APPLICATION OF ROUTINE ACTIVITY THEORY TO CYBERCRIMES IN THE EXTREMIST CYBERCRIME DATABASE

By

Elizabeth Mae Griffith

A THESIS

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

Criminal Justice – Master of Science

2024

ABSTRACT

Routine Activity Theory was first proposed in 1979 as one of the first situational explanations of crime. Later on, four factors of target suitability were further defined by the theory's originators. The rapid and recent development of cybercrime has meant that application of this theory's components to cyberattacks is still rather limited. This study will contribute to this growing literature, focusing especially on the relationship between several target characteristics and the perpetrator's nation-state sponsorship in committing the cyberattack. Target type, attack isolation, and vulnerability use were used to measure the proposed target suitability, against perpetrator state-sponsorship. Motivation, group affiliation, technical skills, and attack type were used as controls. Logistic regression with no control variables proved a weak fitting model (Pseudo $R^2 = 0.094$). Various models with differing controls led to a range of model fits, including better and worse models (Pseudo $R^2 = 0.152 – 0.423$). However, a final model with only significant control variables proved the best fit (Pseudo $R^2 = 0.607$). Given these results and based on this dataset, routine activity theory may not provide the best explanation for nation-state sponsored cybercrime target selection. More research will be needed to find the best criminological explanation for cybercriminal perpetrator motivation.

TABLE OF CONTENTS

INTRODUCTION

This study examines whether perpetrator motivation in nation-state cyberattacks are different from perpetrator motivation in non-nation state cyberattacks. The differences between these two types of attacks are examined using routine activity theory (RAT framework). This will be done through the use of data from the Extremist Cyber Crime Database (ECCD). The dataset contains attack, victim, and perpetrator level data for cyberattacks committed against targets in the United States from 1998-2018 (Holt T. J., Chermak, Freilich, Turner, & Greene-Colozzi, 2022). The cases are ideologically motivated attacks which involve misuse of computer technologies. Although gathered from open-source data, several precautions were taken during data collection to ensure the maximum quality possible, including review of all available sources on the same scheme and review of collected data by project managers before addition to the master dataset (Holt T. J., Chermak, Freilich, Turner, & Greene-Colozzi, 2022).

The study is significant for several reasons. First, new technologies and the use of these technologies to communicate have had a profound impact on the world. The internet has impacted the way that people engage and interact with one another, revolutionized how policymakers, industry leaders, and criminal justice officials think about their work, and created new opportunities to think about and try to solve difficult social problems. It is also not surprising that, although many positive outcomes have occurred because of these changes, there are numerous downsides, especially in how individuals and groups have attempted to use them to do criminal harm.

Second, scholars have tried to make sense of these changes and there is a growing body of literature about internet-related crimes, and some thoughtful work on cybercrime and cyberterrorism. As the work on cybercrime and cyberterrorism is a relatively new research area,

the hope of the present project is both to contribute some insights to this area and prompt further research and thus provide a better understanding of the phenomenon of both cybercrime and cyberterrorism.

Third, such crimes cause a significant amount of harm. Cyberterrorism, for example, is known to have wide-ranging impacts. For governments, a cyberattack occurring in their jurisdiction has been shown to reduce public confidence in the government's ability to protect against threats (Shandler & Gomez, 2022). Due to the high pace, evolving nature of cyberattacks and the digital space in general, governments may struggle to defend against these attacks or at least prevent them from being publicly announced. An impact of cyberterrorism that is more easily quantified is the financial impact to targets of an attack. One study limited to hospitality businesses found significant negative returns on publicly listed hospitality companies after announcing a cyberattack (Arcuri, Gai, Ielasi, & Ventisette, 2020). There can be more direct impacts as well in the case of ransomware attacks, which involves the capture and encryption of an organization's data, only returning it upon payment of the ransom amount. Cybersecurity firm Mandiant estimated the average ransomware payment at over $150,000 and increasing annually in 2020. The same group estimated that over half of targets paid the demanded amount (Mandiant, 2022)..

Fourth, a 2023 review by Holt found that an increasing amount of literature is being published on cybercrime, but not necessarily covering all areas of study (Holt T. J., 2023). For example, Holt discusses that studies on hacking tend to focus on simpler methods such as password cracking in a limited context and timeframe. Holt suggests that the use of alternative data sources could improve understanding of cyberattacks performed on behalf of nation-states or ideological causes (Holt T. J., 2023). One area of great potential for the study of cybercrime

is the use of open source methodologies. Scholars have increasingly used such methodologies to study terrorism, mass shootings, school shootings, and other hard to discover crimes (citations). This study analyzes the Extremist Cyber Crime Database—the first of its kind national database that documents the characteristics of ideological-motivated cybercrime and cybercriminals. This study will go beyond the previous studies, as the data includes several varieties of complex cyberattacks over a twenty-year time period, thus attempting to fill this identified gap in the literature.

Fifth, another contribution is the application of Routine Activity Theory to an area in which it has rarely been applied. Routine Activity Theory has been used to study a large number of crimes, but this research attempts to extend it as a framework to utilize in cybercrime research. As the theory has evolved over time, it is useful to know how applicable it is to emerging fields of criminal activity. Some studies have applied RAT to cybercrime to some degree. Holt & Bossler (2009) studied if RAT accurately estimated the occurrence of online harassment victimization based on expected factors of guardianship and found some support for RAT in cybercrime. They concluded that RAT would be most successfully applied to specific cybercrimes and probably not to entire typologies (Holt & Bossler, 2009). Later studies found support for RAT principles in web defacements (Holt, Leukfeldt, & Weijer, 2020). Other studies have reviewed the components of RAT applied to several different cybercrimes and similarly found that RAT does not serve as an overarching explanation for these crimes (Leukfeldt & Yar, 2016). This study will extend this work by examining the differences across perpetrator type (nation-state v. non nation state) to further verify these previous findings on RAT and cybercrime.

Finally, this research has policy implications. The results from this study could help identify online behaviors or patterns that could be indicative of future targeting in a nation-state sponsored cyber incident and/or radicalization. These identified online behaviors or patterns could be shared with various social institutions to help deescalate radicalization and prevent individuals from going as far to engage in nation state affiliated cyber incidents. Nation-state cybercrime has been identified in the literature to occur for strategic or advantage purposes, whereas non-nation-state sponsored cybercrime typically focuses on revenue (Ahmad, Webb, Desouza, & Boorman, 2019) (Mansfield-Devine, 2020). This study will test some of the previous literature and help differentiate leading factors of a nation-state sponsored cyberattacks.

The thesis will be structured as follows. First, a review of the existing literature on cybercrime, terrorism, and cyberterrorism. Then, review of how terrorists and extremists have used the internet to date and how nation-states have interacted with these activities. Next, a review of Routine Activity Theory and how it has been applied to cybercrime and terrorism. Following that, information on the method of the study and the data used. Finally, a discussion of the results, limitation, further study needed and conclusion.

LITERATURE REVIEW

First, I will discuss the literature related to extremists' use of the internet historically. This will include defining the terms to be used in the study. Then, I will cover existing literature on why extremists' use the internet. Finally, I will cover existing literature on the perpetrators of cybercrime and gaps in the previous research.

Section 1. Extremists' Use of the Internet

Definitions and Concepts

Historically, it has been difficult to define cybercrime when compared to other types of crime. A universal definition for the crime does not yet exist, and definitions and concepts of the crime are always evolving and being debated. In 2006, Gordon and Ford defined cybercrime as being "any crime that is facilitated or committed using a computer, network, or hardware device" (Akdemir, Sungur, & Basaranel, 2020). For the purposes of this study, cybercrime will be defined using Gordon & Ford's definition. As will be discussed in the study methods later, crimes facilitated by a computer and carried out in the physical world are included in the data. This makes Gordon & Ford's definition the most useful of existing definitions for this study.

A universal definition of terrorism also has yet to be accepted by experts in the field, leading to inconsistencies in how acts of terrorism are identified and dealt with by judicial systems (Scrivens & Gaudette, 2021).

In resolution 1566 (2004), the UN Security Council put forth their own definition of terrorism as being:

> "…criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a

population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism…" (Saul, 2015).

The UN definition of terrorism will be used for the purpose of this study. The definition does not require a certain motivation or background of the offender, and the data used in this study includes suspects of many backgrounds, which will be further discussed in the methods. Due to these reasons, the broad definition of terrorism published by the UN will be suitable for this study.

Extremism has similarly evaded definition by many institutions and researchers. However, some academics have proposed definitions and this study will choose to use a definition for the term to differentiate extremism from terrorism and recognize the wide variety of beliefs that could be extremist and may be included in the study data. This definition was proposed by Hassan, et. al. in a philosophical argument: "Extremism is a position of a radical nature with the aim of challenging or changing a status quo, and which can be held by an individual or a group, which is about political or non-political subject matter, and which can have both positive or negative applications, and that is held in a resolute manner" (Hassan, Farine, Kinnish, Mejia, & Tindale, 2023).

Extremists' and Terrorists' Use of the Internet

In recent years, terrorists and violent extremists have adopted the internet for several purposes. In the earlier days of the internet, the expanded communications abilities of email and blogs were quickly adopted by terrorist groups as it was faster, cheaper, and had wider reach than previous communication methods they had utilized (Weimann, 2006). As the years progressed and the internet and technology expanded to include a wider variety of services, terrorists took

advantage of each new option for their own nefarious purposes. One researcher tracked over time that the number of websites operated by terrorist organizations rose from just a dozen in the 1990s to almost 7,000 in 2009 (Kaplan & Weimann, 2011). The use of the internet for these groups evolved over time to include organizing groups, recruitment for physical attacks, and advanced methods of money transfer (Piazza & Guler, 2019). The structure behind many of these online systems can be adopted very quickly by terror groups and other extremists, making them ideal for use. Although research is limited, violent non-state actors have been found to be early adopters of new technologies and methods of using such technologies. One study from 2019 found that the success of ISIS (Islamic State of Iraq and Syria) in the early 2010s could be attributed to its early use of unmanned drones and social media for communication and recruitment (Gartenstein-Ross, Shear, & Jones, 2019). A variety of other extremists have used the internet include the Ku Klux Klan (KKK). One study from 2004 found that the KKK was using the internet for community building and encouraging violence on its websites. Other analyses of previous literature have found varying claims of the reach of terrorists on the internet, up to and including that all designated foreign terrorist organizations have an internet presence (Lennings, Amon, Brummert, & Lennings, 2010). Additional research on ranges of extremist groups has found that a large majority of all groups had an online presence (Holt, Freilich, Chermak, & McCauley, 2015).

Section 2. Why Extremists Use the Internet

As discussed, extremists have adapted to the growing use of the internet. While internet usage has provided great benefit to society, nefarious actors have been able to take advantage of several internet functions for malicious purposes. Next, I will discuss why and how extremists use the internet.

What Information is Available on the Internet

The internet has become a widespread forum of many purposes. Some of the many uses include communication via blogs and other websites, payment methods which may be traditional or untraceable, and provision of information. The internet allows for faster information transmission across broader area than previous communication methods. Networking and coordination are also crucial processes that can be facilitated by the internet. People do not have to travel and meet up to create a network or plan physical activities (Conway, 2006). Each of these functions of the internet can be utilized by extremists online.

Recruitment and Communication

Several extremist and terrorist groups have used the internet to recruit and radicalize new members. For example, as the group attempted to ramp up physical operations, ISIS turned to the internet, particularly social media, to recruit new fighters from around the world to come fight for the group (Piazza & Guler, 2019). ISIS' online recruitment allowed for a wider variety of members in the group to help various efforts as the group attempted to both expand and legitimatize itself. Those coming from foreign nations would be brought to separate training camps from native fighters to determine if they were spies and if they had some special skill to offer (Gates & Podder, 2015). Other extremist groups use the internet in a similar fashion to promote communication that might not otherwise occur if the internet were not available to them (Bowman-Grieve, 2009). One study of a right-wing extremist website found several elements including discussion of movement literature, sharing personal stories and grievances, and calls to action that led the researchers to label it a community of practice for terrorism (Bowman-Grieve, 2009). The internet facilitates these types of communities in a way that would have required significantly more effort to arrange in physical space.

Social Media and Propaganda

Social media use by terrorists may date to the beginning of social media. Several researchers studied Al-Qaeda blogs and the terror group's move to social media platforms as they became available (Rudner, 2016). (Lennings, Amon, Brummert, & Lennings, 2010). Social media can be flooded by terrorist groups who utilize bots to automatically post content. It has been estimated that 20% of ISIS-related tweets per day were being generated by bots or apps (Jurich & Kayaalp, 2017). With extremists creating new accounts that post automatically, it can become extremely difficult to keep up with content moderation (Jurich & Kayaalp, 2017). Given the user base of Twitter at the time, this exposes a large global audience to a significant volume of propaganda beyond posting on a blog or website, and well beyond publishing a newspaper or handing out flyers (Jurich & Kayaalp, 2017).

Another way in which terrorists and violent extremists utilize social media is by documenting and archiving violent extremist events. One example of this, shown in a 2022 research study, was several threads on social media forum Reddit created specifically to archive the details of the U.S. Capitol insurrection of January 6th, 2021 (Harel, 2022). The author noted that some elements of a traditional archive were missing from these pages, but nevertheless they did serve as a place to document and memorialize an extremist event for future reference (Harel, 2022). Additionally, a large amount of the materials included pictures and videos of the event from those perpetrating the invasion (Harel, 2022). This is a type of documentation and access that would likely have been impossible before widespread use of the internet.

Fundraising

It has been posed by researchers that the main methods of money transfer for ISIS have been cryptocurrencies and prepaid cards (Shostak, 2017). These methods avoid anti-money

laundering regulations that other transfer methods might be subject to. Using the internet also allows extremists to expand their possible sources of funding if they are seeking private donors, or to arrange illicit sales previously discussed. Secure dark web marketplace sites serve as an ideal location for ISIS fighters to list for sale and arrange sales and payment for artifacts stolen during physical operations (Paul, 2018).

Moving from Physical Terrorism to Cyberterrorism

Cyberspace can also be utilized by terrorist groups to coordinate and amplify their physical operations. For example, taking advantage of the cyber space allowed ISIS to increase its reach more quickly than other terrorist groups and maintain a significantly larger audience for an extended period. As the United States and other nations moved in to take over ISIS' land claims, the group's leaders maintained that they would never be defeated, "only if you were able to remove the Koran from Muslims' hearts" (Liang, 2017). The group's change of mission by moving online was reflected in ISIS' English language magazines, which saw a shift to more state-building focused imagery vs. military-focus imagery, as determined by one research team (Kaczkowski, Winkler, Damanhoury, & Luu, 2021). Organizations can also be targeted virtually via data breaches or other means to instill the most fear in the general population. They can more easily deal with other terrorist groups, such as Shadow Brokers, who stole software from the NSA and attempted to sell it off online for Bitcoin. Acquisition of these tools would allow much faster proliferation for the group, since it is lacking nation-state support and is many years behind on research and development of new weaponry (Rudner, 2016).

Far-left groups have also been found to use both cyber and physical attack methods and relate the two together. One study found that cyberattacks by far-left groups increased as physical attacks decreased in the 2010s. There are several proposed ideas behind this, including

lower risk of being caught online and an equivalent emotional response to these ideologically motivated attacks. That is to say, the attackers may have felt they were achieving their goals during a cyberattack as much as a physical attack (Holt, Stonhouse, Freilich, & Chermak, 2021).

Section 3. Perpetrators of Cybercrime

Existing research is limited on the motivations of cyber actors due to their overall desire for anonymity. However, a handful of studies have looked at perpetrator's motivations for committing an attack. One well-known repository of defacements allows hackers to self-report their attack along with their reasoning. This data was obtained by Holt, Leukfeldt, and Van De Weijer (2020) to study the motivations of cyber attackers and any relationship with target selection that could be determined (Holt, Leukfeldt, & Weijer, An Examination of Motivation and Routine Activity Theory to Account for Cyberattacks Against Dutch Web Sites, 2020). The study found that attackers with ideological motives were more likely to target the homepage of a website, while those looking for entertainment or other reasons were more likely to attack secondary webpages. Additionally, those who cited patriotism as their reasoning were more likely to use mass defacement, changing the content of many webpages at once for the most visibility (Holt, Leukfeldt, & Weijer, An Examination of Motivation and Routine Activity Theory to Account for Cyberattacks Against Dutch Web Sites, 2020). The authors noted findings from other areas of criminological research that appeared to align with the findings. Differences in motivation will be studied further in this thesis as actors with nation-state sponsors will likely have different motivations than those that offend for other reasons. For this study, target type will be used to test visibility and value as previous literature indicates that nation-state sponsored attackers will select higher value targets.

Cybersecurity media has noted that target selection and motivation could be different than one may suspect when it comes to nation-state attackers. These sophisticated actors will work their way through the entire supply chain to the point of, as one example illustrated, attacking adhesive companies in an attempt to eventually take over stamp production (Mansfield-Devine, 2020). It certainly follows logic that professional hackers working for military unit, for example, would not be utilizing ransomware because they are being paid a salary to commit the attack and would be instructed to remain undetected (Mansfield-Devine, 2020). These motivations were also considered in the development of the thesis' hypotheses.

Far-left groups have also been found to use both cyber and physical attack methods and relate the two together. One study found that cyberattacks by far-left groups increased as physical attacks decreased in the 2010s. There are several proposed ideas behind this, including lower risk of being caught online and an equivalent emotional response to these ideologically motivated attacks. That is to say, the attackers may have felt they were achieving their goals during a cyberattack as much as a physical attack (Holt, Stonhouse, Freilich, & Chermak, 2021). This finding, while not directly tested in this study, will be included in the control variables as motivation was recorded in the dataset.

Nation-States and Cyberattacks

The phenomenon of nation-state cyber threats has been described using multiple terms. The most common of these is Advanced Persistent Threat (APT). There are varying definitions of what constitutes an APT in the literature, but one study from 2019 proposed a broad definition:

> "An entity that engages in a malicious, organized, and highly sophisticated long-term or reiterated network intrusion and exploitation operation to obtain information from a target organization, sabotage its operations, or both."

This definition was intended to highlight the main factors that define an APT while leaving enough room in the definition to include a variety of groups (Ahmad, Webb, Desouza, & Boorman, 2019). Other definitions include that an external source is supporting the goals and funding of the organization. While this could be a variety of entities, nation-states and militaries have been some of the organizations linked to APTs in the past by cybersecurity groups (Ahmad, Webb, Desouza, & Boorman, 2019).

State-sponsored cyberattacks are committed for various reasons. A preliminary study of data from 2005-2012 found that nation-states were more likely to initiate a cyberattack if they had higher measures of power or authoritarianism (Hunter, Albert, & Garrett, 2021). This analysis failed to find any additional associations that could explain the initiation of cyberattacks. Additionally, political researchers have recognized the changing role of nation-states in cybersecurity over time from security and knowledge to slowly include regulation and perpetration (Cavelty & Egloff, 2019). However, data and study of the differences between nation-state sponsored cyber attackers and non-sponsored attackers has been very limited overall due to a lack of data. That is, until the introduction of the Extremist Cyber Crime Database in 2022 (Holt T. J., Chermak, Freilich, Turner, & Greene-Colozzi, 2022). The full details of this dataset are included in the Methods section, as this is the data used for this study. Important for the literature review is that this data includes perpetrator- and suspect-level characteristics on a wide range of cyberattacks. This allows for comparison between the two perpetrator groups: nation-state sponsored and non-sponsored cyber attackers.

State-sponsored cyberattacks have been extremely difficult to prove. Several private firms, including FireEye and Mandiant, have undertaken the process of attempting to connect attacks to specific geographic areas and potential sponsors/funders. Mandiant has a list of number APT groups and suspected attributions based on target selection, tactics used, time of attacks, frequently used tools, and other factors (Mandiant, 2023). Researchers have noticed the issue attributing cyberattacks from a technical evidence perspective and noted that attempting to publicly attribute attacks carries significant political risks if done by another nation-state (Egloff F. J., 2020). Therefore, it is important to recognize that attribution may be undesirable even when it is possible.

The definition and attribution of APT actors highlights a link to the theoretical propositions tested in this study. Persistence (inertia) and value of targets are two components that determine target selection in RAT as discussed later in *Theory*. In the data, persistence is recorded through linked or chronic attacks, and this warrants the inclusion of this variable in the analysis.

Academic literature on specific threat actors is extremely limited due to difficulties proving attribution via peer review. Reputable information from expert cybersecurity firms is used instead to discuss specific APTs. Mandiant was owned by FireEye from 2013-2021, when it was sold to Google (Shead, 2022). Mandiant's 2022 trend report identified 40 APT groups total, with only 6 active groups from China, Iran, and Vietnam. The researchers also identified 339 uncategorized cyber threat groups attributed to a range of other nations including Russia, North Korea, and Turkey (Shead, 2022). The limited research in this area seems to indicate that China, Russia, Iran, and North Korea of the top nation-state threats of concern.

Mandiant estimates that Chinese state-sponsored cyberattacks began in earnest with the matriculation of Xi Jinping in 2012, although some attribute earlier attacks the Chinese military. APT1, the first threat group defined by Mandiant, was believed to be comprised mostly of Chinese military members in a cyber unit. In 2018, the United States indicted two members of APT10, also believed to be Chinese-sponsored and include government employees. Although nothing has come of this particular action, there are heavy implications that the US and China have been in constant cyber warfare for many years (Mandiant, 2022). Russian cyberattacks have also originated from multiple APT groups over the last several years. Some of the most high-profile included alleged misinformation campaigns leading up to the US presidential election in 2016. Russian cyber attackers were identified by Mandiant based on target selection comparison to Russian political and military targets (FireEyre iSight Intelligence, 2017). Iran's cyber capabilities are typically tied back to the Stuxnet malware that was used against it by the United States. This malware was used to degrade Iranian nuclear facilities, and this has been seen as a provocation to which it is retaliating. The Iranian's use of cyberattacks show another relationship between the physical and digital criminal worlds, as many of their attacks are related to physical systems such as industrial control and electrical grid infrastructure (Mitre, 2022). North Korean attackers have been targeted mainly at South Korea companies and government infrastructure. APTs such as Lazarus Group have been identified as being sponsored by the North Korean state (Mitre, 2022).

While existing literature has explored the use of cyberattacks by extremists and terrorists and the details of the incidents, there is still much to be answered. Research on the perpetrators is mainly focused on identification and attribution of attackers for specific incidents. However, this does not fully address the differences amongst them on the whole. Are ideologically motivated

cyberattacks frequently sponsored by nation-states or not? When they are, what differences exists in the target selection that may help with attribution and prevention of such attacks in the future? Can existing theoretical models of crime be utilized to explain these attacks? These questions will be addressed using the routine activity theory framework in the remainder of this thesis.

THEORY

In this section, I will discuss each of the key concepts in Routine Activity Theory as it was originally conceptualized. Then, I will discuss how it has been applied to the relevant areas of cybercrime and ideologically motivated crimes, and through which variables I will study these factors in this study. Then, I will summarize this literature to re-iterate this study's contribution to the existing literature.

Overview

Routine activity theory (RAT) was first devised by Lawrence E. Cohen and Marcus Felson in their 1979 article "Social Change and Crime Rate Trends: A Routine Activity Approach" and was then further developed by Felson in later years. When first developed and introduced, Cohen and Felson's theory was unique in the fact that it focused on the situational context of crime rather than characteristics of offenders or victims like nearly all other criminological theories were focused on at the time (Hollis-Peel, Reynald, van Bavel, Elffers, & Welsh, 2011).

The theory revolves around three elements: a likely or motivated offender, a suitable target, and the absence of a capable guardian. Cohen and Felson state that when these three elements converge in both time and space, a crime is more likely to occur (Cohen & Felson, 1979). Routine activities themselves are considered the frequent and recurring activities an individual or population needs to survive and thrive. Routine activities could occur in any given place; however, they are dependent upon the daily practices of any given individual. It is these routine activities that allow for an offender and target to meet (Hollis-Peel, Reynald, van Bavel, Elffers, & Welsh, 2011). Since the conception of RAT, it has become one of the most widely cited criminological theories and has influenced numerous other conceptual frameworks (Miró,

2014). The theory has faced much analysis and has been the subject of a multitude of research studies to test its relevance in the field of criminal justice, thus, the operationalization of theory and its main elements have been subject to change over time (Hollis-Peel, Reynald, van Bavel, Elffers, & Welsh, 2011).

The Likely Offender

Cohen and Felson formed the concept of the likely offender, which is an individual who has both the motivation and the ability to commit a criminal act (Cohen & Felson, 1979). In the initial proposal of RAT, the term 'motivated offender' was used to describe this type of individual; however, the terminology 'likely offender' was later used because Cohen & Felson believed that the situational context and physical elements that allowed for a crime to be committed was more important than the offender's motivation to engage in criminal behavior (Miró, 2014). Additionally, motivation of the offender is always assumed, thus the term 'likely offender' makes more sense when operationalized.

Although an offender is assumed to always be motivated, there is still value to knowing what is motivating said offender. Traditionally, because RAT focuses on the situational context of crime, motivation is mostly ignored. When applying the theory to cybercrime, this trend tends to continue (Yar, 2005). However, for this study, motivation is included as a control factor because it may explain the differences between perpetrators of state-sponsored and non-sponsored cyberattacks. This is not a completely new idea to the field. For example, a 2022 study used RAT to see whether web defacements associated with Jihadi beliefs varied from all other web defacements. The study concluded that Jihadi cyberattacks were generally uncommon, that they were more likely to deface organizational websites than non-Jihadi associated defacers, and that they were more likely to use higher-skill attack methods (Holt, Turner, Freilich, & Chermak,

2022). Understanding more about the likely offender is useful, although this study attempts to look at this through characteristics of the targets.

The Suitable Target

A suitable target is defined as being a person, property, or object that a likely offender is able to cause harm against (Miró, 2014). The more suitable a target is determined to be, the higher the probability of victimization becomes. When discussing target suitability, there are four components that are considered: value, inertia, visibility, and accessibility. These four elements are often referred to as VIVA when discussing target suitability. The concept of VIVA will be a critical component of this study and analysis.

The value of a target refers to how desirable the target is in the eyes of a potential offender. This desirability could stem from the target's monetary or symbolic value (Felson & Cohen, 1980). In the case of cybercrimes, there could be either or both types of value from certain targets. The value of a target in the physical world varies on several factors; cybercrime follows the same pattern (Yar, 2005). Because of this, many cybercrime studies do not attempt to measure the potential value of targets. However, other ideologically motivated crimes have been studied by the use of target value. A study on ideologically motivated homicides proposed that ideologically motivated perpetrators were less likely to have known each other previously (Parkin & Freilich, 2015). This study implied that ideologically motivated offenders were more likely to see the value of a potential target in symbolic reasoning. For this study, government and military targets are seen to have a higher value to nation-state sponsored cyber attackers because this would advance political and ideological goals more effectively, thus providing more value to the state-sponsored offender than those which are not sponsored. The non-state attackers find more value out of financially driven attacks because they are not being paid to commit them.

The inertia of a target refers to any characteristic of the target that may make it more difficult to attack (Felson & Cohen, 1980). Related to the physics definition, an individual, object, or property that is perceived to have greater inertia is often considered a less suitable target because they would be more difficult to discreetly move and control (Miró, 2014). In the case of a human target, inertia could be the size or strength of the potential victim. Usage of this component in cybercrime has been less common because online content does not have a measurable physical weight (Yar, 2005). However, some studies have found varying support for inclusion of this factor to account for cybercrimes. A study of web defacements found that inertia may have some effects in cybercrime, because targets can be revictimized – in that case, by redefacement of the same website (Holt, Leukfeldt, & Weijer, 2020). For the data in this study, attacks were recorded as an isolated, linked, or chronic attack. This variable will be used to operationalize inertia and its potential contribution to target selection based on perpetrator motivation.

The visibility of a target refers to how noticeable a potential target is to a likely offender. When a potential target has a higher visibility, the likelihood of victimization increases (Kao & Kluaypa). For instance, an individual who is extremely active on social media and shares significant information about their daily life and whereabouts may be more likely to experience stalking than somebody who has no social media and does not share personal information online. This may also be applicable in some cybercrimes. A study on internet consumer frauds found some support for this usage of visibility, proposing that offenders could learn more about potential targets if they had a more active online presence (Wilsem, 2013). Visibility has been used in several cybercrime contexts, with some studies finding that certain motivation types,

including ideological, were associated with higher visibility targets (Leukfeldt & Yar, 2016) (Holt, Leukfeldt, & Weijer, 2020).

The accessibility of a target refers to how suitable the target's placement is for potential criminal activity. If the target is a physical person, accessibility could pertain to the convenience of their location (Felson & Cohen, 1980). Accessibility in cyberspace has been used for certain types of attacks. In a study of defacements previously referenced, website home pages were considered more accessible than those that required clicking through one or more sub-pages. This hypothesis found mixed support in the data based on the available perpetrator information (Holt, Leukfeldt, & Weijer, 2020). Accessibility in this study is measured as using a vulnerability to commit the attack. A vulnerability represents a target that is easier to access.

The Capable Guardian

The third original element of RAT is the capable guardian, which are individuals or tools within society whose presence make it more difficult to execute a crime. The function of a guardian has always been to decrease the suitability of a target through way of preventative measures such as surveillance or informal social control (Hollis, Felson, & Welsh, 2013). A more recent encapsulation of the theory, following the expansion of the guardian concept, is that crime is much more likely when an offender and target are present in the same place at the same time and there is no guardian nearby to either protect the target, survey the location, or manage the offender (Eck J. , 2003). This adjusted version of the crime triangle accounted for the importance of place when it comes to criminal acts (Hollis-Peel, Reynald, van Bavel, Elffers, & Welsh, 2011).

The use of guardianship for cybercrimes can be much more complicated than physical crimes. Many studies and media sources emphasize the need for additional guardianship,

especially from nation-state sponsored attacks (Plachkinova & Vo, 2021). Guardianship in cyberspace can include a variety of technologies, and the varying implementation of such measures can make it easier to study than other measures of RAT in cybercrime (Leukfeldt & Yar, 2016). Some of these guardianship measures include anti-virus software, multi-factor authentication, and VPN usage (Plachkinova & Vo, 2021). Some cybercrime studies have gone in-depth and found varying support for guardianship in certain cybercrimes (Williams, 2016). However, as this study focuses on target suitability and perpetrator motivation, measures of guardianship are not included in the study. This would have also been a challenge due to the type of data used, as discussed further in *Methods*.

Previous studies have examined several applications of routine activity theory relevant to the present study. This includes analysis of the likely offender and guardianship in cyberattacks (Yar, 2005) (Holt, Turner, Freilich, & Chermak, 2022) (Plachkinova & Vo, 2021) (Williams, 2016) (Leukfeldt & Yar, 2016). Focusing on target characteristics, there have been previous studies on each. This includes value of targets to ideologically motivated perpetrators (Parkin & Freilich, 2015), inertia in cyberspace including, in one example, for ideologically motivated perpetrators (Yar, 2005) (Holt, Leukfeldt, & Weijer, 2020), visibility of online targets (Wilsem, 2013) (Leukfeldt & Yar, 2016) (Holt, Leukfeldt, & Weijer, 2020) and accessibility of online targets for certain cyberattack types (Holt, Leukfeldt, & Weijer, 2020).

This primary research question of this study asks whether perpetrator motivation for nation-state cyberattacks are different from perpetrator motivation for non-nation state cyberattacks, using routine activity theory (RAT) as a theoretical framework for the question. This contribution is unique because it will assess the differences in the two offender types based on target suitability factors derived from RAT.

HYPOTHESES AND SUPPORT

The three hypotheses of the study presented below were generated using the VIVA principle of routine activity theory reviewed with a focus on targets of cyberattacks.

H_1: Targets of nation-state sponsored cyberattacks are more likely than targets of non-nation-state sponsored cyberattacks to be a government or military target. These targets hold a higher symbolic value for nation-state perpetrators than non-nation state perpetrators as discussed above. Further, government and military targets may be the only ones that nation-state attackers are interested to attack. By contrast, non-nation-state sponsored attackers may have a variety of other valuable targets to consider. For instance, the far-left may attack a business that deals in animal slaughter, the far-right may attack a nonprofit that supports people of color, and a Jihadist may attack a target that is well known among the general public to instill fear and terror. Some of these differing motivations have been studied previously (Holt, Turner, Freilich, & Chermak, 2022) (Parkin & Freilich, 2015). However, this thesis will compare all nation-state sponsored attackers against all non-sponsored attackers.

$H_{2:}$ Targets that have a vulnerability, specifically a zero-day vulnerability, are more likely to be targets of nation-state sponsored cyberattacks. This represents the visibility and access to the target. This hypothesis is based on previous research on visibility and accessibility in cybercrime. Previous literature has found that visibility of targets varies based on what information is available about the target without extensive research by the offender (Wilsem, 2013). Additionally, cybercrime perpetrators of different motivations have been found to target webpages of various accessibilities previously (Holt, Leukfeldt, & Weijer, 2020). To meet their differing goals, nation-states will have motivation to attack lower visibility targets and remain in networks for a long period of time. This would be consistent with the APT framework of nation-

state cyberattacks (Plachkinova & Vo, 2021). Additionally, nation-state sponsored attackers have both the resources and the patience to seek and find vulnerabilities in potential target networks and build tools to exploit these vulnerabilities.

H_3: Targets of nation-state cyber attackers are more likely to be targeted within linked or chronic attacks. This represents the inertia related to the selected target. Previous literature has found that online targets with greater inertia are only attacked by certain perpetrators (Holt, Leukfeldt, & Weijer, 2020). In the case of a cyberattacks, those attackers which are sponsored by a nation-state is likely to have greater resources to continue an attack for a longer period or return to a target repeatedly (Plachkinova & Vo, 2021). In comparison, a non-sponsored attacker is more likely to reach their goal and move on to another target because they have less resources available to maintain a constant attack. Non-state sponsored attackers may also achieve their established goal in a single attack, while state-sponsored attackers will carry out more complex attacks as part of military operations or other government-defined strategies. These differences in inertia between state-sponsored APT attacks and non-state-sponsored traditional cyberattacks is documented and supported by cybersecurity researchers (Alshamrani, Myneni, Chowdhary, & Huang, 2019). Although some cybercrime research has excluded inertia, it is included here as a factor of target suitability since it has been supported in certain cases (Yar, 2005) (Leukfeldt & Yar, 2016).

METHODS

In this section I discuss the methodology for the study. First, I discuss open-source data generally and its reliability in previous criminological studies. Next, I describe the key attributes of the dataset including an overview of the cases included, inclusion criteria, and data collection methods. Then, I provide an overview of the variables to be used for analysis and then describe the analytical methods to be used in the study.

Use of Open-Source Data

Publicly available sources have been increasingly used to analyze extremist attacks. One notable source is the US Extremist Crime Database (ECDB) (Freilich, Chermak, Belli, Gruenewald, & Parkin, 2014). In this study, I will be using the Extremist Cybercrime Database (ECCD) (Holt T. J., Chermak, Freilich, Turner, & Greene-Colozzi, 2022). Both datasets have taken careful consideration in the data collection to ensure quality and consistency. A review of the ECDB found that any single source can have biases in inclusion and content. However, accumulation of multiple sources on the same incident resulted in the most accurate record (Chermak, Freilich, Parkin, & Lynch, 2012). The review also found that victim, suspect, and incident information was similar across all types of data sources. Although research is still limited, it seems that open-source data can be reliably used for research if precautions are taken, and consistency tested.

The data used is from the United States Extremist Cyber Crime Database (ECCD). The dataset was introduced by Holt, et al in 2022. The introductory study for the dataset contains full detail on the creation process and inclusion of cases, but the most relevant points are discussed here. The dataset has three inclusion criteria: The attacks occurred between January 1, 1998 and December 31, 2018; the attack targeted internet infrastructure or targets operating within the

United States; the attack must have been completed to support an ideological belief or agenda (Holt T. J., Chermak, Freilich, Turner, & Greene-Colozzi, 2022). Data was gathered from a range of open-source searches and ranked for credibility and reliability. Variables were coded and justified before verification by a project manager that quality was being maintained through the process (Holt T. J., Chermak, Freilich, Turner, & Greene-Colozzi, 2022). Codes were recorded for each scheme, suspect, and targets, with the latter two being related back to the scheme via identifying variables. These were utilized in the analysis to relate characteristics from each codebook to the respective targets for each scheme. A scheme was defined as, "any series of attacks motivated by the same ideological cause or purpose carried out by one or more perpetrators against a target, or a series of targets over a period of time." (Holt T.J., Chermak, Freilich, Turner, & Green-Colozzi, 2022). The variables used will be discussed further below.

The dataset includes 314 schemes perpetrated by 433 suspects against 588 targets. The unit of analysis for this study will be the targets and how attacks against them differ based on whether the attack was sponsored by a nation-state or not. This requires relating the targets back to the schemes and suspects for certain variables as discussed below, but the analysis focuses on the targets.

Hypotheses

When discussing target suitability, there are four components within RAT that are used to determine how suitable a target may be for a likely offender: value, inertia, visibility, and accessibility (VIVA). A government or military target has higher value to a nation-state attacker or group than to a cyber-extremist not associated with a nation-state. The inertia of a government or military target is more comparable to a nation-state attacker or group than a non-nation-state attacker, thus making the target more suitable. Of this group, the federal government would have

more value and inertia than a local or state government. These differences are categorized in Target Type variable in the ECCD. A government or military target may be more visible to a nation-state attacker or group than to an attacker with no nation-state association. A government or military target may be more accessible to a nation-state attacker because of resources given to them by their sponsored country. Accessibility is partly measured in the ECCD by vulnerabilities used for the attack. This concept, also discussed in the "suitable target" portion of the theory section was used to produce the hypotheses discussed below.

H_1 is tested using the variable Target Type. This variable records the type of entity represented by the target using 10 categories. Federal, state, and local governments are each recorded separately, along with individual, business, military, transportation, educational institution, healthcare, and other. Each category was assigned a number 1-10 in the original dataset and is based on information available from searching the cases as described previously. I predict that government and military organizations are more likely to be targeted by nation-state actors compared to the other target types.

H_2 is tested through the Target Vulnerability and Target Zero-Day Vulnerability variables. These variables record if a vulnerability was used and if the vulnerability was zero-day, respectively. Both are recorded as yes, no, or missing. Each is therefore measured as a dichotomous variable for use in the analysis. For the ECCD, a vulnerability was defined as: "A *vulnerability* is flaws or errors in computer software or hardware, or people (in the case of social engineering) that can be compromised to gain access to computer systems and networks" (Holt T. J., Chermak, Freilich, Turner, & Greene-Colozzi, 2022). A zero-day vulnerability is a vulnerability that was unknown to the parties responsible for the target's security prior to the attack.

H_3 is tested using the Isolated Attack variable. This records if an attack was isolated, linked, or chronic relative to other attacks. This was originally recorded numerically using the following definitions. "*Isolated* refers to one single attack. *Linked* refers to a series of attacks all associated with the same banner or incident. *Chronic* refers to multiple attacks perpetrated by the same person over a period of time without any clear linkages between targets." The three categories will be considered separately because the number of linked or chronic attacks was not recorded. Therefore, these categories are independent of each other.

ANALYSIS

In this section, I further discuss the data and analysis. First, I present the frequencies and descriptives for each variable. I discuss how the variables were coded and provide percentages and means for each variable. Second, I discuss the results from the bivariate and multivariate statistical analyses.

Findings

Table 1. Variables

Variable	Coding Definition	Percentage of Valid Cases	N
Dependent Variable			
State-sponsorship Was the attack believed or proven to be state-sponsored?	0 = Not state-sponsored 1 = State-sponsored Missing	47.1% 52.9%	188 211 189
Independent Variables			
Target Type	1 = Government 2 = Individual 3 = Business 4 = Other Missing	27.2% 14.9% 35.7% 22.2%	157 86 206 128 11
$\chi^2 = 11.679$, df = 3, Significance = 0.009			
Isolated Attack	1 = Isolated 2 = Linked 3 = Chronic Missing	28.6% 59.6% 11.8%	112 233 46 197
$\chi^2 = 17.059$, df = 2, Significance < 0.001			
Vulnerability Used	0 = No 1 = Yes	87.6% 12.4%	515 73
Table 1 (cont'd)			
$\chi^2 = 1.223$, df = 1, Significance = 0.269			
Zero-day Vulnerability Used	0 = No 1 = Yes	98.0% 2.0%	576 12
$\chi^2 = 0.209$, df = 1, Significance = 0.648			
Control Variables			
Perpetrator Military Involvement	0 = No 1 = Yes	99.1% 0.9%	583 5
$\chi^2 = 1.494$, df = 1, Significance = 0.222			

Table 1 (cont'd)

Technical Skills	0 = None/no evidence 1 = Some skills 2 = Moderate skills 3 = Highly skilled Missing	49.5% 30.2% 18.6% 1.7%	285 174 107 10 12
$\chi^2 = 23.285$, df = 3, Significance < 0.001			
Motivation	0 = Unclear/none 1 = Retaliation 2 = Entertainment 3 = Monetary 4 = Chaos/anger 5 = Ideological Missing	38.0% 27.1% 5.6% 5.4% 5.0% 18.9%	219 156 32 31 29 109 12
$\chi^2 = 130.221$, df = 5, Significance < 0.001			
Table 1 (cont'd)			
Attack Type	1 = DDoS 2 = Data Breach 3 = Web defacement 4 = Doxxing 5 = Other Missing	24.0% 37.8% 15.4% 16.2% 6.3%	139 219 89 95 37 9
$\chi^2 = 87.653$, df = 4, Significance < 0.001			
Group Affiliation	1 = Working Solo 2 = Working as formal group 3 = Working as informal group Missing	4.2% 59.0% 36.7%	14 196 122 256
$\chi^2 = 92.773$, df = 2, Significance < 0.001			

Note: χ^2 was calculated based on each variable's relationship to the dependent variable.

Variables

Dependent Variable

Frequencies for each variable are shown in Table 1. Categorical variables were recoded as dummy variables. Variables were cross-referenced to each other with manual coding changes made as appropriate by referencing the original case materials. Variables for use of a vulnerability and zero-day vulnerability had missing cases recoded to no because such it was expected that such vulnerabilities would have been reported in the sources used to study if

present. For some other variables, categories were combined where appropriate or included as "other" if too small to be effectively utilized in the analysis.

The dependent variable is State-Sponsored attack. It is a dichotomous variable coded as yes or no representing whether the target was victimized in a nation-state sponsored scheme or not. Due to the data collection methods and the nature of cyberattacks, "yes" cases include those which have definitive evidence of state sponsored victimization and those in which state sponsored victimization is suggested by the available evidence. "No" cases include those which lack any evidence or those in which there is evidence proving that a nation-state did not sponsor the attack. The dependent variable represents the affiliation of the perpetrator: 35.9% of targets were attacked by a state-sponsored perpetrator. 32.0% were attacked by a non-state perpetrator, with 32.1% of cases missing a determination. Given the nature of open-source data, some cases did not have enough information to decide in either direction.

Independent Variables

The independent variables to test the influence of the VIVA acronym are target type, attack isolation, and use of vulnerabilities. The ten target types from the dataset were condensed into four categories: government, individual, business, and other. The percentages of each are included in Table 1. 27.2% were government targets, 14.9% were individual targets, 35.7% were business targets, and 22.2% were other types of organizations. These variables were dummy coded, and for the purpose of testing the hypothesis, business target was used as the reference category.

Attack isolation was dummy coded into three categories: isolated, linked, and chronic. Isolated attacks made up 39.6% of the cases, linked targets made up 59.6% of the cases, and chronic attack made up the remaining 11.8%. The reference category for hypothesis testing was

isolated attacks, thus the impact of an attack being linked or chronic is compared to the isolated attacks.

Vulnerabilities is a challenging variable as it was reported in a very small number of cases, and zero-day vulnerabilities was provided in an even smaller number of cases. Just 12.4% of targets were attacked using a vulnerability, and 2.0% of targets were attacked using a zero-day vulnerability. These are both dichotomous variables.

Controls were included based on three factors: They were relevant to better understand cyber offending, they were highlighted as being potentially important in the existing literature on nation-state cyber attackers, and data about potential variables had to be captured using open sources. The database includes a large number of variables, but many have no or few affirmative characteristics. There are a few, however, that are included in this analysis.

First, two controls, technical skills and motive were given numerical values based on the string variables recorded in the original data. Technical skills were coded in 4 categories: no technical skills, some skills, moderate skills, and highly skilled. No skills was coded when no information was given or the attack was extremely basic (49.5%), some skills was coded for applying existing tools to commit an attack (30.2%), such as DDoS bots or previously created malware. Moderate skills was coded when a tool was modified or customized and applied to a new attack (18.6%). Highly skilled was used when a proprietary tool was created and used for the attack, or when the attack was on a highly secured target if no specific tools or methods were addressed in the collected data (1.7%). Some skills was used as the reference category in the analysis. Technical skills may vary between nation-state and non-nation state perpetrators on the whole. However, findings to this effect were not found in existing literature. Assessing the skills of the perpetrator may be difficult in other datasets, so this allows for another unique aspect of

this study. Another control was motivation. Categories for this included unclear/none (38.0%), retaliation (27.1%), entertainment (5.6%), monetary (5.4%), chaos/anger (5.0%), ideological (18.9%). The reference value for this variable was entertainment. While the motivations of sponsored and non-sponsored attackers have been proposed to be consistently different, because there is enough crossover among them and they do not involve target suitability, they are included here as controls.

The next control was attack type. The attack types in the dataset were DDoS (24.0%), data breach (37.8%), web defacement (15.4%), doxing (16.2%), and other (6.3%). The reference value was DDoS. All of these attack types have been used variably by both sponsored and non-sponsored cyber attackers. Although some of the attack types may be more in line with the typical activities of one perpetrator type, none are exclusive and they are therefore included as controls for this study. Another control was perpetrator military involvement. This was recoded as a simple yes (0.9%) or no (99.1%).This variable was not used for the multivariate analysis because of the small number of cases that were affirmative, and it was not significant in the bivariate analysis. The final control is group affiliation. This includes three categories of working solo (4.2%), working with a formal group (59.0%), and working with an informal group (36.7%). Working solo was the reference category. Again, there have been some proposed differences in group involvement among state-sponsored and non-state-sponsored perpetrators, but it is included as a control here because it is not target-related and is therefore more appropriate as a control.

Chi-Square analysis of each variable is also presented in Table 1 to determine whether there is a significant bivariate relationship between them. Two of the independent predictors were significant. The target type and isolated attack variables were each found to be significant,

while the vulnerability and zero-day vulnerability variables were not significant. Of the control variables, military affiliation was found not significant while technological skills, attack type, group affiliation, and motivation were all significant.

MULTIVARIATE ANALYSIS

I conducted multiple multivariate analyses using IBM SPSS. Multivariate analysis was done using binomial logistic regression because the dependent variable is dichotomous. First, a logistic regression equation using only the independent variables on the dependent variable were run. Next, the second analysis including only the control variables. **Afterwards, the third analysis measured the separate effects of each control variable on the model.** Finally, the fourth and final model includes only the significant control variables.

The logistic regression results for only the independent variables are presented in Table 2. The logistic coefficient, standard error, odds ratio and significance for target type, attack type, and vulnerability is presented. The chi-square statistic is significant, and the pseudo-R2 is low at .09.

The results, in general, do not support the VIVA model. For example, the government target variable was not significant. That is, government targets were not statistically more likely to be nation state attacks when compared to business targeted attacks. Individual and other targets, however, were significantly more likely to be nation-state sponsored attacks. The vulnerability variable was not significant, but chronic attacks were significantly more likely to be nation state sponsored compared to isolated attacks which supports hypothesis 3.

The logistic regression results for the control variables are shown in Table 3 below. The logistic coefficient, standard error, odds ratio, and significance for each is again presented. The pseudo-R2 is much higher for this model at 0.607. This suggests that the control variables were much more effective at predicting state sponsorship.

Table 2. The Effects of Independent Variables on State Sponsorship

State-sponsored (Ref=No)		B	Std. Error	aOR	N
Yes	Target Type (Ref=Business)				
	Government Target	.291	.293	1.338	80
	Individual Target*	1.224	.386	3.401	58
	Other Target*	.910	.298	2.485	97
	Attack Isolation (Ref=Isolated)				
	Linked	-.205	.259	.815	204
	Chronic***	-1.833	.440	.160	41
	Vulnerability (Ref=Yes)				
	Vulnerability	-.337	.311	.714	40
	Intercept	-.066	.768		

Note: *p<0.05, **p<0.01, ***p<0.001, -2LL = 118.052, χ^2 = 33.991, df = 6, Pseudo R^2 = 0.094

Several control variables were significant. Web defacement and doxxing attack types were significantly less likely to be state sponsored compared to DDoS attacks. The only motive variables that were significant were ideological motivation and no motive. Specifically, ideologically motivated attacks and when no motive was identified were significantly more likely to be state sponsored compared to those that are motivated of entertainment purposes. Formal groups were significantly more likely to do a state sponsored attack compared to those perpetrators who offended solo. Finally, no skills were significantly less likely to do a state sponsored attack compared to some with some skills.

Table 3. The Effects of Possible Control Variables on State Sponsorship

State-sponsored (Ref=No)		B	Std. Error	aOR	N
Yes	Attack Type (Ref=DDoS)				
	Data Breach	1.773	.959	5.887	137
	Web Defacement*	-4.258	1.803	.014	60
	Doxxing*	-3.597	1.774	.027	79
	Other Type	.173	1.162	1.189	19
	Motivation (Ref=Entertainment)				
	No motive**	4.116	1.653	61.324	122
	Retaliation	3.101	2.099	22.223	71
	Monetary***	-14.899	.000	3.386E-7	8
	Chaos/anger	1.283	2.655	3.607	29
	Ideological*	4.069	1.682	58.522	89
	Group Affiliation (Ref=Solo)				
	Informal Group	-.977	.915	.376	113
	Formal Group*	3.767	1.443	43.254	57
	Technical Skills (Ref=Some)				
	No/unknown skill*	-1.327	.796	.265	145
	Moderate skills	.530	.939	1.698	84
	Highly skilled	.357	10.648	1.429	9
	Intercept	-4.602	2.070		

Note: *p<0.05, **p<0.01, ***p<0.001, -2LL= 50.287, χ^2= 170.863, df= 14, Pseudo R^2= 0.607

Next, I wanted to determine whether or not any of the independent variables remained significant when the control variables are also included in the model. The challenge with doing this was managing the small number of cases with variables that had somewhat large numbers of categories. To address this concern, I ran several models to explore whether any of the independent variables were significant. To do this, I ran the independent variables target type and isolation with each of the significant control variables separately. When putting any of the significant control variables in with the independent variables, the importance of those variables diminished as they were not significant. These results are shown in Table 4.

Table 4. The Effects of Each Control on the Final Model

State-sponsored (Ref=No)		B	Std. Error	aOR	N
Yes	Attack Type (Ref=DDoS)				
	Data Breach***	.606	.335	1.833	137
	Web Defacement	-.788	.487	.455	60
	Doxxing***	-2.622	.566	.073	79
	Other	-.538	.610	.584	19
	Target Type (Ref=Business)				
	Government Target	.246	.325	1.279	80
	Individual Target	-.215	.514	.806	58
	Other Target***	.792	.327	2.209	97
	Isolation (Ref=Isolated)				
	Linked	-.206	.298	.814	204
	Chronic***	-1.587	.536	.204	41
	Intercept	1.086	.890		
Note: * = Significant $\alpha<0.05$, -2LL = 163.864, $\chi^2 = 100.155$, df = 9, Pseudo $R^2 = 0.253$					
Yes	Group Affiliation (Ref=Solo)				
	Informal Group***	-4.008	1.000	.018	113
	Formal Group	.684	.868	1.981	57
	Target Type (Ref=Business)				
	Government Target	.411	.767	1.509	43
	Individual Target*	1.426	1.091	4.164	37
	Other Target	1.330	.729	3.781	61
	Isolation (Ref=Isolated)				
	Linked	-.995	.684	.370	204
	Chronic	-.052	.953	.949	41
	Intercept	-1.210	1.874		
Note: *p<0.05, **p<0.01, ***p<0.001, -2LL = 39.541, $\chi^2 = 87.379$, df = 7, Pseudo $R^2 = 0.423$					
Yes	Motivation (Ref=Entertainment)				
	No motive***	3.322	.790	27.721	122
	Retaliation	-.710	.966	.492	71
	Monetary	.752	.940	2.121	8
	Chaos/anger***	3.250	.892	25.797	29
	Ideological**	2.273	.788	9.711	89
	Target Type (Ref=Business)				
	Government Target	.534	.376	1.705	79
	Individual Target*	.832	.514	2.298	56
	Other Target**	.883	.382	2.417	97
	Isolation (Ref=Isolated)				
	Linked	-.567	.325	.567	204

Table 4 (cont'd)

	Chronic***	-.956	.478	.384	41
	Intercept	-2.987	1.137		
Note: *p<0.05, **p<0.01, ***p<0.001, -2LL = 112.714, χ^2 = 139.763, df = 10, Pseudo R^2 = 0.340					
Yes	Technical Skills (Ref=Some)				
	No/unknown skill***	-1.178	.308	.308	145
	Moderate skills	-.249	.315	.780	84
	Highly skilled	1.158	.840	3.184	9
	Target Type (Ref=Business)				
	Government Target	.075	.314	1.078	79
	Individual Target***	1.065	.411	2.902	56
	Other Target***	.908	.312	2.479	97
	Isolation (Ref=Isolated)				
	Linked	-.297	.283	.743	204
	Chronic***	-2.336	.480	.097	41
	Intercept	.894	.800		
Note: *p<0.05, **p<0.01, ***p<0.001, -2LL = 176.301, χ^2 = 55.450, df = 8, Pseudo R^2 = 0.152					

As shown in Table 4, there was considerable variation in each of the single control models. Model fit was greatest for the model controlled with group affiliation, followed by motivation, attack type, and technical skills (Pseudo R^2 = 0.423, 0.340, 0.253, 0.152 respectively). Each of these besides technical skills seems to have a greater fit than the initial model with only the independent variables.

The final model, table 5, displays the results of the model with all of the significant control variables combined into one model. This model had several significant variables and a better fit than any of the models in Table 4 with a pseudo R^2 of 0.607.

Table 5. Final Model with Only Significant Control Variables

State-sponsored (Ref=No)		B	Std. Error	aOR	N
Yes	Technical Skills (Ref=Some)				
	No/unknown skill	-1.326	.793	.266	145
	Moderate skills	.535	.942	1.708	84
	Highly skilled	.361	10.745	1.434	9
	Group Affiliation (Ref=Solo)				
	Informal Group	-1.010	.917	.364	113
	Formal Group*	3.764	1.447	43.128	57
	Attack Type (Ref=DDoS)				
	Data Breach	1.666	.977	5.290	137
	Web Defacement	-4.388	1.831	.012	60
	Doxxing*	-3.729	1.800	.024	79
	Other	-.059	1.160	.942	19
	Motivation (Ref=Entertainment)				
	No motive**	4.123	1.655	61.722	122
	Retaliation	3.130	2.098	22.874	71
	Monetary***	-14.899	.000	3.382E-7	8
	Chaos/anger	1.284	2.670	3.610	29
	Ideological*	4.093	1.690	59.895	89
	Intercept	-4.484	2.083		

Note: *p<0.05, **p<0.01, ***p<0.001, -2LL = 49.496, χ^2 = 170.844, df = 14, Pseudo R^2 = 0.607

DISCUSSION

Three hypotheses were tested in this study. First, I predicted that government and military organizations would be more likely targeted by nation-state sponsored actors. This hypothesis did not turn out to be true. Government target was an insignificant factor in the initial and controlled regressions. Second, I predicted that nation-state actors would be more likely to use vulnerabilities. This hypothesis was also not significant when tested. Finally, I predicted that nation-state attacks would more likely be linked or chronic than isolated. Chronic attacks were significant in the initial model but not significant when certain controls were included in the regression.

Adding the significant controls improved the model fit greatly, suggesting that the independent variables were not the best explanation of variation in the state-sponsorship. This aligns with the lack of or lesser significance of the independent variables when studied alone.

The main inquiry of this thesis is whether or not RAT, specifically VIVA, can be used as an analytical framework to differentiate between cyber offenses which are perpetrated by nation-state sponsored and non-nation-state sponsored attackers. This thesis builds on preexisting studies that question whether RAT can be used to effectively study cybercrime, though like many other studies in the field of cybercrime, it does have numerous limitations. Despite these limitations, however, the analyses brought forth in this thesis allow for a better understanding of the applicability of RAT and VIVA as a way to understand and study cybercrime.

In this study, VIVA as a theoretical framework does not seem to impact whether the motive in the types of cyber offenses is different between nation-state and non-nation state attacks. The individual target type, other target type, and chronic attack variables all had a significant effect with nation-state sponsorship (Table 2).

Significant controls included group affiliation, attack type, motivation, and technical skills (see Table 3). It was interesting the extent to which the control variables improved the fit of the model, and certain controls diminished the significance of the independent variables (see Table 4). Value was measured using the target type, with a hypothesis that government targets would be more likely to be targeted by nation-state sponsored perpetrators. This did not turn out to be significant (see Table 2). This is in line with previous research that shows mixed support for value in target selection for extremists and unclear target value estimations for APT perpetrators (Parkin & Freilich, 2015) (Plachkinova & Vo, 2021). Given the many factors that impact target value for a given perpetrator, it is possible that the non-nation state perpetrators in this data, given that they were most or all extremists, still found similar value in government and military targets even when they were not attacking on behalf of another nation-state. Inertia saw some significance in this study, but not in the way expected with chronic attacks having a significant negative association with state-sponsorship, even with several different controls. This adds to previous research on inertia for cybercrimes, which has held mixed support in the past (Holt, Leukfeldt, & Weijer, 2020) (Leukfeldt & Yar, 2016). The overall applicability of inertia for cybercrimes has long been questioned, with some research questioning whether it applies at all in cybercrimes (Yar, 2005). With the various attack methods represented in this dataset, it is possible that non-sponsored attackers were able to acquire the tools necessary to carry out a chronic attack. Also, several non-nation-state sponsored groups exist in the dataset which could "hand off" attacks from one person to the next. Visibility and accessibility, measured in this study by vulnerability usage, were not significant in this data (see Table 2). However, these factors' importance in cybercrime has gained support in some studies (Leukfeldt & Yar, 2016) (Holt, Leukfeldt, & Weijer, 2020) (Wilsem, 2013). It is likely that with the variety of different

cybercrimes included in this dataset and the proportion that used a vulnerability being rather small (12.4%, see Table 1), these components of target selection may apply in certain cases of cybercrime. This measure was also not the strongest being that the data was collected largely from publicly available media and news articles. Vulnerabilities may have been used, but if there was no specific mention made in the available materials, these cases would have been recorded as having no vulnerability. Overall, the factors of target selection in routine activity theory were not clear predictors of perpetrator nation-state sponsorship in this study.

Limitations and Future Research

As previously mentioned, this study is not short of limitations. One limitation of the study is the quantity and quality of data available. The ECCD utilized open-source data, which comes with the issue of missing data and thus a reduction in the quality of available data. Many potential variables that could have been used in the study had to be eliminated because of the number of missing codes. The inclusion criteria for the dataset were another limitation; for instance, certain attack types that have had RAT applied in the past may not have been included in this dataset. Additionally, the data used comes from what the individuals searching and coding on the project could locate from open-sources such as news articles and public databases, thus, the data used in the study may not be a full or accurate representation of cyber offenses by nation-state and non-nation-state perpetrators. Further, this could have led to the variables not being able to be measured in a way that can fully capture their significant. Because of this, further research is necessary.

Future research could focus on a smaller portion of the data, perhaps attempting to achieve high accuracy data on a smaller number of cybercrimes that could help determine possible relationships between target selection and state-sponsorship. Additionally, the same data

could be used with another criminological theory and perhaps greater support would exist through a different framework. Finally, additional variables might be added to more closely study each value, inertia, visibility, and accessibility and how it influenced the identified cases in the ECCD. Each of these would be valuable contributions to further expand our knowledge of cybercrime perpetrator characteristics.

The findings of this study will contribute to the study of routine activities theory as it does (or does not) apply to cybercrime. Additional inclusion criteria could also help determine the appropriate situations to utilize RAT for cybercrime. Nevertheless, this study is an important contribution to RAT research and cybercrime research.

REFERENCES

Ackerman, G. A., & Burnham, M. (2019). Towards a definition of terrorist ideology. *Terrorism and Political Violence*, 1160-1190.

Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security*, 402-418.

Ahmad, R., & Yunos, Z. (2012). The Application of Mixed Method in Developing a Cyber Terrorism Framework. *Journal of Information Security*, 209-214.

Ahmad, R., Yunos, Z., Sahib, S., & Yusoff, M. (2012). Perception on Cyber Terrorism: A Focus Group Discussion Approach. *Journal of Information Security*, 231-237.

Ahmadu, A. (2018). The Roles of Routine Activity Theory on Crime Prevention in the Era of Terrorism in Nigeria. *Fulafia Journal of Social Sciences*.

Akdemir, N., Sungur, B., & Basaranel, B. (2020). Examining The Challenges of Policing Economic Cybercrime in The UK. *The Journal of Security Sciences*, 113-134.

Al Mazari, A., Anjariny, A., Habib, S., & Nyakwende, E. (2018). Cyber Terrorism Taxonomies: Definition, Targets, Patterns, Risk Factors, and Mitigation Strategies. In I. R. Association, *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications* (pp. 608-621). Information Science Reference.

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials* (pp. 1851-1877). New York: Institute of Electrical and Electronics Engineers.

Arcuri, M. C., Gai, L., Ielasi, F., & Ventisette, E. (2020). Cyber attacks on hospitality sector: Stock market reaction. *Journal of Hospitality and Tourism Technology*, 277-290.

Bigot, C. L. (2017). Guardians and Targets: A Routine Activity Approach to Terrorism in Southeast Asia. *Open Journal of Social Sciences*.

Bossler, A. M., & Holt, T. J. (2009). On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology*, 400-420.

Bostdorff, D. M. (2004). The internet rhetoric of the Ku Klux Klan: A case study in web site community building run amok. *Communication Studies*, 340-361.

Bowman-Grieve, L. (2009). Exploring "Stormfront": A virtual community of the radical right. *Studies in Conflict & Terrorism*, 989-1007.

Brickey, J. (2012). Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace. *Combating Terrorism Center at West Point* , 4-6.

Bryan, D., Kelly, L., & Templer, S. (2011). The failed paradigm of "Terrorism". *Behavioral Sciences of Terrorism and Political Aggression*, 80-96.

Canetti-Nisim, D., Mesch, G., & Pedahzur, A. (2006). Victimization from Terrorist Attacks: Randomness or Routine Activities? *Terrorism and Political Violence*, 485-501.

Carter, J. A., Maher, S., & Neumann, P. R. (2014). *#Greenbirds: Measuring importance and influence in Syrian foreign fighter networks.* London: The International Centre for the Study of Radicalisation and Political Violence.

Cartwright, A., & Cartwright, E. (2019). Ransomware and reputation. *Games*.

Cavelty, M. D., & Egloff, F. J. (2019). The politics of cybersecurity: Balancing different roles of the state. *St Antony's International Review*, 37-57.

Chermak, S. M., Freilich, J. D., Parkin, W. S., & Lynch, J. P. (2012). American terrorism and extremist crime data sources and selectivity bias: An investigation focusing on homicide events committed by far-right extremists. *Journal of Quanitative Criminology*, 191-218.

Chhabra, S. S. (2010). Adapt-Qaeda: Analyzing the relationship between organizational transformation and the exploitation of information technology. *Critique: A worldwide journal of politics*.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 588-608.

Conway, M. (2006). Terrorism and the internet: New media - New threat? *Parliamentary Affairs*, 283-298.

Correia, V. J. (2022). An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom. *SN Computer Science*.

Denning, D. (2000, May 23). Cyberterrorism. *Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*.

Eck, J. (2003). Police Problems: The Complexity of Problem Theory, Research and Evaluation. *Crime Prevention Studies*, 79-113.

Eck, J. E. (2010). Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure. *Security Journal*, 37-51.

Egloff, F. J. (2020). Public attribution of cyber intrusions. *Journal of Cybersecurity*.

Egloff, F. J. (2022). Intentions and Cyberterrorism. In P. Cornish, *The Oxford Handbook of Cyber Security.* Oxford University Press.

Felson, M. (2017). Linking Criminal Choices, Routine Activities, Informal Control, and Criminal Outcomes. In D. B. Cornish, & C. V. Ronald, *The Reasoning Criminal* (pp. 119-128). Routledge.

Felson, M., & Cohen, L. E. (1980). Human Ecology and Crime: A Routine Activity Approach. *Human Ecology*, 389-406.

FireEyre iSight Intelligence. (2017). *APT28: At the center of the storm.* FireEye.

Fox, G. (2019, October 27). *ISIS Caliphate defeated: A timeline of the terror group's brutal project.* Retrieved from Independent: https://www.independent.co.uk/news/world/middle-east/isis-timeline-caliphate-iraq-syria-territory-defeated-a8782351.html

Freilich, J. D., Chermak, S. M., Belli, R., Gruenewald, J., & Parkin, W. S. (2014). Introducing the United States extremist crime database (ECDB). *Terrorism and Political Violence*, 372-384.

Gartenstein-Ross, D., Shear, M., & Jones, D. (2019). *Virtual plotters. Drones. Weaponized AI?: Violent non-state actors as deadly early adopters.* Valens Global.

Gascon, J. A. (2023). The inferential meaning of controversial terms: The case of "Terrorism". *Topoi: An International Review of Philosophy*, 1-13.

Gates, S., & Podder, S. (2015). Social media, recruitment, allegiance and the Islamic State. *Perspectives on Terrorism*, 107-116.

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., & Horgan, J. (2017). Terrorist use of the internet by the numbers. *Criminology & Public Policy*, 99-117.

Gottfredson, M. R., & Hirschi, T. (1990). *A General Theory of Crime.* Stanford University Press.

Harel, T. L. (2022). Archives in the making: Documenting the January 6 capitol riot on Reddit. *Internet Histories*, 391-411.

Hassan, H., Farine, L., Kinnish, N., Mejia, D., & Tindale, C. (2023). What is Extremism? Advancing Definition in Political Argumentation. *Topoi: An International Review of Philosophy*, 573-581.

Hodgson, J. S., & Tadros, V. (2013). The Impossibility of Defining Terrorism. *New Criminal Law Review*, 494-526.

Hollis, M. E., Felson, M., & Welsh, B. C. (2013). The capable guardian in routine activities theory: A theoretical and conceptual reappraisal. *Crime Prevention and Community Safety*, 65-79.

Hollis-Peel, M. E., Reynald, D. M., van Bavel, M., Elffers, H., & Welsh, B. C. (2011). Guardianship for crime prevention: a critical review of the literature. *Crime Law Soc Change*, 53-70.

Holt, T. J. (2023). Understanding the state of criminological scholarship on cybercrimes. *Computers in Human Behavior*.

Holt, T. J., & Bossler, A. M. (2009). Examining The Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior*, 1-25.

Holt, T. J., Chermak, S. M., Freilich, J. D., Turner, N., & Greene-Colozzi, E. (2022). Introducin and Exploring the Extremist Cybercrime Database (ECCD). *Crime & Delinquency*, 1-26.

Holt, T. J., Chermak, S. M., Freilich, J. D., Turner, N., & Greene-Colozzi, E. (2022). Introducing and exploring the extremist cybercrime database (ECCD). *Crime & Delinquency*.

Holt, T. J., Freilich, J. D., Chermak, S., & McCauley, C. (2015). Political radicalization on the Internet: Extremist content, government control, and the power of victim and jihad videos. *Dynamics of Asymmetric Conflict*, 107-120.

Holt, T. J., Lee, J. R., Freilich, J. D., Chermak, S. M., Bauer, J. M., Shillair, R., & Ross, A. (2022). An Exploratory Analysis of the Characteristics of Ideologically Motivated Cyberattacks. *Terrorism and Political Violence*, 1305-1320.

Holt, T. J., Leukfeldt, R., & Weijer, S. v. (2020). An Examination of Motivation and Routine Activity Theory to Account for Cyberattacks Against Dutch Web Sites. *Criminal Justice and Behavior*, 487-505.

Holt, T. J., Stonhouse, M., Freilich, J., & Chermak, S. M. (2021). Examine ideologically motivated cyberattacks performed by far-left groups. *Terrorism and Political Violence*, 527-548.

Holt, T. J., Turner, N. D., Freilich, J. D., & Chermak, S. M. (2022). Examining the Characteristics That Differentiate Jihadi-Associated Cyberattacks Using Routine Activities Theory. *Social Science Computer Review*, 1614-1630.

Hunter, L. Y., Albert, C. D., & Garrett, E. (2021). Factors that motivate state-sponsored cyberattacks. *The Cyber Defense Review*, 111-128.

Hutchings, A., & Hayes, H. (2009). Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the 'Net'? *Current Issues in Criminal Justice*, 433-452.

Iqbal, M. (2004). Defining Cyberterrorism. *UIC John Marshall Journal of Information Technology & Privacy Law*, 397-408.

Jackson, R. (2010). In defence of "Terrorism": Finding a way through a forest of misconceptions. *Behavioral Sciences of Terrorism and Political Aggression*, 116-130.

Jurich, J., & Kayaalp, E. (2017). Reconceptualizing Propaganda in the internet age: An examination of terrorist online propaganda. *Culture & Communication*, 93-108.

Kaczkowski, W., Winkler, C., Damanhoury, K. E., & Luu, Y. (2021). Intersections of the real and the virtual caliphates: The Islamic State's territory and media campaign. *Journal of Global Security Studies*.

Kao, D.-Y., & Kluaypa, B. (n.d.). Victimization of Cyberbullying Target: VIVA Observation from Lifestyle Exposure. *Journal of Information, Technology, and Society*, 69-80.

Kaplan, A., & Weimann, G. (2011). *Freedom and terror: Reason and unreason in politics.* New York: Routledge.

Kechichian, J. A. (2006). Terror on the internet: The new arena, the new challenges. *Perspectives on Political Science*, 233.

Kello, L. (2021). Cyber legalism: Why it fails and what to do about it. *Journal of Cybersecurity*, 1-15.

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review*, 470-486.

Lennings, C. J., Amon, K., Brummert, & Lennings, N. J. (2010). Grooming for Terror: The internet and young people. *Psychiatry, Psychology and Law*, 424-437.

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, 263-280.

Liang, C. S. (2017). Unveiling the "United Cyber Caliphate"" and the birth of the e-terrorist. *Georgetown Journal of International Affairs*, 11-20.

Luiijf, E. (2014). Definitons of Cyber Terrorism. In B. Akhgar, A. Staniforth, & F. Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 11-17). Syngress.

Mandiant. (2022). *M-Trends 2022.* Mandiant.

Mandiant. (2022, February). *Multifaceted extortion: The evolution of ransomware*. Retrieved from Mandiant: https://www.mandiant.com/sites/default/files/2022-02/MFE-Infographic.pdf

Mandiant. (2023). *Advanced Persistent Threats (APTs).* Reston: Mandiant.

Mansfield-Devine, S. (2020, December). Nation-state attacks: the escalating menace. *Network Security*, pp. 12-17.

Martin, G. (2014). Types of Terrorism. In G. Martin, *Exchanging Terrorism Oxygen for Media Airwaves: The Age of Terroredia* (pp. 81-82). IGI Global.

Miró, F. (2014). Routine Activity Theory. *The Encyclopedia of Theoretical Criminology*.

Mitre. (2022, August 23). *Lazarus Group*. Retrieved from MITRE ATT&CK: https://attack.mitre.org/groups/G0032/

Mitre. (2022, October 20). *Stuxnet*. Retrieved from MITRE ATT&CK: https://attack.mitre.org/software/S0603/

Mozes, T., & Weimann, G. (2010). The E-Marketing Strategy of Hamas. *Studies in Conflict & Terrorism*, 211-225.

Parkin, W. S., & Freilich, D. J. (2015). Routine Activities and Right-Wing Extremists: An Empirical Comparison of the Victims of Ideologically- and Non-Ideologically-Motivated Homicides Committed by American Far Rightists. *Terrorism and Political Violence*, 182-203.

Paul, K. A. (2018). Ancient artifacts vs. Digital artifacts: New tools for unmasking the sale of illicit antiquities on the dark web. *Arts*.

Payne, B. K. (2020). Defining Cybercrime. In T. J. Holt, & A. M. Bossler, *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 3-25). Palgrave Macmillan.

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies, and Taxonomies. *Forensic Sciences*, 379-398.

Piazza, J. A., & Guler, A. (2019). The online caliphate: Internet usage and ISIS support in the Arab world. *Terrorism and Political Violence*, 1256-1275.

Plachkinova, M., & Vo, A. (2021). A taxonomy of cyberattacks against critical infrastructure. *Journal of Cybersecurity Education, Research and Practice*.

Plotnek, J., & Slay, J. (2020). Cyber Terrorism: A Homogenized Taxonomy and Definition. *Computers & Security*.

Pollitt, M. M. (1998). Cyberterrorism - fact or fancy? *Computer Fraud & Security*, 8-10.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, 267-296.

Puttonen, R., & Romiti, F. (2022). The linkages between organized crime and terrorism. *Studies in Conflict & Terrorism*, 331-334.

Qin, J., Zhou, Y., Reid, E., Lai, G., & Chen, H. (2007). Analyzing terror campaigns on the internet: Technical sophistication, content richness, and web interactivity. *International Journal of Human-Computer Studies*, 71-84.

Ramsay, G. (2014). Why terrorism can, but should not be defined. *Critical Studies on Terrorism*, 211-228.

Redmond, S., Jones, N., Holman, E., & Silver, R. C. (2019). Who watches an ISIS beheading - And why. *American Psychologist*.

Rudner, M. (2016). "Electronic Jihad": The internet as Al Qaeda's catalyst for global terror. *Studies in Conflict & Terrorism*, 10-23.

Saul, B. (2015, September). Defining Terrorism: A Conceptual Minefield. Sydney, New South Wales, Australia: The University of Sydney Law School.

Saul, B. (2019). Defining Terrorism: A Conceptual Minefield. In E. Chenoweth, R. English, A. Gofas, & S. Kalyvas, *The Oxford Handbook of Terrorism* (pp. 34-49). Oxford University Press.

Scrivens, R., & Gaudette, T. (2021). Terrorists' and Violent Extremists' Use of The Internet and Cyberterrorism. In T. J. Holt, *Crime Online: Causes, Correlates and Context* (pp. 231-262). Carolina Academic Press.

Shandler, R., & Gomez, M. A. (2022). The hidden threat of cyber-attacks - undermining public confidence in government. *Journal of Information Technology & Politics*.

Shead, S. (2022, March 8). Google to acquire cybersecurity firm Mandiant for $5.4 billion.

Shehabat, A., & Mitew, T. (2018). Black-boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics. *Perspectives on Terrorism*, 81-99.

Shostak, A. (2017). Striking at their core - De-funding the Islamic State of Iraq and Syria. *Journal of Terrorism Research*, 43-52.

Talihärm, A. (2010). Cyber Terrorism: in Theory or in Practice? *Defence Against Terrorism Review*, 59-74.

Terzi, M. (2019). E-Government and Cyber Terrorism: Conceptual Framework, Theoretical Discussions and Possible Solutions. *Turkish Journal of TESAM Academy*, 213-247.

Unlu, A., & Yilmaz, K. (2022). Online terrorism studies: analysis of the literature. *Studies in Conflict and Terrorism*.

Weimann, G. (2006). *Terror on the internet: The new arena, the new challenges.* Washington, DC: The United States Institute of Peace Press.

Williams, M. L. (2016). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at The Country and Individual Level. *The British Journal of Criminology*, 21-48.

Wilsem, J. v. (2013). 'Bought it, but Never Got it' Assessing Risk Factors for Online Consumer Fraud Victimization. *European Sociological Review*, 168-178.

Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 407-427.