cyberterrorism incidents and explore how and why Al-Qaeda and ISIS's offender-victim relations have divergent patterns. We investigated in-group and out-group network dynamics by running a network analysis on a unique dataset of 83 cyberterrorism incidents between 2011 and 2016.

This study makes several important contributions to the literature relating to the political implications of the developing phenomenon of cyberterrorism. First, our findings demonstrate the efficacy of a new cyberterrorism database to map network relations between the cyberterrorists and cybervictim countries. Second, the network analyses give rise to two distinct cyberterror strategies operated by Al-Qaeda and ISIS terror cells. Breaking down the analyses dispels the prior oversimplification of cyberterror as a homogeneous terror tactic. Our subsequent discussion below identifies the political and geo-strategic implications of the divergent cyber strategies. Third, we used space transition theory to combine parallel perspectives of political science and criminology to

understand terrorism in the cyber-domain. Finally, we laid the foundation for a new cyber conflict theory that integrates conflict theory with space transition theory to observe how terrorism becomes more complex in nature as terrorists capitalize on the unique characteristics of cyberspace.

The data revealed several similarities and differentiating features between the cyberterrorism strategies and networks operated by Al-Qaeda and ISIS. Both Al-Qaeda and ISIS victims are predominantly the United States and other western democratic countries. In terms of methods of cyberterror, concurrent with previous studies, both Al-Qaeda and ISIS engaged with cyber-resources differently (Awan, 2017; Choi et al., 2018). Regardless of the format of terrorism (whether traditional or cyberterrorism), terrorists and terrorist groups hold different, distinct worldviews than others. Their disagreement shapes how they view the world, their terrorist groups, and other counterparts. This is in line with a conflict theoretical view. Moreover, the data reveals that cyberterror actions are clustered not only by ideology-based terrorist affiliations but also by countries of offenders.

The results of the network analyses of national origins of cyberterror and victim countries, and the distinction we revealed between the Al-Qaeda and ISIS networks, bear significant implications for counter-terrorism strategy, international relations and public policy. First, the data reveals a clear distinction in attacking profiles towards major western countries versusAfrican, Asian and Middle Eastern countries. While cyber terror strikes on the US, UK and France predominantly originate cross-border, the cyberattacks on less wealthy countries largely originate inside their countries. This upends traditional thinking on cyberterror strategy that suggested that cyberattacks take place transnationally in light of the global reach of digital systems and the ability to avoid capture by distancing oneself from the scene of the crime. Despite this widely accepted conception of cyberattacks, the data indicates that there is a threshold of target country power under which this tenet does not hold. At this stage we can only hypothesize about why this is the case, although one obvious proposition is that where countries don't possess sophisticated cybersecurity and intelligence apparatuses, the disadvantage of removing a terror cell temporally and physically from the scene of the crime is higher than the risk of risking a loss of anonymity.

Second, as summarized above, the data reveals stark differences in cyberterror strategies wielded by Al-Qaeda and ISIS. ISIS cyberattack strategy prioritizes multiple low casualty strikes in more countries that are initiated by in-country assailants. Their cyberterror networks have a higher number of actors inside each active network, yet these actors are connected to a smaller number of nodes than Al-Qaeda. Moreover, there are a relatively low number of interactions among the networks reflecting a more isolated and self-contained network structure. By contrast, the Al-Qaeda cyberterror strategy employs more transnational attacks targeting a more concise bank of country targets. Their network structure is denser and more centralized than the ISIS networks, and there are a higher number of interactions within the terror network, reflecting the central control wielded by senior operatives. Even before tackling the implications of this divergent cyber strategy, the fact of its existence is noteworthy. In the realm of conventional (kinetic) terrorism, substantially divergent strategies are widely acknowledged. But the fluidity of digital technology and the immaturity of cyber-offensive theories mean that it is often oversimplified a homogenous practice that merely combines traditional strikes with cyber methods (Jarcis, Macdonald & Whiting, 2017). Our findings reinforce the fact that cyberterrorism, though still in a fledgling form, has already developed multiple strategic approaches that correspond in many ways with conventional terror forms (i.e., centralized / decentralized, locally based / regionally based / internationally based). In the same way that different counter-terrorism approaches would be developed to combat Hezbollah and Boko Haram in light of their dissimilar techniques, so too will an effective counter-cyberterrorism approach need to take account of divergent digital strategies.

Third, it has long been assumed that the fact that cyberterror attacks can be instigated from anywhere with relative impunity and anonymity means that they will be. Yet our data suggests that cyberterror attacks are clustered by countries of origin, indicating a form of regionalism in cyberterrorism. Why would this be the case? There are several theories.

Terrorism remains a highly regional phenomenon that is primarily driven by local factors and ideological considerations (Down & Raleigh, 2013). As most terror groups are concerned with national and regional issues, it makes sense to base their operations within a regional setting. Where cyber terror attacks do transcend regional boundaries, as in the case of Al-Qaeda and ISIS, the origins of the cyberattacks still fall into clustered centers. Possible explanations for this phenomenon include the a) need for particular infrastructure to conduct highly sophisticated international cyberattacks; b) a connection to centralized authorities and support services; and c) freedom for sophisticated and / or antagonistic intelligence services. Whatever combination of above factors explains the clustering factor, the implications are profound for international relations and counter-terrorism strategy as it narrows down the search for cyberterrorists from "the world" to those environments within relatively confined clusters that provide the necessary prerequisites to successfully conduct transnational cyberattacks.

A space transition theory for cyberterrorism would explain many of the patterns the data reveals in relation to the behaviour of conventional terror organizations as they transition from a physical to a cyberspace environment. Though it will require further dedicated theoretical development and research, the findings offer encouraging support for the need and utility of this proffered theory. The three elements of Jaishankar's seminal model that we identified as the relevant variables in a terror environment were changeable identity of offenders, space convertibility and criminal opportunity, and a low risk of detection in cyberspace. These elements combine to rationalize terror behavior in the cyberspace as asymmetric and dissociative conditions enable terror groups with limited resources to combat major powers as an extension of their terror strategies. This is where space transition theory and conflict theory combine in that traditional notions of socially driven conflict premised on the notion of inequality play out on a global and borderless scale. Terror activities act differently in a digital environment due to unique characteristics including an artificially created environment with malleable geography (Shandler, 2019). "Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the flick of a switch" (Rattray, 2009). Under these circumstances, aggrieved organizations – which include terror groups at the extreme end of the scale – can exert significant power. Indeed, communications and activities conducted in cyberspace can be done with minimal risks of identification or detection. Cyberterrorists take advantage of such levels of secrecy to execute political and religious acts of terrorism. A 2020 Europol stressed the importance of prioritizing efforts to mitigate terrorist groups' use of Internet-based media communications for the purpose of formulating, directing, and executing terrorist activities anonymously on a global basis (Europol, 2020).

We acknowledge a related limitation of this database, which is that the database only includes cyberterror attacks that have been officially recorded or identified by the U.S. Department of State. The very nature of cyberterrorism, unlike conventional kinetic terrorism, means that certain cyberattacks can remain under the radar without acknowledgement, attribution or identification. This means that the findings only relate to successful or publicly reported cyberterror attacks.

This study builds on a unique dataset on cyberterror attacks through publicly available information. This data has already proven its utility in analysing previously unspecified patterns of cyberterror cells and developing new theories of cyber behaviour online. Despite this, we strongly encourage the construction of even more sophisticated and comprehensive datasets that includes information on additional terror groups, and the accumulation of other attacker characteristics (socio-demographic, ideological, and technical) that are critical for detecting and policing cyberterror.

Our results indicated that the patterns of cyberterrorism of Al-Qaeda and ISIS are not simple. Not only the countries of source and target are important; internal patterns and activities that shape such patterns also need attention. While national origins and regional boundaries still play a role in cyberterrorism, the nature of cyberterrorism, which is inherently ubiquitous and has a

power to move between physical space and cyberspace, needs to be taken into account. Thus, there is a need for more a systematic attention and examination.

References

Abrahms, M. (2019). The strategic model of terrorism revisited. In The Oxford Handbook of Terrorism (p. 445-457). Edited by Erica Chenoweth, Richard English, Andreas Gofas and Stathis N. Kalyvas. Oxford: Oxford University Press.

Agustina, J. R. (2015). Understanding cyber victimization: Digital architectures and the disinhibition effect. International Journal of Cyber Criminology, 9(1), 35–54.

Archetti, C. (2013). Understanding Terrorism in the Age of Global Media: A Communication Approach. Basingstoke: Palgrave Macmillan.

Arosoaie, A. (2015). Doctrinal differences between ISIS and Al Qaeda: An account of ideologues. Counter Terrorist Trends and Analyses, 7(7), 31–37.

Atwan, A. B. (2015). Islamic state: The digital caliphate. Oakland: University of California Press.

Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. Society 54, 138–149.

Barabási, A.L. (2016). Network Science. Cambridge: Cambridge University Press.

Barry, E. (2015). Al-Qaeda branch claims responsibility for Bangladeshi blogger's killing. New York Times, May 3. https://www.nytimes.com/2015/05/04/world/asia/bangladesh-al-qaeda-indian-subcontinent-attack-on-bloggers.html?_r=0 (Accessed June 6, 2017).

Bright, D., Whelan, C., & Harris-Hogan, S. (2020). Exploring the hidden social networks of 'lone actor' terrorists. Crime, Law and Social Change, 1–18. https://doi.org/10.1007/s10611-020-09905-2.

Byman, D. (2014). Buddies or burdens? Understanding the Al-Qaeda relationship with its affiliate organizations. Security Studies, 23, 431–470.

Campana, P. & Varese, F. (2012). Listening to the wire: Criteria and techniques for the quantitative analysis of phone intercepts. Trends in Organized Crime, 15(1), 13–30.

Campana, P. (2016). Explaining criminal networks: strategies and potential pitfalls. Methodological Innovations, 9(1), 1–10.

Canetti, D., Gross, M., Waismel-Manor, I., Levanon, A., & Cohen, H. (2017). How cyberattacks terrorize: cortisol and personal insecurity jump in the wake of cyberattacks. Cyberpsychology, Behavior, and Social Networking, 20(2), 72-77.

Carley, K.M. (2005). Dynamic network analysis for counter-terrorism.

Chalancon, G., Kruse, K., & Badu, M. M. (2013). Clustering coefficient. In W. Dubitzky, O. Wolkenhauer, K.-H. Cho, H. Yokota (Eds.), Encyclopedia of Systems Biology. New York: Springer (pp. 422–424).

Choi, K. S., Lee, C. S., & Cadigan, R. (2018). Spreading propaganda in cyberspace: Comparing cyber-resource usage of Al Qaeda and ISIS. International Journal of Cybersecurity Intelligence & Cybercrime, 1(1), 21-39.

Conway, M. (2005). Terrorist web sites: Their contents, functioning, and effectiveness. In M. Philip, P. Seib (Eds.), Media and Conflict in the Twenty-First Century. New York: Palgrave Macmillan (pp. 185–215).

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.

Council on Foreign Relations. (2008). Basque Fatherland and Liberty (ETA). November 17, 2008. http://www.cfr.org/separatist-terrorism/basque-fatherland-liberty-eta-spain-separatists-euskadi-ta-askatasuna/p9271 (Accessed November 28, 2016).

Council on Foreign Relations. (2016). Institute for the study of war: Haqqani Network. October 2011. http://www.cfr.org/afghanistan/institute-study-war-haqqani-network/p26126 (Accessed November 28, 2016).

Denning, Dorothy E. 2000. "Cyberterrorism: Testimony before the special oversight panel on terrorism committee on armed services US house of representatives". Washington D.C., May 2000.

Dowd, C., & Raleigh, C. (2013). The myth of global Islamic terrorism and local conflict in Mali and the Sahel. African Affairs, 112(448), 498–509.

Duyvesteyn, I. (2004). How new is the new terrorism? Studies in Conflict & Terrorism, 27(5), 439–454.

Egloff, F. J. (2020) Intentions and cyberterrorism. In Oxford Handbook of Cyber Security, P. Cornish (Ed.). Oxford: Oxford University Press.

Enders, W. & Su, X. (2007). Rational Terrorists and Optimal Network Structure. The Journal of Conflict Resolution, 51(1), 33–57.

Europol. (2020). Online Jihadist Propaganda – 2019 in Review. https://www.europol.europa.eu/newsroom/news/online-jihadist-propaganda-2019-in-review (Accessed July 28, 2020).

Fleisher, M. S. (2006). Youth gang social dynamics and social network analysis: Applying degree centrality measures to assess the nature of gang boundaries. In J. F. Short, Jr. & L. A. Hughes (Eds.). Studying Youth Gangs. Lanham: Alta Mira.

Gaharwar, R. D., Shah, D. B., & Gaharwar, G. K. (2015). Terrorist Network Mining: Issues and Challenges. International Journal of Advance Research in Science and Engineering, 4(1), 33–37.

Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes. Journal of Cybersecurity, 3(1), 49-58.

Gross, M. L., Canetti, D., & Vashdi, D. R. (2016). The psychological effects of cyber terrorism. Bulletin of the Atomic Scientists, 72(5), 284–291.

Grund, T. U. & Densley, J. A. (2012). Ethnic heterogeneity in the activity and structure of a black street gang. European Journal of Criminology, 9(4), 388–406.

Grund, T. U. & Densley, J. A. (2015). Ethnic homophily and triad closure: Mapping internal gang structure using exponential random graph models. Journal of Contemporary Criminal Justice, 31(3), 354–370.

Gunnell, D., Hiller, J. & Blakeborough, L. (2016). Social Network Analysis of an Urban Street Gang Using Police Intelligence Data. Research Report 89. London: The Information Policy Team, The National Archives.

Gustini, R. (2011). Report: FBI warns of Al-Qaeda "hit list". The Atlantic.

Harel, D. & Koren, Y. (2000). A fast multi-scale method for drawing large graphs," GD '00 Proceedings of the 8th International Symposium on Graph Drawing (pp. 183–196). September 20–23, 2000.

Harris-Hogan, S. (2012). Australian neo-jihadist terrorism: Mapping the network and cell analysis using wiretap evidence. Studies in Conflict & Terrorism, 35(4), 298–314. https://doi.org/10.1080/1057610x.2012.656344

Heavy (2016). Watch: New ISIS video message to U.S. shows mass beheading of Syrian soldiers. http://heavy.com/news/2016/03/new-isis-islamic-state-news-pictures-videos-english-language-message-to-united-states-america-president-obama-assad-syrian-soldier-beheading-execution-full-uncensored-youtube/ (Accessed June 6, 2017).

Holt, T. J., Stonhouse, M., Freilich, J. & Chermak, S. M. (2019). Examining ideologically motivated cyberattacks performed by far-left groups. Terrorism and Political Violence, DOI: 10.1080/09546553.2018.1551213.

Jaishankar, K. (2007). Establishing a theory of cyber crimes. International Journal of Cyber Criminology, 1(2), 7–9.

Jarvis, L., Macdonald, S., & Whiting, A. (2017). Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat. European Journal of International Security, 2(1), 64–87.

Jocelyn, C. (2013). Why the West fears Islam: An exploration of Muslims in liberal democracies. New York: Palgrave Macmillan.

Kelly, M. & McCarthy-Jones, A. (2019). Mapping connections: A dark network analysis of Neojihadism in Australia. Terrorism and Political Violence, https://doi.org/10.1080/09546553.2019.1586675.

Klerks, P. (2001). The network paradigm applied to criminal organizations. Connections, 24(3), 53–65.

Koschade, S. (2007). A social network analysis of Jemaah Islamiyah: The applications to counterterrorism and intelligence. Studies in Conflict & Terrorism, 29(6), 559–575. https://doi.org/10.1080/10576100600798418

Magoirk, J., Atran, S., & Sageman, M. (2008). Connecting Terrorist Networks. Studies in Conflict & Terrorism, 31, 1-16.

McIllwain, J. S. (2004). Organizing crime in Chinatown: Race and racketeering in New York City: 1890–1910. Jefferson: McFarland and Company.

Kliegman, A. (2015). Islamic State Affiliate attacks Sinai as Muslim Brotherhood calls for Jihad. January 30, 2015, Center for Security Policy, http://www.centerforsecuritypolicy.org/2015/01/30/islamic-state-affiliate-attacks-sinai-as-muslim-brotherhood-calls-for-jihad/ (Accessed November 28, 2016).

Krebs, V. E. (2002). Mapping networks of terrorist cells. Connections, 24(3), 43–52.

Krueger, A. B. & Malečková, J. (2003). Education, Poverty and Terrorism: Is There a Causal Connection? Journal of Economic Perspectives, 17(4), 119–144.

Lachow, I. (2009). Cyber terrorism: Menace or myth. Cyberpower and national security, 434-467.

LaFree, G., & Dugan, L. (2016). Global terrorism and the deadliest groups since 2001. Peace and conflict, 2016, 67.

Leaksource (2014). "Islamic State claims beheading of former U.S. Army Ranger/aid worker Peter Kassig," https://leaksource.wordpress.com/2014/11/16/graphic-video-islamic-state-claims-beheading-of-former-u-s-army-rangeraid-worker-peter-kassig/ (Accessed June 6, 2017).

Luiijf, E. (2014). Definitions of cyber terrorism. In Cyber Crime and Cyber Terrorism Investigator's Handbook (pp. 11–17). Syngress.

Mair, D. (2017). #Westgate: A case study: How Al-Shabaab used Twitter during an ongoing attack. Studies in Conflict & Terrorism, 40(1), 24–43.

Marx, K. (1859) [1971]. A contribution to the critique of political economy. Translated by S. W. Ryanzanskaya and edited by M. Dobb. London: Lawrence & Whishart.

Mastrobuoni, G. & Patacchini, E. (2012). Organized crime networks: An application of network analysis techniques to the American mafia. Review of Network Economics, 11(3), Article 10.

McGloin, J. M. & Piquero, A. R. (2010). On the relationship between co-offending network redundancy and offending versatility. Journal of Research in Crime and Delinquency, 47(1), 63–90.

McGloin, J. M., Sullivan, C. J., Piquero, A. R. & Bacon, S. (2008). Investigating the stability of co-offending and co-offenders among a sample of youthful offenders. Criminology, 46, 155–188.

McGloin, J. M. (2005). Policy and intervention considerations of a network analysis of street gangs. Criminology and Public Policy, 4(3), 607–636.

Morselli, C. (2003). Career opportunities and network-based privileges in the Cosa Nostra. Crime, Law and Social Change, 39(4), 383–418.

Morselli, C. (2009). Inside Criminal Networks. Studies of Organized Crime. New York: Springer.

Natarajan, M. (2006). Understanding the structure of a large heroin distribution network: A quantitative analysis of qualitative data. Journal of Quantitative Criminology, 22(2), 171–192.

National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland (2020). Global Terrorism Database. https://www.start.umd.edu/gtd/ (Accessed July 15, 2020).

National Counterterrorism Center (NCTC). (2014). Haqqani Group – Al-Qaeda Linkage, https://www.nctc.gov/docs/2014_worldwide_threats_to_the_homeland.pdf (Accessed December 6, 2016).

Neumann, P. R., & Smith, M. L. R. (2007). The strategy of terrorism: How it works, and why it fails. Routledge.

Ogun, M. N. (Ed.). (2015). Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses (Vol. 42). IOS press.

Papachristos, A. V. (2009). Murder by structure: Dominance relations and the social structure of gang homicide. American Journal of Sociology, 115(1), 74–128.

Park, S. J., Lim, Y. S. & Park, H.W. (2015). Comparing Twitter and YouTube networks in information diffusion: The case of the "Occupy Wall Street" movement. Technological Forecasting & Social Change, 95, 208–217.

Perliger, A. & Pedahzur, A. (2011). Social network analysis in the study of terrorism and political violence. PS: Political Science and Politics, 44(1), 25–50.

Qvortrup, M. (2015). T-Test for terrorism: Did the introduction of proportional representation reduce the terrorist threat? A time-series case study of Algeria and Northern Ireland. Studies in Conflict & Terrorism, 38(5), 293–304.

Rattray, G. J. (2009). An environmental approach to understanding cyberpower. In Wentz, L. K., Starr, S. H., & Kramer, F. D. (2009). Cyberpower and National Security: (Vol. 1st ed., pp. 253 – 274). Potomac Books.

Reiss, A. J. Jr. & Farrington, D. P. (1991). Advancing knowledge about co-offending: Results from a prospective longitudinal survey of London males. Journal of Criminal Law and Criminology, 82(2), 8202–8360.

Roberts, N., Everton, S.F. 2011. Strategies for combating dark networks. Journal of Social Structure, 12, 1–32.

Roggio, B. (2011). US adds Islamic Caucasus Emirate to list of terror groups. Long War Journal, May 26, 2011, http://www.longwarjournal.org/archives/2011/05/us_adds_islamic_cauc.php (Accessed March 20, 2020).

Rozentsvaig, A. I., Kovalenko, K. E., & Gubareva, A. V. (2018). Basic approaches and definitions of international cyberterrorism. Revista QUID, (2), 120–124.

Rudner, M. (2017). 'Electronic Jihad': The Internet as Al-Qaeda's catalyst for global terror. Studies in Conflict & Terrorism, 40(1), 10–23.

Sardarnia, K., & Safizadeh, R. (2019). The internet and its potentials for networking and identity seeking: A study on ISIS. Terrorism and Political Violence, 31(6), 1266-1283.

Sarnecki, J. (2001). Delinquent Networks: Youth Co-offending in Stockholm. Cambridge: Cambridge University Press.

Shandler, R. (2019). White Paper: Israel as a Cyber Power. DOI: 10.13140/RG.2.2.15936.07681.

Silber, M. D., Bhatt, A., & Analysts, S. I. (2007). Radicalization in the West: The homegrown threat (pp. 1-90). New York: Police Department.

Sterman, D. (2015). Don't dismiss poverty's role in terrorism yet. February 5, 2015, Time, http://time.com/3694305/poverty-terrorism/ (Accessed September 25, 2017).

Suler, J. (2004). The online disinhibition effect. Cyberpsychology & behavior, 7(3), 321-326.

Turk, A. (1969). Criminality and Legal Order. Chicago: Rand McNally.

US Dept of State, & United States of America. (2012). Country Reports on Terrorism 2011.

US Dept of State, & United States of America. (2013). Country Reports on Terrorism 2012.

US Dept of State, & United States of America. (2014). Country Reports on Terrorism 2013.

US Dept of State, & United States of America. (2015). Country Reports on Terrorism 2014.

US Dept of State, & United States of America. (2016). Country Reports on Terrorism 2015.

US Dept of State, & United States of America. (2017). Country Reports on Terrorism 2016.

Van Mastrigt, S. B. & Farrington, D. P. (2009). Co-Offending, age, gender and crime type: Implications for criminal justice policy. The British Journal of Criminology, 49(4), 552–573.

Walther, O. J., & Christopoulos, D. (2014). Islamic terrorism and the Malian rebellion. Terrorism and Political Violence, 27(3), 497–519.

Weimann, G. (2015). Terrorism in Cyberspace: The Next Generation. Washington, D.C.: Woodrow Wilson Center Press and New York: Columbia University Press.

Yalibnan (2014). Free Sunnis of Baalbek Brigade pledges allegiance to IS Caliphate. June 30, 2014. http://yalibnan.com/2014/06/30/free-sunnis-baalbek-brigade-pledges-allegiance-caliphate/ (Accessed November 28, 2016).

Zafarani, R., Abbasi, M.A, & Liu, H. (2014). Network measures. In Social Media Mining: An Introduction, Zafarani, R., Abbasi, M.A, & Liu, H. (Eds.). Cambridge: Cambridge University Press (pp. 51–79).

Zehoral, I. (2018). The Richest Terror Organizations in the World. Forbes. Accessed at: https://forbes.co.il/e/the-richest-terror-organizations-in-the-world/.

Zelin, A. Y. (2013). Foreign jihadists in Syria: Tracking recruitment networks. Policywatch 2186, Washington D.C.: The Washington Institute for Near East Policy, 3-4.