Spring 4-21-2024

# An Evidence-Based Investigation on The Offending Behaviors of Website Defacers

Cameron J. Hoffman



Recommended Citation

Hoffman, Cameron J., "An Evidence-Based Investigation on The Offending Behaviors of Website Defacers." Dissertation, Georgia State University, 2024.
doi: https://doi.org/10.57709/36973842

ABSTRACT

An Evidence-Based Investigation on The Offending Behaviors of Website Defacers

By

Cameron John Hoffman

May 2024

Committee Chair: Dr. David Maimon

Major Department: Criminal Justice and Criminology

The rapid development of the internet has far outpaced our ability to protect the internet. As new technologies have developed, so have new ways to exploit these technologies to use them for criminal purposes. This is extremely true of the core of the internet, websites. While the number of websites both personal and business focused have skyrocketed, so too have the number of cyber-attacks against these sites. These cyber-attacks are known as website defacements and can cause costly losses and damage the reputation of their internet victims. In such an attack the website defacer gains unauthorized access to the website and changes the appearance of the website, rendering it inoperable for extended periods of time.

Prior research on website defacers has provided a preliminary understanding of the motivation and attack preferences of website defacers but given the relative newness of this line of research there are many avenues to deepen our understanding beyond description of these brazen cybercriminals. This dissertation addresses two such areas in need of further study by examining the criminal careers of website defacers and how they respond to potential changes in capable guardianship. As our review of the literature shows, over half of the studies in this literature utilize a data source that was shown to be faulty in measuring the motivational factors of website defacement. Thus, this dissertation used detailed data created by tracking the

individual offending patterns of website defacers and utilizing open-source intelligence methods to gather information about each defacer's characteristics in the sample, rather than the previously mentioned data source.

This three-paper dissertation contains a scoping review of the website defacement literature, the first of its kind, to reveal the existing scholarly gaps in this field of research. This dissertation's second paper uses my previously published paper using this data that revealed important findings on the criminal trajectories of website defacers. The dissertation closes with the first study to examine the effect of holidays on website defacement attack frequencies. These papers serve to outline the direction of future research, aid law enforcement agencies, and bolster our understanding of these cybercriminals' activities.

# AN EVIDENCE-BASED INVESTIGATION ON THE OFFENDING BEHAVIORS OF WEBSITE DEFACERS: A THREE PAPER DISSERTATION

BY

CAMERON JOHN HOFFMAN

A Dissertation Submitted in Partial Fulfillment
of the Requirements for the Degree
of
Doctor of Philosophy
in the
Andrew Young School of Policy Studies
of
Georgia State University

GEORGIA STATE UNIVERSITY
2024

ACCEPTANCE

This dissertation was prepared under the direction of the candidate's Dissertation Committee. It has been approved and accepted by all members of that committee, and it has been accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Criminal Justice and Criminology in the Andrew Young School of Policy Studies of Georgia State University.

Dissertation Chair: Dr. David Maimon

Committee: Dr. David Sabol
Dr. Mark Reed
Dr. C. Jordan Howell

Electronic Version Approved:

Thomas J. Vicino, Dean
Andrew Young School of Policy Studies
Georgia State University
May, 2024

## Table of Contents

**List of Tables…….ix**

**List of Figures……....xi**

**Chapter I: Introduction.....1**

**1.1. Abstract…….…...……1**

**1.2. Hackers and their Targets……..……..…….1**

**1.3.Victims……..…….2**

**1.4.Victim Features……..……..5**

**1.5.The Progression of the Hacking Event……...…….…….10**

**1.6. Hacker Profiles……..……..…….…….15**

**1.7. Website Defacement……...…….……..……18**

**1.8. The Proposed Research.....22**

**1.9. Theoretical Background.....23**

***1.9.1. Life Course Criminology*……..…….…….23**

***1.9.2. Routine Activities Theory*…….……..…...…….27**

***1.9.3. Routine Activities Theory in Cyberspace*…….…….28**

***1.9.4. Capable Guardianship in Cyberspace*……...…….29**

***1.9.5. Holidays and Traditional Criminology*……..……..……..32**

***1.9.6. Holidays and Hackers*……..……..……34**

**1.10. Research Hyptheses.....37**

**1.11. Methods……..…….…….……38**

***1.11.1. Data*…….…..……..38**

***1.11.2. Models*……...…….39**

**1.12. Outline of the Dissertation……..…….39**

**1.13. Summary…….……...……..40**

**Chapter II: Scoping Review of Website Defacement: The Problem, Practices, Policies, and Prevention……..……...……...…….41**

**2.1. Abstract……..…….…….…….41**

**2.2. Introduction …….……..…….……...……...……42**

**2.3. Methods ……..……..…..……44**

***2.3.1. Protocol and Registration……..…..……..…..……44***

***2.3.2. Eligibility Requirements…….……..…....……45***

***2.3.3. Information Sources……...……46***

***2.3.4. Search Strategy…….……..47***

***2.3.5. Selection of Sources of Evidence…….……...……48***

***2.3.6. Data Extraction and Coding…….……..49***

**2.4. Results……...……...……..……49**

***2.4.1. Study Screening and Selection……..…….……...……49***

***2.4.2. Selection of Sources of Evidence……50***

***2.4.3. Characteristics of Sources of Evidence…….…….……51***

**2.5. Results of Individual Sources of Evidence……..……52**

**2.6. Synthesis of Results…….……..……52**

***2.6.1. Routine Activities in Website Defacement…….…….……53***

***2.6.2. Life-Course Criminology……..……...…63***

***2.6.3. Social Learning Theory……...…..……65***

***2.6.4. Other…….……..……...…..67***

***2.6.5. Other Methodology*……..……...…69**

**2.7. Discussion……..…..…….…….72**

***2.7.1. Summary of Evidence and Conclusions*……..……...…72**

***2.7.2. Limitations*…….…..…….…..….76**

***2.7.3. Funding*……..…….……...…..……..….78**

**Chapter III: Predicting New Hackers' Criminal Careers: A Group-Based Trajectory Approach.....79**

**3.1. Abstract……...……...……..…….79**

**3.2. Introduction…….....……...……..…….79**

**3.3. Theoretical Framework…….…….……..……...…….81**

***3.3.1. Life-Course Criminology*……...……..……...….81**

***3.3.2. Life-Course Criminology and Malicious Hacking*……..…..……83**

**3.4. Literature review……..……..…….……..84**

***3.4.1. Hackers*……..……...……84**

***3.4.2. Website Defacement*…….……...……...……..87**

**3.5. Current Study…….……..……..……...……89**

**3.6. Methods……..……...……...…..91**

***3.6.1. Data*…….....…….……..……..91**

***3.6.2. Sample*……..…….……..91**

***3.6.3. Dependent Variables*…….……...…….…….93**

***3.6.4. Independent Variables*……..……...……94**

**3.7. Analytic Strategy……...…..…….……..97**

**3.8. Results……..……...……98**

***3.8.1. Descriptive Statistics*……...……98**

***3.8.2. Bivariate Analysis*……..……..99**

***3.8.3. Group-Based Trajectory Models*……..…….100**

**3.9. Conclusion…….……..104**

***3.9.1. Theoretical Implications*……..……..……...……106**

***3.9.2. Policy Implications*……..…….…...……..107**

***3.9.3. Limitations*……..…….……...…..……..109**

**Chapter IV: Holidays and Hacking: Analyzing Website Defacement Patterns Through Routine Activities Theory…….……..……..…….111**

**4.1. Abstract……..……...……...……111**

**4.2. Introduction…….…..……..…….……111**

**4.3. Literature Review……..……..……113**

***4.3.1. Routine Activities Theory in Brief*……..……..113**

***4.3.2. Routine Activities in Cyberspace*……..……..…….…….114**

***4.3.3. Website Defacement*……...……..……..…114**

***4.3.4. Routine Activities and Website Defacement*……..…….…..115**

***4.3.5. Holidays as a Measure of Capable Guardianship*……..……..…117**

**4.4. Current Study…….....……119**

**4.5. Methodology……...……..…..……..120**

***4.5.1. Data*…….……..……120**

***4.5.2. Sample*……...……..……...…….……..122**

***4.5.3. Dependent Variables*……...……..……...…..……124**

***4.5.4. Independent Variables*…….…….……..……..125**

**4.6. Analytic Strategy……..…….……..131**

***4.6.1. A Note on Model Building*……..……..136**

**4.7. Results……...……...…138**

***4.7.1. Descriptive Statistics*……..……..…..……138**

***4.7.2. Bivariate Correlation*…….……..…….140**

***4.7.3. Regression Analysis*……..……142**

**4.8. Discussion of Results…….……..……155**

***4.8.1. Conclusions and Implications for Theory and Policy*……..…...……159**

***4.8.2. Limitations*…….…….…….……160**

**Chapter V: Overall Conclusions……..…….……166**

**5.1. Abstract……...…….…….……...166**

**5.2. Discussion of Findings……..……..……..……..166**

**5.3. Policy Implications……..……....……173**

**5.4. Limitations…….....……..……174**

**5.5. Conclusion……..……..……..…….176**

**Appendix A. Complete Data Extractions .....…….……..……178**

**Appendix B. Full Multilevel Model Output.…….....……..…….....181**

**List of References……...…….…….……..199**

**Vita…….……....……...…….237**

## List of Tables

**Table 2.1. Search Results……..……..……..…….49**

**Table 2.2. General Characteristics of Included Studies……..…….…….……..….52**

**Table 2.3. Offenders, RAT Motivation……..……..…….…..56**

**Table 2.4. Offenders, RAT Suitable Targets…….…….……..…..…60**

**Table 2.5. Offenders, RAT Capable Guardian……..……..……..62**

**Table 2.6. Life Course Studies……..…….……..…..…….….65**

**Table 2.7. Social Learning Theory Studies……..…….……..……..….67**

**Table 2.8. Other Studies……..…….……..……....…….68**

**Table 2.9. Other Methodology……..…….……..……..…71**

**Table 3.1. Descriptive Statistics……..…….……..…….……...98**

**Table 3.2. Bivariate Correlations……..……..…..…….99**

**Table 3.3. Model Fit statistics……..…….……..……..100**

**Table 3.4. Group-Based Trajectories of Hackers……...…….....102**

**Table 3.5. Group-based Trajectories of Hackers with Interaction Term……...…...103**

**Table 4.1 Descriptive Statistics……..…….……..139**

**Table 4.2. Bivariate Correlation Table……..…….....….141**

**Table 4.3. Logistic, Overall Holiday Effect……..……...…….…144**

**Table 4.4. Logistic, Individual Holidays…….…….……..…145**

**Table 4.5. Negative Binomial, Overall Holiday Effect…….……...147**

**Table 4.6. Negative Binomial, Individual Holidays…….……..…...…...……149**

**Table 4.7. All Defacements, Sensitivity Analysis…….…….....…152**

**Table 4.8. Special Defacements, Sensitivity Analysis……..……154**

**Table A1. Summary of Included Studies for Scoping Review...……...……..……...178**

**Table B1. Aggregated Holiday Effect Logit Regression…….…...…..……181**

**Table B2. Individual Holiday Effects Logistic Regression…….……184**

**Table B3. Aggregated Holiday Effect Negative Binomial Regression……...…..……..187**

**Table B4. Individual Holiday Effects Negative Binomial Regression……...……190**

**Table B5. Sensitivity Analysis for All Defacements…….…….…….……..193**

**Table B6. Sensitivity Analysis for Special Defacements…….……196**

## List of Figures

**Figure 2.1. Query Terms……..…….……..…….48**

**Figure 2.2. Flow Chart…….…..…….…..……51**

**Figure 3.1. Defacer Trajectories…….…….……..….……..101**

**Figure 4.1. Career Defacements…….…….……..…...……...127**

**Figure 4.2. Defacer Careers....……..…….……..……..127**

# Chapter I: Introduction

## 1.1. Abstract

Website defacement is a relatively simplistic form of hacking, but it results in serious damages. In general, small seemingly insignificant code processes can be exploited to cause significant digital and even physical harm. To understand website defacers, it is first important to discuss the background of hacking research and the varied approaches taken to address this growing problem. Following this discussion, this section provides a brief overview of the main facets of the three papers and the structure of the dissertation.

## 1.2. Hackers and Their Targets

The explosive growth of the internet in recent years has opened up numerous opportunities for committing crimes (Bossler & Berenblum, 2019). The internet's global nature has removed geographical barriers, making potential victims more accessible to attackers compared to traditional crime (Furnell & Dowling, 2019). One of the most common computer-based crimes is hacking. Hacking is the unauthorized access of computer systems and internet technologies, often using this access for criminal purposes (Grabosky, 2016; Maimon & Louderback, 2017). Those who exploit weaknesses in computer tools to gain unauthorized access are commonly referred to as hackers (Grabosky, 2016; Schell & Dodge, 2002). These tech-savvy criminals can employ their access for various criminal activities, such as data leaks, carding, ransomware, website defacement, and Denial of Service attacks. While these hacks primarily target digital infrastructure like websites and databases, their consequences extend into the real world, resulting in issues like identity theft and financial losses.

The academic study of hacking can be divided into two distinct research streams. The first stream, predominantly from the fields of computer science and information security, aims to

better understand and secure the technical aspects of digital technologies. This research also delves into the functions of malicious software, known as malware (Bossler & Holt, 2009; Hughes & DeLeon, 2007). Cybercriminals use malware to compromise and alter the functions of computer systems as well as to eliminate evidence of their intrusion on infected systems (Furnell, 2002; Kapersky, 2023; Taylor et al., 2006). Given the potential for costly losses, a significant portion of this research focuses on developing intrusion detection systems and anti-virus software to detect and prevent malware installation (D'Arcy & Herath, 2011; Eivazi, 2011; Hsiao et al., 2014; Kaspersky, 2023; PandaLabs, 2022). However, despite their widespread adoption, the true effectiveness of these tools in preventing cyber-attacks is unknown, nor have these technologies eliminated the threat of new and evolving computer exploits (Ashibani & Mahmoud, 2017; Bossler & Holt, 2009; Choi, 2008; D'Arcy & Herath, 2011; Denning & Baugh, 1999; Maimon & Louderback, 2019; Ngo & Paternoster, 2011). Consequently, security breaches continue to make headlines as new vulnerabilities emerge alongside advancing technologies. This leads us to the second stream of hacking research, which concentrates on the human aspects of hacking incidents.

The second stream of research aims to provide a comprehensive view of cybersecurity by examining the individuals committing cybercrimes and those who become victims. In general, this stream of the hacking literature seeks to better understand the characteristics of those targeted by cybercrimes, the progression of hacking events, and the profiles of hackers.

### 1.3. Victims

In 1992 Flanagan & McMenamin claimed that future generations of hackers would cause damages to their victims ranging from 500 million to 5 billion dollars annually in the coming years. Despite the significant margin of error in their estimate, cybercriminals have consistently

exceeded these expectations, with victims experiencing over 5.5 billion dollars in damages each year over the past five years (FBI, 2023). Moreover, it appears that a newer generation of victimization has emerged, as losses have surged by a staggering 281% from 2018 to 2022, reaching a remarkable 10.3 billion dollars in that year (FBI, 2023). During this period, the FBI recorded over 3.26 million complaints of cybercrime victimization, averaging 2,175 complaints per day (FBI, 2023). While this daily figure is lower than the average rate of traditional burglary, US citizens express greater fear of falling victim to cybercrime than any other type of crime, perhaps in part because they are victimized more than citizens of other countries (FBI, 2019, 2023; Maimon & Louderback, 2019; Reinhart, 2017; Wall, 2012; Yu, 2014). Additionally, while the official numbers may show that rates of cybercrimes are lower than traditional crimes, it is important to note that data on cybercrimes suffers from extreme under-reporting compared to traditional crimes, preventing the true scope of cybercrime from being revealed (Decker, 2020, van de Weijer et al., 2018).

In fact, the FBI estimates that its reports likely account for only about 12% of cybercrimes (Decker, 2020). This is due in large part to individuals either not knowing they have been victimized or as many choose not to report their victimization to authorities (Button et al., 2009; Choi, 2008; Reyns et al., 2018; Rostami et al., 2022; Standler, 2002). Furthermore, the poor reporting of cybercrimes is not just from individuals, but businesses also tend to underreport their cyber victimization, with estimates ranging from 15% to as low as 6% of potential cybercrimes being reported (Caneppele & Aebi, 2017; Kemp et al., 2021; Rantala, 2008; Sukhai, 2004). Among businesses, administrative and financial services companies are particularly reluctant to report malicious cyber incidents (Kemp et al., 2021). Despite the lack of official reporting, the results of victimization surveys show that cybercrimes likely account for

one-third to one-half of the total crimes in any given country (Caneppele & Aebi, 2017). Even with potentially more accurate results from victimization surveys, it remains impossible to create detailed data on the financial impact and the total number of victims until reporting improves. This raises the question of why there is such a lack of reporting for these crimes.

While there is no conclusive evidence, the literature suggests that companies often fail to report cybercrimes against them to avoid negative publicity. Public knowledge of a business falling victim can harm its reputation, public image, and consumer trust (Kemp et al., 2022; Lagazio et al., 2014; Sukhai, 2004), resulting in costly financial consequences (Kemp et al., 2022; Lagazio et al., 2014).

Individuals, however, fail to report for very different reasons. Aside from not realizing they were victimized, many individuals feel ashamed to admit that they were victimized (Abdulai, 2020; Sikra et al, 2023; Standler, 2002). Research also found that victims were less likely to report instances of hacking than they were of other cybercrimes like online fraud (van de Weijer et al., 2018) In a similar vein, people are less likely to report victimization unless it constituted a serious cybercrime (van de Weijer et al., 2020). There is also a gap between the intention to report and actually reporting a cyber-offense (van de Weijer et al., 2020). In fact, it appears that victims either do not know who to report their victimization to, given the variety of public and private agencies they could report the crime to, or are discouraged from reporting when they do not receive assistance from the ill-equipped government organization they reach out to for help (Bossler et al., 2019; Button et al., 2012; Cross et al., 2016). Perhaps this is why victims are less likely to report their victimization to the police in favor of other institutions, like their banks, who themselves do not disclose the victimization (van der Weijer et al., 2018). However, this lack of reporting does more than just underestimate the scale of cybercrime's

impact, without knowing exactly who is being victimized and what their characteristics are, it is difficult to determine what factors of a victim enable or encourage cyber criminals. However, despite the lack of a full picture, criminologists have learned a great deal about the characteristics of victimization from those who do admit to being the victim of cybercrimes.

### 1.4. Victim Features

Much of the research on cybercrime victims has endeavored to understand who was victimized and why they were targeted by cybercriminals in the first place. However, this is a complex matter as the targets of cybercriminals have changed over time. For instance, in the United States in 2005, the telecommunications industry was the most likely to be victimized, followed by computer system design and chemical and drug manufacturing (Rantala, 2008). Yet in 2022, according to the FBI's cybervictimization data, the healthcare industry was the most victimized with the telecommunications industry being victimized at 12% the volume as healthcare (FBI, 2023). The primary reason for this shift is the valuable personally identifiable information stored in healthcare databases, which hackers can steal and monetize (Coventry & Branley, 2018; Lorenzini et al., 2022). Another increasingly targeted sector is the financial industry, although the industry's lack of reporting, as previously discussed, obscures the true figures (FBI, 2023; Kemp et al., 2022). Nevertheless, it is likely that banks are the most targeted sector as the large sums of money present in their clients' bank accounts provides a significant incentive to cybercriminals (Cadwell, 2014; Kemp et al., 2020; Korauš et al., 2017; Levi, 2016; Najaf et al., 2021). These financial incentives are further supported by the fact that wealthier nations with developed technological infrastructure experience higher levels of attempted cyber-attacks than other nations (Holt et al., 2016; Kigerl, 2012). However, these impacts are likely not

just due to the characteristics of companies and countries, but the characteristics of the people they represent.

This is because cybercriminals are increasingly bypassing the robust security of larger entities' databases to target unsuspecting individuals, a trend especially prominent in online banking (Arachchilage et al., 2016; Chiu et al., 2016; Gupta et al., 2016; Jaswal et al., 2022; Williamson, 2006). These studies indicate that cybercriminals are increasingly using tactics like phishing emails to steal banking credentials from their victims and commit online fraud. Increasingly, humans are the weak link in cybersecurity, which is why they are targeted by cybercriminals (Alsayed & Bilgrami, 2017; Gupta et al., 2016; Jaswal et al., 2022; Sasse et al., 2002; Yan et al, 2018). But what characteristics or attributes of an individual make them more likely to be victimized compared to others?

Firstly, the reason that humans are the weakest link in cybersecurity is that we have socialized desires to trust and cooperate with others, as well as a preference for convenience and inattention (Christiansen et al., 2019). These behaviors can lead individuals to engage in risky cyber behaviors such as visiting pornography websites, using weak passwords, clicking on suspicious links, and downloading unknown files (Bossler & Holt, 2013; Christiansen et al., 2019). However, these preferences can be counteracted, as individual sensitivity to indicators of cyber risks and their severity varies across topics, likely as a result of life experiences and education in specific cybersecurity aspects (Yan et al., 2018). In fact, while knowledge of security aspects is crucial to improving cyber defense, research by Squires & Shade (2015) shows that there can be a communication breakdown between IT staff and non-technical employees that perpetuates cyber-victimization.

Other aspects of human behaviors and tendencies also are indicative of cyber-victimization. For instance, individuals with low self-control are more likely to fall victim to virus infections, file tampering, and unauthorized password access (Bossler & Holt, 2010; Kerstens & Jansen, 2016; Ngo & Paternoster, 2011; Weulen-Kranenbarg et al., 2018). Additionally, people with high levels of neuroticism, openness to experiences, and sensation-seeking behaviors, but low levels of conscientiousness, are also more likely to be victims of cybercrime (Jones et al., 2019; Tcherni et al., 2015). Furthermore, individuals experiencing feelings of loneliness and isolation are also more likely to fall victim (Buil-Gil & Saldana-Taboada, 2021). Conversely, those individuals who exhibit cognitive reflection in their internet behaviors were less likely to open fraudulent emails (Jones et al., 2019). Interestingly, while not directly related to thinking patterns, individuals with higher levels of education experienced lower levels of hacking victimization (van Wilsem, 2013). However, research into other demographic factors that may influence cyber-victimization is limited.

In terms of age, FBI victimization data reveals that most cybercrime victims are older than 30, with those older than 60 experiencing losses on average three times greater than other age groups (FBI, 2023). This data is supported by a study indicating that older individuals report more hacking attacks (Leukfeldt & Yar, 2016). However, other academic studies have found no significant relationship between cyber-victimization and age (Bossler & Holt, 2009, Ngo & Paternoster, 2011). Thus, the effect of age is up for debate. Conversely, research consistently shows that females are more likely than males to be victims of malware or hacking incident (Bossler & Holt 2009, 2010; Button et al., 2012; Ngo & Paternoster 2011). Moreover, there is evidence to suggest that ethnicity or race is not significantly associated with cyber-victimization (Louderback & Antonaccio, 2017). However, while demographic information has helped to

understand who is more likely to be victimized, the literature shows that like thought processes, that particular cyber behaviors and tendencies are more predictive of cyber-victimization than demographic factors.

For instance, several studies have found that higher levels of computer use are positively related to cyber-victimization (Guerra & Ingram, 2022; Leukfeldt & Yar, 2016; Reyns, 2015; Yucedal, 2010). Specifically, it is not just increased usage but also the extent to which one's life revolves around technology that can increase vulnerability to cybercrime (Choi, 2008). Additionally, those who have been victims of cybercrime before are more likely to fall victim again, often because they do not change their risky online behaviors that lead to their victimization in the first place (Reyns et al., 2018). This is likely because people mistakenly believe that systems like anti-virus software will protect them from hackers, despite their activities (Jardine, 2020). However, an individual's proactive actions to avoid cyber risks effectively reduce their likelihood of victimization from cyber-attacks (Holt & Bossler, 2013).

In fact, the literature is divided on the effectiveness of anti-virus software and whether individuals are at less risk than those without this software. One side of the research suggests that increased computer security methods reduced hacking victimization, while simultaneously the lack of anti-virus software made individuals more likely to fall victim (Choi, 2008; van Wilsem, 2013). For example, in a separate study of almost 27 million Windows computers, researchers found that only 1.22% of the systems with antivirus had malware, compared to almost 15% of the computers without this software (Levesque, et al., 2016). Furthermore, an earlier study by Levesque and colleagues (2013) found that nearly half of the laptops given to participants would have been infected if anti-virus was not installed. However, this research also found that approximately 20% of the computers in the study were infected by malware that went undetected

by the anti-virus software (Levesque et al., 2013). This is likely because as technology evolves, hackers and the malware they create becomes more sophisticated and can evade detection systems like anti-virus software, leaving older software obsolete (Pérez-Sánchez & Palacios, 2022).

However, these conclusions are challenged by research that indicates that personal usage of anti-virus software does not have a significant effect on reducing victimization (Bossler & Holt, 2009; Reyns et al., 2018). In fact, in some cases, computer users with anti-virus software might be more likely to report being victimized than those without it (Jardine, 2020). This is because, computer users without anti-virus software were more likely to consider the riskiness of online threats and behaviors and chose safer actions, while those with the software had lower risk perceptions of the same threats and often chose to engage in riskier online behavior (Jardine, 2020). Corroborating a study by Pearman et al. (2016) it also was found that those with anti-virus software engaged in riskier cyber-hygiene practices such as visiting risky sites more frequently and not updating software applications. These findings cast doubt on anti-virus's effectiveness and support findings based on individuals with higher levels of cognitive reflection. Thus, while individuals with anti-virus software have more protection from a variety of malware than others, as they often engage in riskier behaviors online, it is difficult to determine definitively whether individuals with or without anti-virus software are more likely to be victimized.

However, one characteristic that clearly increases the likelihood of cybercrime victimization is being a victimizer oneself (Bossler & Holt, 2013; Choi, 2008; Kerstens & Jansen, 2016; Weulen-Kranenbarg et al., 2018; Wolfe et al., 2008). Individuals with higher levels of cyber deviance, including engaging in hacking or other illicit online activities, are more likely to become victims themselves (Choi, 2008; Wolfe, 2008), especially involving malware

victimization (Bossler & Holt, 2013). This crossover between offenders and victims is notable, particularly for less technical cybercrimes (Weulen-Kranenbarg et al., 2018). Yet, even for more technical hacking offenses, such as financial cybercrimes, there is also considerable overlap (Kerstens & Jansen, 2016). As in the cyber realm too, there exists no honor among thieves.

In summary, the literature on cyber-victimization has enhanced our understanding of the scale of cybercrime and who is most likely to be targeted. It has also contributed to insights on how individuals can better protect themselves. However, victimization only tells part of the story. To gain a more comprehensive understanding of cybercrimes, it also is essential to study how hacking occurs, which is the focus of the second stream of hacking research.

### 1.5. The Progression of the Hacking Event

Hacking is not easy nor requires a straightforward approach. Rather, hacking is highly sophisticated, with methods and techniques changing based on the hacker's goal and the victim's security. However, to successfully infiltrate a system hackers need to accomplish a consecutive series of steps (Dey et al. 2012; Hartley, 2015; Holt & Bossler, 2016; Hutchins et al., 2011; Maimon & Louderback, 2019; Marcum et al., 2014, Steinmetz, 2015; Young et al., 2007). These steps are known as the "cyber kill chain." Originally created as a militaristic model for combatting cyber-attacks by creating actionable intelligence for cyber defenders based on keen understandings of their adversaries, the kill chain also accommodates for insider threats, new technology, social engineering, and highly sophisticated attacks (Hutchins et al., 2011; Neubert & Vielhauer, 2020).

The first step of the kill chain is reconnaissance. In this initial phase, hackers gather information about their target before beginning the attack to determine any potential technical and social vulnerabilities (Dargahi et al., 2019; Hutchins et al., 2011; Maimon & Louderback,

2019). This stage can be done remotely on the internet (public websites and social media), or in the physical world (observing others computer screens) (Hutchins et al., 2011; Maimon & Louderback, 2019). With this information, an attacker formulates the best method to attack (Dargahi et al., 2019). Once the hacker has collected sufficient information, they move on to the weaponization phase. During this phase the attackers create malware, such as trojan horses or utilize Zero-Day vulnerabilities to create and disguise a custom package to exploit the weaknesses they observed during their reconnaissance (Hughes & DeLone, 2007; Hutchins et al., 2011; Maimon & Louderback, 2019; Wolfe et al., 2008).

Next, a hacker must find a way to deliver their malicious payload to their target. Hackers use many methods to do this from targeted phishing emails, USB drives, infected files, and employing other techniques to trick or compel the victim to deliver the digital payload (Hutchins et al., 2011; Dargahi et al., 2019). After the payload is successfully delivered to the target system and the victim has triggered the malicious code, the exploitation step begins. In this stage, the attacker's code targets vulnerabilities in the application or operating system, enabling them to gain remote access to the compromised system. (Hutchins et al., 2011; Waldrop, 2016). This initial access is a critical step in the attack chain. After gaining initial access, the hacker moves to the fifth step, installation. Using the existing digital foothold hackers aim to escalate the access they have within the system by uploading additional tools, modifying security protocols, and even creating new lines of code within the infected system (Dargahi et al., 2019; Hutchins et al., 2011). This privilege escalation then also enables lateral movement in the system, allowing a hacker to seek out sensitive information and critical data, as well as administrative access and email servers (Holz et al., 2009; Maimon & Louderback, 2019; Mirkovic & Reiher, 2004; Perkins et al., 2022). It is at this stage that hackers set themselves up to deal the most damage.

The next step, command and control (C&C or C2), the hacker leverages the accesses they have gained to take remote control over the compromised system and create a communication channel through which they can remotely manage the infected system and interact with the installed malware (Bahrami et al., 2019; Dargahi et al., 2019; Hutchins et al., 2011; Waldrop, 2016). This phase enables the hacker to issue commands to the malware, exfiltrate data, or carry out other malicious actions (Bahrami et al., 2019; Dargahi et al., 2019; Hutchins et al., 2011; Waldrop, 2016). Finally, with command and control established, the hacker can now act on their specific objectives. In the actions—on—objectives stage the hacker is able to accomplish a variety of actions such as: exfiltration of data, encrypting files, locking legitimate users out of the system, changing the appearance of the site (website defacement), altering databases, and even completely removing evidence of intrusion, just to name a few (Borgolte et al., 2015; Dargahi et al., 2019; Holt et al., 2017; Hutchins et al., 2011; Maimon & Louderback, 2019; Shakarian et al., 2013).

Importantly, the kill chain model serves as a valuable framework for understanding how hackers operate and move through various stages of an attack. Furthermore, it demonstrates that to protect systems from hackers that incident response should not only occur after the point of compromise or that compromises are the result of fixable flaws (Cichonski et al., 2012; Mitropoulos et al., 2006; Neubert & Vielhauer, 2020). Rather it shows that as the adversary must progress successfully through each stage of the chain before it can achieve its desired objective by disrupting any stage of the kill chain, security professionals can thwart the attacker's progress and prevent them from achieving their objectives (Hutchins et al., 2011). This assumption that hacking events can be disrupted after initial intrusion is further supported by literature that has

utilized new technologies to observe hacker behavior during a hacker's progression through the kill chain.

This research utilizes a computer system, known as a honeypot, deliberately designed to be vulnerable to cyberattacks, but serves the purpose of monitoring and recording key details about hackers who infiltrate the system such as the attack frequency, the attacker's target and the attack's source (Gupta & Gupta, 2019; Krishnaveni et al., 2018; Nawrocki, 2016; Perkins & Howell, 2021; Spitzner, 2003). Originally developed as a cybersecurity tool, computer science experts quickly began adapting and improving their function, making them less detectable by intruders and able to collect robust data on the hacker, such as IP addresses, operating systems, the attack's frequency, the attack's target(s), the attack's source, even email addresses (Alata et al., 2006; Holz & Raynal, 2005; Kaaniche et al., 2007; Leita et al., 2008; Nawrocki et al., 2016; Perkins & Howell, 2021; Pouget & Dacier, 2004; Trivedi et al., 2007; Yegneswaran et al., 2005). Collecting data on these newly observable characteristics empowers researchers to delve into both the technical and human aspects of cyberattacks and has proven invaluable for social scientists in their efforts to study the progression of hacking (Perkins & Howell, 2021).

The pioneering study that effectively utilized honeypot data to gain insights into the decision-making processes of hackers in action was conducted by Maimon and colleagues in 2014. Their research revealed that the display of a warning banner to individuals attempting unauthorized access to a system resulted in a reduction in the duration of these intrusion incidents (Maimon et al., 2014). Expanding on this research, Jones (2014) found that the content of the warning message played a crucial role in shaping the actions of hackers within the system. Specifically, Jones discovered that altruistic messages tended to discourage further unauthorized

entries, while messages with ambiguous wording or threats of legal consequences actually increased the number of commands entered by hackers (Jones, 2014).

Howell and colleagues corroborated these findings in their 2017 study finding that hackers increased their use of surveillance commands upon seeing warning banners with threats of sanction. Surveillance commands are typically employed to gather information about a computer's content and processes, often to assess the legitimacy of a potential threat, and are generally less intrusive. It stands to reason that these messages have a deterrent effect (Howell et al., 2017; Jones, 2014). Building upon this assumption, Maimon and colleagues (2019) further demonstrated that hackers who received unambiguous messages regarding surveillance altered their behavior by issuing commands to erase evidence of their intrusion. Moreover, hackers who suspected they were being monitored were more inclined to modify their behavior to avoid detection (Maimon et al., 2019).

Other studies suggest that the effectiveness of a warning banner in a honeypot environment may be influenced more by the characteristics of the hackers themselves rather than solely the content of the warning message. Wilson and colleagues (2015) conducted research that indicated that the presence of a surveillance banner in a compromised computer system reduced the likelihood of further commands being executed during initial intrusion events. Additionally, the surveillance banner deterred command entries in future intrusions by the same hacker if they had been discouraged during their first intrusion (Wilson et al., 2015). However, the study found that hackers who were not deterred by the warning banner in their initial intrusion were not deterred by the same banner in subsequent intrusions, suggesting that the effectiveness of the warning banner can vary based on the individual hacker's initial response to it (Wilson et al., 2015). Another study by Testa et al. (2017) further emphasized that the change in the actions of

hackers after encountering a warning banner depends on the level of administrative privileges the attacker has gained within the system. Specifically, the study found that hackers without administrative privileges were deterred by the warning banner, while those who had acquired administrative privileges in the attacked system remained undeterred by it (Testa et al., 2017). This highlights the importance of access privileges in influencing a hacker's response to warning banners. In essence, these studies underscore that the decision-making practices and behaviors of hackers are not static or uniform but rather change during the course of their criminal activities. Moreover, this change differs among hackers, challenging the notion that hackers are fixed or monolithic. In fact, hackers demonstrate a spectrum of distinctions that extend beyond decision-making processes within the act of hacking itself. The exploration of these variations among hackers constitutes the focal point for the third stream of hacking research.

### 1.6. Hacker Profiles

As with traditional offenders, it is difficult to describe the "generic hacker." Thus, early in the criminological study of hackers, researchers endeavored to create classifications to distinguish groups of hackers in the ecosystem, as hackers exhibit diverse characteristics, behaviors, and motivations. In 1985, Landreth introduced the first hacker typology, grouping hackers into one of five categories: novices, students, tourists, crashers, and thieves. Since then, researchers have employed different social scientific perspectives and data sources to create new classifications.

For example, researchers have investigated online forum activity to differentiate groups of hackers based on technical skill and posting frequency. These studies identified distinguishable groups, highlighting that novice hackers and those learning to hack far outnumber skilled hackers (Holt et al., 2012; Zhang, 2015). Instead of using forum activity, the

Hacker Profiling Project (HPP) used survey responses from hackers to classify them into categories such as script kiddies (low-level hackers), high-level hackers, and industrial espionage/terrorism hackers (ISECOM, 2012). While these classifications consider behavior over time and a cybercriminal's changing career, the drawback of studies like the HPP lies in their historical failure to incorporate critical distinguishing factors, notably attack frequency.

A more recent effort by Chng and colleagues (2020) sought to update past structures by conducting a comprehensive review of 11 past hacker classification attempts. Their classification system contained a total of 13 hacker subtypes based primarily on hacker motivations—an aspect frequently overlooked in previous classification systems (Chng et al., 2022). Although this classification also neglects to consider attack frequency, it does show the significance of understanding the motivations of cyber offenders.

In fact, hacker motivations are crucial to understanding their behavior and decision-making, as well as distinguish them from traditional offenders and from other hackers (Burruss et al., 2021; Chng et al., 2022; Holt et al., 2017, 2019, 2020; Leukfeldt et al., 2017; Maggi et al., 2018; Ooi et al., 2012; Romagna & van den Hout, 2017; Woo et al., 2004). These variations in motivations among hackers are known to influence factors such as target selection, persistence, and resistance (Burruss et al., 2021; Holt et al., 2019; Holt et al., 2020; Leukfeldt et al., 2017; Woo et al., 2004). However, understanding hacker motivation is useful for more than just classification, as their motivations lead hackers to attack different targets over others (Ooi et al., 2012). For instance, hackers with similar motivations tend to consistently choose similar targets and methods (Holt et al., 2020).

Hacker motivations range from personal financial gain, to testing their skills, to excitement and thrill seeking, to seeking prestige and admiration within the hacker community.

(Burruss et al., 2021; Holt et al., 2017, 2019; Holt et al., 2020; Leukfeldt et al., 2017; Ooi et al., 2012; Steinmetz, 2015). For example, participation in the hacker community, often facilitated through online forums, is a significant predictor of cybercriminal activity. (Holt, 2007; Holt et al., 2010; Jordan & Taylor, 1998; Morris & Blackburn, 2009). This desire for prestige in the community furthers the likelihood of criminal activity in that gaining a positive reputation in the hacker community often leads to their admission into an organized hacking team (Holt, 2013; Holt & Kilger, 2012). In these teams, hackers share knowledge, tools, and resources, as well as plan coordinated cyber-attacks (Décary-Hétu et al., 2012; Holt et al., 2012; Lu et al., 2010). Moreover, congruent with social learning theory, membership to a team creates a feeling of both identity and belonging among hackers, encouraging deeper involvement in hacking activities (Holt, 2007; Holt et al., 2010; Jordan & Taylor, 1998; Taylor, 1999). However, some hackers are not motivated by financial incentives or a sense of prestige at all, but rather are driven by nationalist and religious ideologies. These individuals who use hacking as a tool of political activism and opposing the status quo are known as hacktivists (Holt et al., 2017, 2020; Jordan, 2017; Romagna & van den Hout 2017; Woo et al., 2004).

Hacktivism differs from using the internet for publicity or communication by activist groups; rather, it is the idea that the internet is a place of political action (Jordan, 2016). Such actions include recreating civil disobedience and mass demonstrations in the digital space, creating free and secure access to information on the internet, as well as damaging the online infrastructure of entities a hacker disagrees with (Holt et al., 2016, 2020; Jordan, 2017). In fact, hacktivists act much like activists in the real world, purposively selecting their targets with the motivation to damage unliked groups and to draw attention to their cause, often with aggressive messaging, and are less easily deterred from criminal activity than their non-ideological

counterparts (Holt et al., 2016, 2019; Howell et al., 2019; Romagna et al., 2017; Woo et al., 2004).

Hackers exhibit a comparable level of diversity in their criminal careers, motivations, and targets when compared to traditional offenders. Similar to traditional criminological research, gaining insights into these distinctions among cyber offenders is crucial for comprehending the reasons behind their criminal actions and formulating effective preventive measures. However, due to the predominant inclination of hackers to maintain anonymity and operate covertly for self-preservation, scrutinizing their characteristics proves to be an exceedingly challenging task.

Fortunately, one subset of hackers defies this prevailing stereotype, providing a valuable avenue for research. In fact, much of our current understanding of hacker profiles stems from the examination of this specific group. Nevertheless, there remains significant gaps in our knowledge of these hackers, particularly concerning their criminal trajectories. This distinct category of hackers is commonly referred to as "website defacers."

### 1.7. Website Defacement

Website defacement is when a hacker takes advantage of a website's security flaws to gain administrative privileges and uses this unauthorized access to alter the website's content, completely disrupting legitimate use of the website and preventing the rightful owners from using their own website (Borgolte et al., 2015; Holt et al., 2017; Maimon & Louderback, 2019; Shakarian, 2013). Website defacement poses substantial threats and costly losses to these entities both financially and to the affected party's reputation (Bannerjee et al., 2021; Borgolte et al., 2015; Kanti et al., 2011). The threat of website defacement is also widespread, with thousands of websites a day falling victim to these attacks (Borgolte et al., 2015; Zone-H, 2022). This behavior is best conceptualized as a form of digital vandalism and is akin to criminal graffiti in

the real-world. The individuals who carry out these attacks are commonly referred to as "website defacers" or simply "defacers."

In recent years, criminologists have increasingly turned their attention to this sub-group of hackers because of the potential for gaining better insights into the most elusive aspect of the human side of hacking—understanding the hackers themselves. The distinction lies in the fact that while many hackers typically go to great lengths to conceal their identities and erase any traces of their cyber intrusions (Howell et al., 2017; Maimon & Louderback, 2019), defacers are much more overt in their activities and expressive of their motivations and characteristics (Holt et al., 2017, 2020; Romagna & van den Hout 2017; Woo et al., 2004). In fact, website defacers intentionally seek attention by leaving their hacker aliases on the websites they attack and by reporting their hacks to websites that verify and document such attacks (Woo et al., 2004). It is these websites cataloguing the thousands of hacks every day (Borgolte et al., 2015; Zone-H, 2022) that provide researchers with the abundant data needed to study these criminals (Holt et al., 2020b, 2020c; Howell et al., 2019; Maimon et al., 2017; Ooi et al., 2012).

One of the most widely used reporting websites in this context is Zone-H, and nearly all studies on website defacement rely on data from this source (Holt et al., 2020; Howell et al., 2019; Maimon et al., 2017; Ooi et al., 2012). It is worth noting that defacers can be considered a microcosm of hackers in general, sharing similar motivations and targeting preferences as other hackers. In fact, much of what we know about hackers as a whole stems from our understanding of defacers.

However, in contrast to other forms of hacking, website defacement attacks do not necessarily require attackers to possess highly advanced technical skills. There are numerous online tutorials available that explain how to infiltrate a server and change the content of a

website, making the process more accessible (Holt et al., 2016, 2017). Additionally, the tools for conducting these attacks are readily available and easy to deploy. Due to these factors, website defacement is often regarded as an entry-level form of hacking, which can serve as a steppingstone into more complex forms of cybercrime (Holt et al., 2016; Seebruck, 2015). Despite being considered an entry-level form of hacking, data obtained from sources like Zone-H provides researchers with a unique opportunity to study cyber offending behavior and determine what factors influence individuals to either persist in or desist from website defacement. In this pursuit, the research on website defacement heavily focuses on understanding variations in the motivations of website defacers. These motivations are closely linked to the frequency of attacks and the selection of targets (Holt et al., 2020; Howell et al., 2019; Ooi et al., 2012).

One key motivation for website defacers is the desire to gain status and recognition among their peers (Holt et al., 2017; Ooi et al., 2012; Woo et al., 2004). In pursuit of this, as mentioned, defacers report their defacements to Zone-H. However, some defacers also use social media as an attention seeking avenue and post about their motivations and achievements to gain a following and increase their prestige (Aslan et al., 2019; Maimon et al., 2017). However, studies suggest a hacker's social media activity can predict their future behavior. For instance, attack frequency varies by sociopolitical background and verbiage used in social media posts (Aslan et al., 2019). Moreover, evidence suggests defacers that use Facebook and Twitter have significantly higher successful attack volumes than those without these social media platforms (Maimon et al., 2017). This suggests that social media plays a significant role in the behavior and success of website defacers, as it can be both a means of self-expression and a way to connect with like-minded individuals in the hacking community.

While most defacers behave in pursuit of beating system administrators and gaining peer recognition, research has revealed the existence of distinct communities of defacers who are driven by nationalist and religious ideologies (Holt et al., 2017, 2020; Romagna & van den Hout 2017; Woo et al., 2004) The research also shows that defacers with ideological motivations behave differently than other defacers. For instance, the defacements carried out by ideologically motivated defacers often feature different and more aggressive messages (Woo et al., 2004). Moreover, these defacers tend to select their targets based on the potential notoriety and attention generated by their attacks (Romagna et al., 2017). Research also suggests that defacement volumes typically increase following real-world events that provoke ideologically motivated defacers (Balduzzi et al., 2018; Holt et al., 2020). Another notable difference in the attack patterns of ideological defacers is their resistance to deterrence. While most defacers are deterred from attacking systems in countries with a strong military presence, those with ideological motivations are not deterred (Howell et al., 2019). Rather, ideologically motivated defacers are more likely to target the websites of governments and companies whose interests the defacer disagrees with (Holt et al., 2020). In fact, hacktivists act much like activists in the real world as they possess more thoughtful target selection and that the motivations of their attacks are to damage unliked groups and to draw attention to their cause (Holt et al., 2019). Given these significant differences in behavior, understanding the motivations of website defacers is crucial for predicting their criminal trajectories and developing effective strategies for addressing cyber threats associated with their activities.

While the research on website defacers has recognized that defacers with different characteristics may exhibit varying attack frequencies, only a limited number of studies have observed defacement behavior over time. For instance, one study examined 119 defacers over a

two-month period and revealed the presence of two distinct groups: a large group of occasional defacers and a much smaller group of frequent defacers (Burruss et al., 2021). In a subsequent study, Weijer and colleagues (2021) observed the attack patterns of more than 66,000 defacers over a much longer seven-year period. This extensive study used various factors, including defacers' self-reported motivations, features of the victims' operating systems, and the attack methods employed by the hackers, in attempts to predict membership to six unique trajectory groups of defacers (Weijer et al., 2021). While both studies advanced the literature, there are many questions that remain about a defacer's criminal trajectory changes over time, and whether these trajectories can be predicted at the onset of a hacker's career.

### 1.8. The Proposed Research

Given what we know about hackers and specifically website defacers, my dissertation seeks to answer three research questions.

1. What are the major conclusions and knowledge gaps in the academic literature on website defacement?
2. How does defacers' activity change over time? What factors lead to a longer defacing career?
3. How do holidays impact defacement levels, between groups of defacers and broadly?

The dissertation will begin with a scoping review to address the lack of a comprehensive and systematic review that utilizes a scientific approach to summarize the current state of website defacement literature. To date, no such review has been conducted, despite the growing literature on website defacement. Utilizing the strict criteria and process checklist of the PRISMA-ScR protocol (Preferred Reporting Items for Systematic reviews and Meta-Analyses extension for Scoping Reviews), this study will use rigorous article sourcing, data coding, and analysis

procedures to create a review of past research findings about defacers and their victims. In doing so, it also aims to determine what criminological theories have been tested in the case of website defacement, especially to reveal the applicability of Life Course Criminology and the Routine Activities Theory. The review seeks to determine what programs, policies/practices, interventions, and laws are used to combat defacement, as well as discussing their applicability and effectiveness. Following this scoping review of the available literature to address the first research question, my dissertation will utilize two separate theories to answer the remaining research questions.

## 1.9. Theoretical Background

### *1.9.1. Life Course Criminology*

Over the past decades, researchers have made significant theoretical and methodological advancements in understanding the life-course engagement of individuals in criminal activities. Life-Course Criminology initially focused on evidence suggesting that most offenders exhibit a spike in criminal offending in late adolescence, peaking during an individual's early 20s, and then declining quickly after this period (DeLisi, 2015; Farrington, 1986a; Hirschi & Gottfredson, 1983; Tremblay & Nagin, 2005). This finding, which came to be called the age-crime curve, still remains the cornerstone of this theory, despite scholars' disagreements as to what explains the relationship between age and crime (DeLisi, 2014). Building on these initial findings, researchers sought to understand what causes individuals to begin, continue, and cease offending.

As the age-crime curve shows that offending begins in adolescence, researchers explored factors linked to the onset of criminal activity. Instead of a singular cause, research revealed that a multitude of risk factors from biological and environmental sources contribute to the likelihood of criminal onset (Bock & Goode, 1996; Farrington, 1990a; MacCord, 2001). Individuals with

higher risks of earlier onset anti-social and delinquent behaviors were found to be more likely to engage in more serious and violent crimes, as well as exhibiting prolonged and chronic criminality (Blumstein et al., 1986; DeLisi, 2005, 2006; Farrington et al., 1990a, 1990b, 2009; Laub & Sampson, 2006; Laub et al., 2018; Piquero et al., 2003; Wolfgang et al., 1987). This pattern highlights the importance and connectedness between stages of criminal activity across the life-course.

Research in these other stages is focused on understanding continued offending. Specifically, how individuals maintain a certain level of criminality over time, known as maintenance, the continuation of criminal activity over time, known as persistence, and the slow cessation of criminal activity, known as desistence (McGee & Farrington, 2019; Sampson & Laub, 1990, 1993). Individuals who continue to commit crimes are of increased importance in criminology as this small proportion of offenders who persist and maintain their criminal careers are responsible for around half of all crimes (Blumstein et al., 1986; Moffit, 1993; Wolfgang et al., 1987). Additionally, while most criminal careers are brief, longer lasting offenders are more likely to commit more serious offenses and cause more economic harm to society, despite societal pressure and government incapacitation efforts to deter them from offending (Cullen et al., 2011; DeLisi & Gatlin, 2003; Laub & Sampson, 2003; Liu et al., 2011; Whitten, 2017). Interestingly, individuals who are deterred and decide to leave their lives of crime do so gradually. Rather than quitting "cold turkey," they slowly reduce the frequency of committing crimes, often with long periods between offenses, making it challenging to determine when one has truly ceased offending (Bushway et al., 2001, Laub & Sampson, 2006, Kang & Kruttschnitt, 2022).

Due to the interconnectedness of onset, persistence, and desistence, researchers have found success in studying criminal behavior by examining the entire trajectory of offending rather than segmented parts of one's life (Blumstein et al., 1986; DeLisi & Piquero, 2011; Elder et al., 1985; Farrington, 1986b; Laub & Sampson, 2006; Laub et al., 2018, 2019; Nagin, 1999, 2005, 2016; Piquero, 2008). For example, multiple studies have successfully plotted life-course criminal trajectories and predicted membership in certain groups of offenders (Benson, 2013; Burruss et al., 2020; DeLisi & Piquero, 2011; Elder et al., 1985; Laub & Sampson, 2006; Laub et al., 2018, 2019; Nagin, 1999, 2005, 2016; Piquero, 2008). These findings support the assumptions of the age-crime curve and highlight that a small number of chronic offenders are responsible for most criminal offenses, with longer-than-average careers (Burruss et al., 2020; Farrington, 1986; Nagin, 1999, 2005, 2014, 2016; Piquero, 2008; van de Weijer et al., 2021). Additionally, studies of criminals over their life course have identified certain life events, known as transitions and turning points, that lead individuals toward conformity and away from criminal activities (DeLisi & Piquero, 2011; Laub & Sampson, 2006; Laub et al., 2018, 2019; Nagin, 1999, 2005, 2016; Piquero, 2008; Sampson & Laub, 1990, 1993, 2018). Some examples of these events are marriage, having children, higher education, and career attainment (DeLisi & Piquero, 2011; Laub & Sampson, 2006; Laub et al., 2018, 2019; Nagin, 1999, 2005, 2016; Piquero, 2008; Sampson & Laub, 1990, 2018). In fact, much of what we know about what causes persistence or desistance from crime comes from these longitudinal studies of criminal careers. However, there is one particular kind of offender that has not benefitted from these types of studies, the cyber offender.

While life-course criminology (DeLisi & Piquero, 2011; Laub & Sampson 2006; Laub et al., 2018, 2019; Sampson & Laub, 1990, 2018) and trajectory modeling (Nagin, 1999, 2005,

2014, 2016) have become standard tools for studying crimes in the physical world, they are not frequently applied to the study of cyber-offending, revealing a significant gap in research. This gap presents an opportunity to use these established methods to better understand the life-course and criminal trajectories of individuals engaged in cybercrime, including activities like website defacement.

Studying the careers of cybercriminals presents unique challenges due to the inherent characteristics of cybercrime. These challenges make it difficult to study the behavior of the majority of cybercriminals longitudinally. While the behavioral changes of traditional offenders are relatively well understood, there is limited knowledge about how the patterns of cybercriminals change over time (Burrus et al. 2020, Décary-Hétu 2012, Hughes et al. 2019, Weijer et al. 2021, Zhang 2015). One significant challenge is the anonymity that cybercriminals enjoy, making it difficult to gather comprehensive offense records and measure traditional life events or turning points that typically influence individuals to transition away from a life of crime, such as relationships or stable employment. These obstacles, coupled with the unique nature of cybercrime, create significant challenges when attempting to apply life-course theory to explain cybercriminal behavior.

Nevertheless, research using this theoretical framework to enhance our understanding of cybercriminals has not been fruitless. For instance, Hughes et al. (2019) used group-based trajectory modeling to reveal that users of online gaming forums fall into one of five distinct groups (i.e., Fickle, Decliner, Sustainer, Engager, and Super-Engager), and that membership to these groups is predicted by posting frequency. Another study by Weulen-Kranenbarg and colleagues (2018) observed and compared suspected cyber offending and traditional offending over individuals' lifetimes. They discovered that, akin to traditional criminals, individuals are

less inclined to commit cybercrimes during years when they share a household with a partner (Weulen-Kranenbarg et al., 2018). However, while education and employment reduce the likelihood of traditional offending, computer technical education and employment in the information technology industry increases the likelihood of committing a cybercrime, contrary to traditional conclusions of life-course criminology (Weulen-Kranenbarg et al., 2018). More recently, research by Weijer and colleagues (2021) delved into the attack volumes of defacers by scrutinizing the attack patterns of over 66,000 defacers over a seven-year period. Their findings identified six distinct groups of defacers distinguishable by both attack volume and frequency as well as a small percentage of defacers being responsible for the majority of attacks, akin to findings in traditional criminology (Weijer et al., 2021). It is worth noting, however, that they were unable to predict membership in these groups based on hacker characteristics (Weijer et al., 2021). Despite these valuable contributions, it is important to highlight that, to date, no known study has succeeded in plotting and predicting the longitudinal criminal careers of cyber-offenders. My dissertation will begin to fill this gap in the research by presenting a paper that endeavors to meet this research goal by predicting belonging to trajectory groups.

### *1.9.2. Routine Activities Theory*

The Routine Activities Theory (RAT) was first introduced to the field of criminology by Cohen and Felson in 1979 as a derivative of the Rational Choice paradigm. Their landmark paper presented what they called a "routine activity approach" to understanding crime trends and cycles by focusing not on the characteristics of offenders, but on the circumstances of the situations in which they commit criminal activities (Cohen and Felson, 1979). At the core of this theory lies the idea that criminal activity occurs when three conditions converge in space and time: "likely offenders, suitable targets and the absence of capable guardians against crime"

(Cohen and Felson, 1979). Conversely, crime is likely to be prevented when any or more of these conditions are not met (Branic, 2015; Jennings, 2015). To elaborate further, "likely offenders" are generally defined as individuals who are motivated to commit a crime (Felson & Cohen, 1980; Felson & Clarke, 1998; Gotham & Kennedy, 2019). "Suitable targets" refer to individuals or objects that attract likely offenders as potential targets for criminal activity (Cohen & Felson, 1979; Gotham & Kennedy, 2019). On the other hand, "capable guardians" are conceptualized as individuals who have the power to protect potential crime targets and who's presence both increases the risks and decreases the rewards for motivated offenders, thus serving as an effective deterrent (Becker, 1968; Gotham & Kennedy, 2019; Hollis et al., 2013; Purpura, 2013). In essence, RAT provides an environmentally focused explanation for the causes of criminal activity by emphasizing the interaction of these three conditions in criminal events.

Since its inception, RAT has played a pivotal role in criminological research, serving as a framework to explain a wide range of criminal activities, from armed robbery and burglary to drug dealing and numerous others. Researchers have extensively explored each of RAT's three conditions, delving into the detailed effects of each dimension. Notably, the conditions most frequently scrutinized in the literature appear to be "suitable targets" and "capable guardianship." This emphasis may stem from one of the significant critiques of RAT, which assumes that offenders are rational actors (Kitteringham & Fennelly, 2020; Sasse, 2004). While RAT has been extensively used to comprehend traditional crimes, it has found limited application in explaining less traditional crimes. One such example is the relatively understudied field of cybercrimes.

### *1.9.3. Routine Activities Theory in Cyberspace*

While RAT is less commonly employed to explain cybercrimes, it, along with a derivative known as the Lifestyle Routine Activities Theory, has shown moderate success in

explaining various forms of cybercrime (Guerra & Ingram, 2022; Maimon & Louderback, 2019). Notably, most of the research applying RAT to cybercrimes has focused on victims of phishing, malware/virus infection, and hacking victimization (Guerra & Ingram, 2022; Howell et al., 2019; Leukfeldt & Yar, 2016; Pratt et al., 2010; Reynes 2015; Wilsem, 2013; Yucedal, 2010). For instance, the amount of time individuals spend online, considered as a measure of their proximity to potential offenders, has been found to increase their likelihood of falling victim to various cybercrimes (Leukfeldt & Yar, 2016; Pratt et al., 2010; Reynes, 2015; Wilsem, 2013; Yucedal, 2010). However, it is important to consider the types of digital spaces where potential victims spend their time. Studies reveal that activities on sites like online shopping, emailing, or chat rooms do not significantly increase the odds of victimization. Conversely, time spent on "risky sites," such as those associated with media piracy or pornography, significantly heightens an individual's risk (Holt & Bossler, 2009; Leukfeldt, 2014).

In measuring target suitability, Kigerl (2012) discovered that wealthier nations experience a higher volume of phishing and spam-related emails. Furthermore, Maimon and colleagues (2013) observed that cyber-attacks against university networks were more likely to occur during business hours, likely due to the increased visibility and accessibility of potential targets. Lastly, Holt and colleagues (2018) found that countries with greater technological infrastructure, more political freedom, and less organized crime were more prone to report malware infections. These findings exemplify how RAT can be effectively employed to explain cybercrime victimization.

#### *1.9.4. Capable Guardianship in Cyberspace*

However, understanding the role of capable guardians in cyberspace has proven to be a complex challenge, with different conclusions drawn in the academic literature. For instance,

Grabosky and Smith (2001) argue that cybervictimization often occurs due to a lack of capable guardians. Other scholars suggest that the use of antivirus software serves as a form of physical guardianship (Mell et al., 2005; Taylor et al., 2006). In more recent research, capable guardianship, measured by a country's military presence, was found to reduce the likelihood of recreational website defacement attacks (Howell et al., 2019).

Conversely, there are studies that have yielded differing results, showing no significant effect of capable guardianship in the realm of cyberspace. For instance, two separate studies using different samples found that computer software designed to detect and remove malware had no discernible impact on reducing the likelihood of victimization (Bossler & Holt, 2009; Wilsem, 2013). Additionally, these studies revealed that a user's personal knowledge of cyber risks did not contribute to a decreased likelihood of being hacked or falling victim to malware (Bossler & Holt, 2009; Wilsem, 2013). While the creators of such software solutions may argue for their ability to protect individuals from victimization, it remains inconclusive whether guardians in cyberspace can be deemed truly capable.

This is not the first instance where varying results have spurred criminological debates regarding the applicability of RAT to the realm of cybercrime. In the past, Yar (2005) argued that the convergence of motivated offenders, suitable targets, and the absence of a capable guardian could not occur in cyberspace, based on the premise that cyberspace is inherently "anti-spatial." However, in subsequent years, an argument put forth by Reyns and colleagues (2011) led many to assume that the convergence of these three elements is indeed possible, regardless of their physical locations, due to the interconnected network systems of the internet. Nonetheless, I believe that the debate concerning the applicability of RAT in cyberspace remains ongoing and

incomplete. Specifically, there is a need to question the relevance of capable guardianship in the context of cyberspace.

I assert this concern not solely based on the contradictory evidence emerging from research results but also due to the manner in which capable guardianship is defined and applied. In most cases, capable guardianship is operationalized through the use of anti-virus software. However, considering Cohen and Felson's (1979) assertion that a capable guardian must be physically present, can we confidently assume that hackers are genuinely deterred by the mere presence of this software? Furthermore, it is essential to note that Cohen and Felson originally conceived of a capable guardian as a person, rather than equipment. According to the principles of the Routine Activities Theory, the presence of a capable guardian increases the risk of offending, while the absence of such a guardian creates situations conducive to criminal activity (Hollis et al., 2013). Additionally, for guardianship to be considered capable, it must create a perception that a criminal believes will heighten the risk associated with engaging in their criminal act (Hollis et al., 2013). However, anti-virus software, in and of itself, poses no inherent risk to cybercriminals.

Considering this line of thinking, the use of such software could alternatively be viewed as a form of target hardening, making the computer less of a suitable target rather than being protected by a capable guardian. In the physical space, we would not typically label security cameras, barbed wire, or fences as capable guardians, but in cyberspace, their digital equivalents are often treated as such. It is perhaps these ambiguities and inconsistencies that contribute to the contradictory results among research studies.

Given the lack of a clear and standardized definition of what constitutes a capable guardian in cyberspace, my dissertation will test a new method to measure the absence of

capable guardianship. This innovative approach, though not yet explored in academic literature, has garnered attention and recognition from government agencies and cybersecurity practitioners who identify it as a pronounced vulnerability: the absence of protective IT staff during holidays.

### *1.9.5. Holidays and Traditional Criminology*

Holidays present an interesting case for the study of crime as they produce a disruption in societal routines as thousands, if not millions, are given the day off of work. While perhaps businesses such as grocery stores or restaurants remain open on these days, most office spaces are noticeably empty as employees use the day to relax, vacation, travel, or spend time with family. The school schedule is also disrupted, with public and private schools from pre-school to universities giving students the day off in observance of the holiday. This break from the regular routines of life has led scholars to examine these disturbances for changes, not in sanctioned behaviors, but of unsanctioned behaviors such as criminal activity, through the lens of the Routine Activities Theory. As my research is the first to examine the effect of holidays on cybercrimes, it is necessary to review the research on holidays and crime in the physical space.

The earliest studies of changes in criminal behavior as a result of holidays were conducted by Lester in the 1970's and 80's. His research found that homicides tended to increase in number on major holidays and attributed this effect to increased connections between friends, family, and acquaintances on these days, as well as the propensity for increased alcohol consumption (Lester, 1979, 1987a, 1987b). Subsequent studies supported these early findings for murders and extended them to other forms of violent crime on holidays including assault, intimate partner violence, and disorderly conduct (Baird et al., 2019; Cohn & Rotton, 2003; Khurana et al., 2022a, 2022b; Kudryavtsev & Kuchakov, 2021; Rotton & Frey, 1985). Interestingly, this spike in violent criminal activity appears to transcend cultural boundaries, with

similar effects observed across populations in the US, Russia, and the UK (Baird et al., 2019; Khurana et al., 2022a, 2022b; Kudryavtsev & Kuchakov, 2021).

However, evidence suggests that certain groups are not as affected by holidays. For instance, Baird et al. (2009) found that while holidays saw increases in homicides compared to the average rate, homicides performed by those with a history of mental illness were more common on weekdays. Additionally, in studying the relationship between Islamic holidays and terrorist attacks in select countries in the Middle East, Reese et al. (2017) found that Islamic terrorist organizations reduced their attacks during holidays, likely due to societal disapproval. These findings indicate that the effect of holidays on criminal activity is not universal and, in some cases, may even have a negative impact.

In fact, research has shown that the impact of holiday-induced changes in crime levels largely depends on the type of offense being examined. While most of this literature focuses on crimes against human victims, studies on holiday variations in offenses against non-human targets reveal an opposite effect. For instance, two separate studies found that economic crimes against personal property, such as theft, burglary, and robberies occurred less frequently on holidays (Cohen & Rotton, 2003; Lam, 2020). These studies argue that the reduction in property-based crime during holidays is a direct reflection of the capable guardianship aspect of the Routine Activities Theory. Simply stated, the presence of individuals at home, rather than at work, acts as a deterrent against property crimes by simultaneously reducing suitable targets and increasing the presence of capable guardians (Cohn & Rotton, 2003). Lam's (2020) study built upon the conclusions of Cohen & Rotton, revealing that holidays typically spent at home experienced lower levels of burglaries and robberies compared to non-holiday periods and

holidays typically spent outside the home. These findings show that the change in levels of guardianship is an important factor when considering crime on holidays.

These studies collectively demonstrate that holidays disrupt the normal flow of criminal activity just as they disrupt sanctioned activities. Furthermore, they alter the typical convergences of motivated offenders, suitable targets, and capable guardians. However, academic literature has yet to explore how holidays affect the behaviors of cyber-criminals. While we may expect these days to change the offending behaviors of criminals in the digital space, there have been no tests of this assumption. Specifically, holidays could impact the actions of hackers in that they may have increased time to commit their offenses with time off from school and work or from reduced guardianship, as workers dedicated to protecting digital systems are away from work. This paper aims to initiate an exploration of the impact of holidays on the behaviors of hackers.

#### *1.9.6. Holidays and Hackers*

As previously mentioned, while employers differ in their practices, most companies follow the norm of giving employees the day off for holidays. However, while these days are consistently looked forward to by employees as welcomed time off for vacations and time with family, it appears that hackers also look forward to these days to conduct their attacks. For instance, in 2021, the FBI and CISA (Cybersecurity & Infrastructure Security Agency) stated that "an increase in highly impactful ransomware attacks occur[s] on holidays and weekends — when offices are normally closed — in the United States" and also stated that "hackers often target companies over holiday weekends when security operations centers may be ill-equipped to handle such threats." So, while IT staff may be enjoying their time off, hackers leverage their absence to attack the systems they protect. While CISA and the FBI did not divulge any data to

support this practice, the agencies appear convinced that businesses are giving IT staff time off on the holidays and that this creates an environment conducive to increased levels of cyberattacks (CISA, 2022). In fact, the assumption that holidays leave the targets of hackers more vulnerable is also shared by journalists, and cybersecurity professionals (Barret, 2021; CISA, 2022; Eaton, 2009; Kapko, 2022; Middleton, 2022; Sakellariadis, 2022; Sganga, 2021a, 2021b; Tung, 2021). All these entities come to this conclusion as a result of the assumption that organizations will have fewer to no IT staff to perform actions such as network analysis and incident response (Barrett, 2021; Eaton, 2009; Kapko, 2022; Middleton, 2022).

But are IT staff given time off in the same way as other employees? Well, as perhaps expected, companies are not advertising when they are and are not digitally protected. Thus, there is little direct evidence of IT staffing practices. In seeking to understand more about whether holidays truly lead to decreased levels of guardianship from IT staff, I conducted open-source intelligence and informal interviews with working professionals at large technology companies and IT staff at small to mid-size companies. Firstly, I examined multiple forums, such as Glassdoor, where employees can anonymously discuss their company's practices and examined the discussions of PTO and holiday time for the largest IT firms. Overall, it seems as though practices vary across firms, but that employees are either given these days off or welcome to use PTO to celebrate the holidays they want to. There were no mentions of being required to work on holidays or increased holiday staffing on these forums. Secondly, examining the job postings for IT staff openings revealed a mixture of positions regarding holidays off and flexible PTO. Although it should be noted that many job postings simply did not mention holiday policies in the posting. My interviews further supported the assumption that holidays lead to less capable guardianship from IT staff and confirmed that the effect varies by company. The

conversations with the respondents showed that while the larger firms are likely to have some sort of IT presence on holidays, though it may be reduced, employees of smaller firms with low numbers of IT staff, would likely have no IT personnel on duty over the holidays. Unfortunately, individuals working for government agencies, specifically my contacts at the NSA and FBI, were unable to comment on the IT staffing policies of their agency on holidays. However, the interviewees who could respond agreed with the FBI and CISA's assumption that in general systems would be less protected from hackers on holidays.

Somewhat shockingly, these assumptions of IT staffing are also supported by the companies themselves. In a survey of businesses, respondents admitted to lower staffing on holidays and stated that identifying, stopping, and recovering from cyber-attacks would take longer if the attack occurred on a holiday (Kapko, 2022). This lack of personnel lessens the chance an attack will be detected and allows hackers more time to escalate privileges and worsen the severity of the attack (Barrett, 2021; Kapko, 2022). Additionally, if an attack occurred on a holiday, it would be more difficult for cyber-defenders to assemble the needed personnel to quickly and adequately respond (Barrett, 2021). Interestingly, larger companies (over 2,000 employees) were more likely to experience longer delays in their response (Kapko, 2022). Furthermore, despite businesses awareness and fear of victimization over holidays, many companies have no contingency plans in place to respond in the event of a cyber-attack (Sganga, 2021b). These assertions align with the facets of the absence of capable guardianship dimension outlined in the RAT framework. While most assumptions and discussions on the lack of capable guardianship from IT staff focus on the potential for severe attacks, like ransomware, the decrease in capable guardianship would logically open a target to any form of hacking. For

instance, journalists observing trends in website defacement incidents on the Zone-H website claim there is evidence of a “traditional Christmas defacement spree” (Scwartz, 2005).

Based on the findings from the literature on traditional crimes and holidays and the conclusions from cybersecurity professionals and leading government agencies, holidays appear evident of a lack of capable guardianship. However, this has yet to be expressly tested in the academic literature for any kind of hacking, let alone website defacement. If traditional criminals understand holidays to be times of increased guardianship of the home, is it not feasible based on the evidence above, to assert that hackers could assume that this leads to a reduced level of guardianship in the digital space as the protectors of digital networks are at home celebrating? Thus, my research approach seeks to broaden our comprehension of whether cybercriminals perceive the presence of guardians and, subsequently, how such awareness influences their decision to attack and successful defacements.

### 1.10. Research Hypotheses

In my dissertation, I aim to fill gaps in the existing literature while addressing hypotheses derived from Life-Course Criminology and Routine Activities Theory. The second research paper will focus on two hypotheses regarding the criminal careers of website defacers. Based on the Life-Course Criminology literature, in our paper focusing on the criminal careers of website defacers we expect to find different trajectory groups among website defacers during their first year of offending. Additionally, we expect that like traditional criminals that the individual characteristics of defacers can lead to the prediction of group membership and thus who will persist and desist from website defacement.

The third research paper will explore three hypotheses related to event-motivated defacement and the absence of a capable guardian. Specifically, it will investigate the assumption

that defacement volumes increase during holiday periods. Additionally, if holidays indeed result in higher defacement levels, we anticipate that defacers with similar traits will exhibit distinct patterns of offending compared to other groups during holidays, driven by variations in motivation. Similarly, because of regional and motivational differences, Middle Eastern defacers should display an increase in defacements on Islamic and Jewish holidays. Advanced statistical models will be employed to test these hypotheses using unique data.

## 1.11. Methods

### *1.11.1. Data*

Data on website defacement is obtained from Zone-H, a widely recognized archive established in 2002 (Maimon et al., 2017). Zone-H serves as a repository for information on successful website defacements, with over 168,000 active users and 15 million verified attacks worldwide. Nearly all past studies on website defacement use this archive as the primary data source (e.g., Weijer et al., 2021; Burruss et al., 2021). As the studies examine the offending behaviors of hackers, the beginning of their criminal careers were defined as their first self-reported defacement to Zone-H. Various exclusion criteria were introduced to ensure a proper sample, these criteria are discussed in the method sections of the corresponding papers. After the initial sample was collected a detailed analysis of the defacements paired with further Open-Source Intelligence methods was conducted to determine defacer traits. This process created variables for political and religious content, team membership, social media presence, and contact information. The dependent variable on offending behavior is tailored for each paper based on the study's goals, allowing for a nuanced exploration of attackers' development and the impact of events on their activities.

### *1.11.2. Models*

For the study of defacers' criminal careers, we will employ a latent group-based trajectory modelling approach that enables tracking the attack prevalence of defacers over time to estimate new hackers' hacking trajectories (Nagin 1999, 2005). Known as group-based trajectory models, these models are a form of finite mixture models that are used to investigate population differences in the developmental courses of behaviors or outcomes over time. This study will use these functions of group-based trajectory modeling to distinguish between the groups of hackers with different attack volume trajectories and analyze the impact of several time-invariant predictors on the probability of group membership. Additionally, in our study of the impact of capable guardianship multi-level models will be used as they best fit the nature of our data. Multi-level models are a powerful statistical approach that allows for the analysis of data with a hierarchical or nested structure (Bryk & Raudenbush, 1988; Goldstein, 2011; Gordon, 2019; Nezlek, 2020; Preacher, 2021; Raudenbush & Bryk, 2002), such as when observing the defacing trends of individual hackers. Using a multi-level mode allows us to estimate the effects of holidays at both within and between defacers, which offers a more accurate results while accounting for the clustering of observations within defacers.

## 1.12. Outline of the Dissertation

This dissertation is divided into a total of five sections. The first section was an introduction, which you have just finished reading, that presented a description of hacking and website defacement, a discussion of relevant criminological theories tested in the dissertation, and a description of the research strategies and goals for each paper. The second section presents the first paper of three, which is a scoping review of the website defacement literature. This paper follows the outline for scoping reviews under the PRISMA protocol and thus does not

follow the same structure as the following two sections. The third section presents the paper published in Computers & Security that examines the criminal trajectories of website defacers. This section is comprised of an introduction, review of relevant literature, discussion of methods, the results of the models, and a discussion of the findings. The fourth section presents the final paper, which follows the format of the second paper. This paper presents the first test of how holidays impact the behavior of website defacers and provides a test of how capable guardianship applies in cyberspace. Finally, section five presents a short discussion based on the findings from the papers discussed above and provides suggestions for future research.

### 1.13. Summary

In summary, the dissertation aims to bridge gaps in understanding cybercriminal behavior. By investigating the developmental patterns of website defacers and examining lapses in capable guardianship, especially during holidays, the research contributes to addressing critical voids in the current scholarly landscape. Despite advancements in traditional criminological research, the complexities of cybercrime demand a more tailored approach to better comprehend and mitigate cybercriminal activities.

# Chapter II: A Scoping Review of Website Defacement: The Problem, Practices, and Prevention.

## 2.1. Abstract

Websites are fundamental components of the internet, serving as both its backbone and face. However, despite their ubiquitous presence in online browsing, they are frequent targets of cyber-attacks. Hackers employ various technical methods to gain unauthorized access to websites, effectively usurping control from legitimate owners, and manipulate the appearance of websites. This paper aims to enhance our understanding of such attacks by conducting a scoping review of existing literature on website defacement.

Following the rigorous methodology outlined by Tricco et al. (2018) for scoping reviews, this study systematically identifies and analyzes relevant articles. The review synthesizes findings from these articles, with a particular focus on the findings about the characteristics of the perpetrators and their victims.

This review identifies several key findings regarding the study of website defacement presenting opportunity for future research. Firstly, there is a notable emphasis on understanding offenders, while limited attention is given to victims' experiences. Predominantly, Routine Activities Theory is employed to comprehend offender motivations, revealing diverse motivations driving website defacements. However, much less knowledge exists in understanding the role of suitable targets and capable guardianship in defacement attacks. While emerging perspectives like Social Learning Theory and Life-Course Criminology provide additional insights into the social dynamics and criminal trajectories of defacers, they are sparingly utilized in the literature. Additionally, methodological challenges, including an overreliance on self-reported data and limited causal analysis, raise concerns about the reliability

of findings. Moreover, while some research uses non-defacement data, its validity for studying active hackers remains questionable. Overall, the review underscores the need for a balanced approach focusing on both offenders and victims, exploring diverse theoretical perspectives, addressing methodological challenges, and engaging directly with offenders to enhance understanding of website defacement.

These identified gaps serve as important pointers for future research endeavors, directing attention toward areas that require further investigation to enhance our understanding of this cybersecurity threat.

## 2.2 Introduction

Website defacers (hereafter called defacers) are hackers that engage in what can be described as digital vandalism, in a cyber-crime known as website defacement. Defacers take advantage of security flaws in a website's or internet server's digital infrastructure to gain administrative privileges while simultaneously blocking the use of the owners of the website. The defacer then alters the appearance of the website or a webpage, completely disrupting legitimate use of the website (Holt et al., 2016). Unlike most hackers who prefer to shroud themselves in anonymity, defacers are more open with respect to their identities and activities. For instance, defacers attempt to gain attention and a reputation within the hacking community by reporting their defacements on platforms devoted to cataloging these attacks (e.g., Zone-h.org) and by bragging about their attacks on social media (Aslan et al., 2020; Maimon et al., 2017).

In fact, defacers often share tutorials on social media platforms like Facebook and YouTube, providing step-by-step guides on how to infiltrate servers and change website content (Holt et al., 2017). Additionally, the tools for conducting these attacks are readily available and

easy to deploy, making website defacement more simplistic than other forms of hacking. For this reason, website defacing is typically considered an entry-level form of hacking that can lead individuals into other forms of cybercrime (Seebruck, 2015).

Despite being an entry-level form of hacking, website defacements are a widespread security issue. While most incidents target private individuals or small to medium-sized companies, even major corporations, healthcare systems, and government websites are frequently defaced (Maimon & Howell, 2020; Howell et al., 2019). Although the visual change may seem trivial, defacement results in significant financial losses due to lost revenue during site downtime and reputational damage from perceived poor security (Kanti et al., 2011).

However, despite the frequency of this type of hack, amounting to over 15 million reported attacks in the last 10 years (Zone-h.com), and a growing body of literature on website defacers, a review of the extant literature has not been concluded. Current research is moving beyond descriptive statistics and bi-variate regression models for more complex research designs and statistical models, such as group-based trajectory modeling. Therefore, a scoping review is necessary to provide future researchers and policymakers with a comprehensive overview of the evidence on website defacement and identify areas for further research and improvement.

Despite dozens of publications on website defacement in the past years, no scoping reviews or protocols for such reviews exist to synthesize the available knowledge and gaps in the research on website defacement. This review seeks to summarize what is known about website defacers and the victims of their attacks. In doing so, it also aims to determine what criminological theories have been tested in the case of website defacement, especially to reveal the applicability of the Routine Activities Theory. It also seeks to review the methods and data sources used to study defacement and if there is need for increased diversity or improvement.

In short, the goal of this procedure is to present an overall picture of current evidence about website defacers and their victims. It will summarize the outcomes, study design, and main findings/conclusions of the included literature. While this planned analysis is more descriptive in nature, as the first review of its kind in this research area, it is a needed first step to identify the current evidence and reveal knowledge gaps.

## 2.3. Methods.

### *2.3.1. Protocol and Registration*

To the best of our knowledge, there are currently no existing comprehensive reviews specifically focused on the literature surrounding website defacement. The closest semblance to such a review are two reviews of the academic literature in computer science related to defacement "detection technology" that can alert administrators to the web attack (Albalawi, et al., 2022; Riera et al., 2020) which can be used to potentially detect a hackers attempt to deface a website before it occurs, and a review of "The evolution from Traditional to Intelligent Web Security" (Martinez Santander et al., 2020) also focusing on computer science literature and is not restricted to website defacement. These papers may discuss topics that are of technical importance to how website defacements are perpetrated, that is computer vulnerabilities that defacers utilize, but they do not fulfill the need for a thorough review of the broader understanding of website defacement and the associated parties involved. Given the absence of previous reviews specifically on website defacement and the lack of review protocols to follow, we employ the PRISMA Extension for Scoping Reviews (Tricco et al., 2018) to guide the methodology for our current review. This approach ensures a systematic and transparent process in our exploration of the existing literature on website defacement.

### *2.3.2. Eligibility Requirements*

Studies will be included if they:

- Examine the perpetrators or victims of website defacement.
- Examine the offending behaviors of website defacers.
- Published and unpublished studies will be included, incorporating research in scientific journals, conference paper archives, and gray literature.
- Written in English. As the author speaks English and the substantive body of the literature is in English.

Studies will be excluded if they:

- Are commentaries, news/magazine articles, or opinion pieces.
- Focus on the technical aspects of how to deface websites.
- Focus generally on computer hacking but mention website defacement only briefly.
- Focus on computer hacking practices that can be used in website defacement but does not discuss website defacement.
- Focus on creating detection systems to alert IT admin about a defaced webpage.
- Focus on developing algorithms and technical tools to prevent defacement.
- Are not in English.

Thus, the filtering questions to be applied to all returned documents are:

1. Does the study focus on the sociological or criminological aspects of website defacement, including perpetrators/offenders, victims/targets, and tactics/procedures/effects of defacement, and related inquiries? Yes -> include, No -> exclude.
2. Is the paper about a detection system to prevent or respond to defacement attacks? Yes -> exclude. No -> include.

3. Does the paper focus on the technical aspect of defacing websites by explaining how vulnerabilities are exploited without connecting them to the preferences of offenders? For instance, does the paper focus on computer specifications, instructions, procedures, or policies rather than on the offender. Yes -> exclude. No -> include.
4. Is the paper a commentary, news article, or opinion piece? Yes -> exclude. No -> include.
5. Is the paper published in English? Yes -> Include. No -> Exclude.

### *2.3.3. Information Sources*

The search for relevant academic literature commenced on December 12, 2023, across various academic databases and concluded on the same day. Supplementary sources were identified through consultations with experts and by conducting forward and backward searches of references on December 20, 2023. The review aimed to identify pertinent studies from a range of academic databases as well as grey literature sources. Additionally, the first 100 results from Google Scholar were examined to identify any potentially overlooked articles that could meet the criteria for inclusion in our review. This comprehensive approach ensured the thorough exploration of available literature on the subject of website defacement. The data sources are listed below.

1. **Academic Databases**: Academic Search Complete (EBSCO Host), ACM Digital Library, Computer Source (EBSCO Host), Criminal Justice Database (ProQuest), Criminal Justice Abstracts (EBSCO Host), Embase (Elsevier), JSTOR, Science Direct (Elsevier), Social Science Database (ProQuest), IEEE Xplore (IEEE), Web of Science (Clarivate).
2. **Gray Literature;** GovInfo (govinfo.gov), Center for Internet Security (https://www.cisecurity.org/), I3P Consortium Members Libraries (https://www.thei3p.org/), Homeland Security Digital Library at NPS

(https://www.cisa.gov/resources-tools/resources/homeland-security-digital-library), Analysis & Policy Observer--Cyber Security (https://apo.org.au/subject/51721), Analysis and Policy Observer—Technology (https://apo.org.au/subject/21582), ACM Digital—proceedings (https://dl.acm.org/proceedings), Dans Easy Archive (https://dans.knaw.nl/en/data-services/easy/), Google Scholar (https://scholar.google.com/).

### *2.3.4. Search Strategy*

This review's database search strategy utilizes natural language rather than controlled vocabulary terms, employing Boolean logic across two domains: (1) Online and (2) Defacement. The decision to refrain from controlled vocabulary was made to mitigate the retrieval of irrelevant studies, a problem encountered during preliminary tests of the search strategy on a limited number of databases. These tests revealed that using controlled vocabulary terms yielded hundreds of results unrelated to website defacement, such as malware attacks or hacking of banking credentials. Given that the terminology used to describe website defacement remains consistent throughout research on this type of hacking, the natural language search terms effectively identify relevant research articles. However, a set of controlled vocabulary terms is included to showcase prior work conducted. The specific terms and logic are outlined in Figure 2.1 below.

Specifically, the exact Boolean search string used for every database was: web* AND deface*. This search string utilizes wildcards to capture any derivatives of terms related to website defacement. The search was restricted to searching among titles, abstracts, and subjects/keywords. Searches of full text were not conducted as they increased the number of irrelevant articles to an unmanageable degree without increasing the number of relevant articles.

Additionally, the search did not allow the use of equivalent terms and did not restrict articles to those with linked full-text articles.

**Figure 2.1. Query Terms**

| Domain | Natural Language | Controlled Vocab |
|---|---|---|
| Online | web* | Cyberspace, digital, web, website, webpage, |
| Defacement | deface* | Computer crimes, defacers, web sites, defacement, website defacement, website attacks, web attacks, defaced, defaced web pages, Cyber-attacks, cyberattacks, malware, system trespass, hacking, technology-driven crime, computer security, online offenders, computer crime, cybercrime, Computer focused crimes, cyberterrorism, cyber terrorism, cyber victimization, computer infection |

### *2.3.5. Selection of Sources of Evidence*

This study utilized a two-stage selection process for determining the eligibility of articles for inclusion. Following the bibliographic search, all returned articles were scrutinized by the first author. During this stage, the titles and abstracts of the retrieved studies were reviewed, and any study deemed potentially relevant was marked for further screening in the second stage. In the second stage, the first author reviewed the full text of all remaining sources identified from the initial screening. Subsequently, a second reviewer was allocated a 30% random sample to review independently. Any discrepancies between the reviewers were resolved through consultation with an independent third reviewer and through group discussion. This rigorous

process ensured the thorough examination and selection of eligible articles for inclusion in the review.

### *2.3.6. Data Extraction and Coding*

The extraction of data from the selected articles was conducted by the primary author by reading the entirety of each article and recording the relevant data into an organized excel sheet. The following data from the selected articles will be extracted and coded: (a) The name of the authors of the article, (b) The year of publication, (c) objective of the study, (d) publication type, (e) research design, (f) target population (ex. victims or offenders), (g) data source(s), (h) sample size, (i) measures, (j) units of analysis, (k) key findings or policy/practical implications.

This study categorized articles into three main themes. The first theme comprised articles focusing on studying the offender, the second theme included studies investigating the victims of defacement, and the final theme encompassed studies examining website defacement without data derived from offenders or victims. This thematic grouping facilitated the analysis and interpretation of the extracted results.

## 2.4. Results

### *2.4.1. Study Screening and Selection*

As shown in Table 2.1, 247 articles were retrieved as potentially eligible from the variety of academic and grey literature sources. 135 sources came from academic databases, while 12 came from grey literature sources. The first 100 hits from google scholar were selected to ensure robust article collection.

**Table 2.1. Search Results**

| Search Source | Number of Items |
|---|---|
| Academic Search Complete | 15 |
| ACM Digital Library | 6 |
| Computer Source | 2 |
| Criminal Justice Abstracts | 8 |

**Table 2.1. Search Results (continued)**

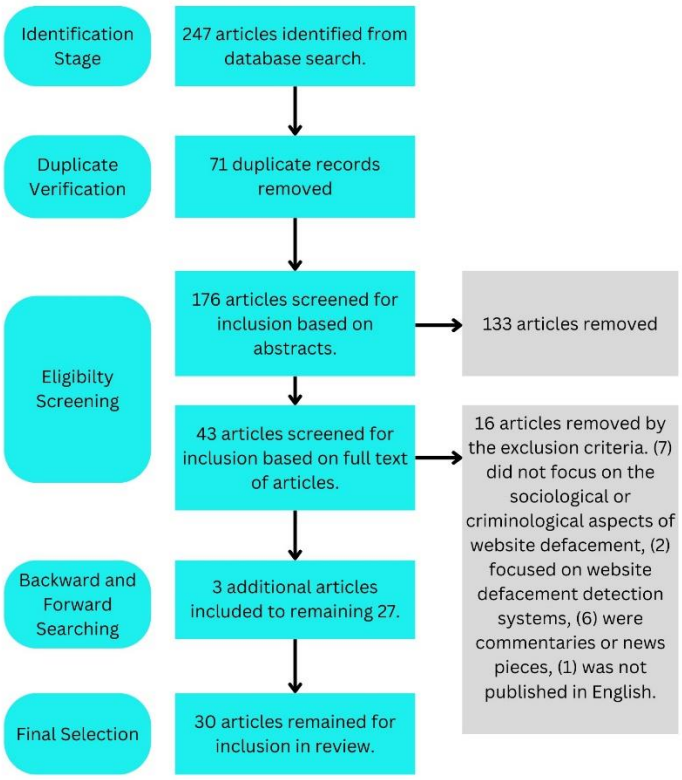
| | |
|---|---|
| Criminal Justice Database | 14 |
| Embase | 2 |
| IEEE Xplore | 40 |
| JSTOR | 11 |
| ScienceDirect | 13 |
| Social Science Database | 3 |
| Web of Science | 21 |
| ACM Digital Proceedings | 5 |
| Homeland Security Digital Library at NPS | 7 |
| Google Scholar | 100 |
| Total | 247 |

### *2.4.2. Selection of Sources of Evidence*

The results of the selection process are presented below as a flowchart in Figure 2.2. In the initial identification stage, our search strings returned 247 results. However, 71 of these records were duplicates, which once removed resulted in a total of 176 articles. After reviewing the title and abstract to determine if the articles could meet the inclusion criteria, 133 articles were eliminated, resulting in 43 articles to undergo full-text screening. In this stage all articles were reviewed under the inclusion criteria by the first author while a near 30% random sample (n=12) were dual screened. After this screening we reached 85% agreement with two articles in dispute, after the examination of the articles in question by a third independent reviewer we reached 100% agreement. After the second screening we removed 16 articles and were left with 27 articles. The reasons for exclusion are as follows: seven did not focus on the sociological or criminological aspects of website defacement, two focused on website defacement detection systems, six were commentaries or news pieces, and one was not published in English, but Korean. After conducting a thorough examination of references both forwards and backwards, three additional articles were deemed relevant and included, bringing the final total of sources

for the review to 30. With the exception of one study, all sources were readily accessible. For the one inaccessible source, direct contact was made with the author, who provided the full text of the study. Comprehensive summaries of each included study are provided at the study-level in the appendix, offering a detailed overview of the key findings, data sources, and insights gleaned from each source.

**Figure 2.2. Flow Chart**




### *2.4.3. Characteristics of Sources of Evidence*

Table 2.2 presents the characteristics of all studies included in our review. Firstly, all the studies were published between the years 2004 and 2023, with the majority of the literature being published after 2016. Secondly, quantitative methods dominate the included articles, with only a quarter employing any form of qualitative analysis. Thirdly, nearly half of the articles relied on

data from the available-for-purchase Zone-H self-report data. Much of the remaining data was obtained by scraping reporting websites like Zone-H and others and supplementing this data (which does not contain self-reported attack motivation or attack methods) with information from other sources.

**Table 2.2. General Characteristics of Included Studies (N=30)**

| Characteristic | Count | Percentage (%) |
|---|---|---|
| Publication Year | | |
| < 2010 | 4 | 13% |
| 2010-2015 | 2 | 7 |
| 2016-2020 | 15 | 50% |
| >2020 | 9 | 30% |
| Publication Type | | |
| Conference proceeding | 7 | 23% |
| Journal article | 21 | 70% |
| Other | 2 | 7% |
| Analytic Approach | | |
| Qualitative | 3 | 10% |
| Quantitative | 22 | 73% |
| Mixed methods | 5 | 17% |
| Data Source | | |
| Zone-H self-report | 14 | 46% |
| Other defacement sources | 12 | 40% |
| Other | 4 | 13% |

## 2.5. Results of Individual Sources of Evidence

For detailed information on each included source of evidence and the relevant data that was charted, please refer to the table provided in the appendix. This table offers a comprehensive overview of the characteristics of each study included in our review, including publication year, research methods, data sources, and key findings.

## 2.6. Synthesis of Results

The synthesis of the results is presented as a thematic analysis, the goal of which is to display the dominant themes of the literature and the variety of ways that website defacement has been studied. It begins with an analysis of the literature through the lenses of applicable and

explicitly tested theory, and ends discussing the literature comprised of the research that seeks to bolster our understanding of website defacement without data explicitly derived from website defacers.

### *2.6.1. Routine Activities in Website Defacement*

In all, there were 15 studies that explicitly or implicitly examined website defacement through the lens of Routine Activities Theory. Of these 15 studies, 11 focused on exploring the motivations and offending behavior of the defacers. Additionally, five studies examined aspects of what defacers consider suitable targets, while only two studies delved into the concept of capable guardianship. As you may have noticed, this math "doesn't add up." This is due to the interconnected nature of the various aspects of Routine Activities Theory, which are rarely discussed in isolation from each other, within the literature. In many cases, the suitability of a target is closely linked to the motivations of offenders. As a result, to enhance the clarity of themes and provide a more cohesive narrative, conclusions regarding specific aspects of the theory have been separated to discuss them alongside other related findings. This approach facilitates a better understanding of the nuances and interrelations within the literature.

**Motivated Offenders.** Individuals listed in the Zone-H archive, having successfully committed website defacements, can be regarded as motivated offenders given their prior criminal activity in this domain. Table 2.3 presents the 11 articles that investigate website defacement by analyzing the offending behavior and motivations of website defacers documented in Zone-H records and expressed within the content of their defacements. In general, the motivations of defacers vary greatly, with most driven by entertainment/thrill-seeking, a desire to establish a reputation as skilled hackers, or to support ideological causes. Importantly, the offending behaviors of defacers vary based on the motivation of the defacer with

common themes amongst defacers with similar motivations. For instance, early studies like Woo et al. (2004) found that approximately 70% of website defacements could be classified as pranking behavior, while the rest exhibited ideological motives. Subsequent research by Das et al. (2017) also found that most defacements are performed for entertainment reasons, though at a lower total percentage of just over 50%. Similarly, research by Maggi et al. (2017) found that defacer motivations range from supporting their personal reputation, to promoting a certain ideology, or their religious or political orientation. Interestingly, these motivations are also reflected in defacers' discussions on social media platforms (Aslan et al., 2021). However, while more recent studies corroborated the diversity in motivations, they found that the proportion of ideologically motivated defacers changes by year but is closer to 10%, rather than 30% (Bannerjee et al., 2021; Burruss et al., 2021; Romagna & van den Hout, 2017).

The majority of research has sought to understand how defacers differ in their offending, such as their modus operandi, based largely on their motivation. For example, hackers who were motivated by overcoming challenges, political reasons, or by revenge were less likely to use known vulnerabilities in their defacements than their hacking for fun counterparts (Holt et al., 2020b). Additionally, this study found that SQL injections were significantly more often used to compromise websites when the attacker was motivated by fun or to be the best defacer (Holt et al., 2020b). While generally there is variation in attack methods between ideological defacers and their counterparts, there is also some conflicting evidence. Another study by Holt and colleagues, that supports their previously discussed paper, found that ideological defacers were more likely to use unknown vulnerabilities to complete attacks compared to defacers with any other motivation (Holt et al., 2020a). However, another study indicated that ideological defacers, despite their capability to create cyber tools and exploit unknown vulnerabilities, often resort to

using known and relatively unsophisticated techniques to deface websites (Romagna & van den Hout, 2017).

While constituting a smaller portion of the overall defacer population, ideologically motivated defacers receive considerable attention in the literature. Despite ideological defacers displaying a large variety of ideological and psychological motivations (right-wing, left-wing, Islamic, nationalistic, etc.) these defacers have interesting similarities with defacers whose ideology differs greatly and whom they have much in common (Maggi et al., 2017). For instance, while sociopolitical motivations are the primary driver for ideological hackers, other factors such as thrill-seeking and self-esteem play secondary roles in their motivations for defacing (Romagna & van den Hout, 2017). However, ideological defacers with similar beliefs tend to exhibit similar defacing characteristics. Interviews with a small sample of ideologically motivated Turkish hackers revealed that their target selection was directly influenced by their religious or political beliefs, and they were often prompted to attack websites by events conflicting with their beliefs or offending them (Holt, 2009; Holt et al., 2017a). In general, ideological defacers are often reactively motivated by real-world global and regional political events, leading to the creation of defacement campaigns varying in length and intensity (Balduzzi et al., 2018; Maggi et al., 2017). Similarly, studies have also found evidence that ideologically motivated defacers are more purposive in their target selection and chose targets intentionally to draw the most attention to their cause (Holt et al., 2020a; Romagna & van den Hout, 2017). This aspect of ideologically motivated defacers will be discussed in more detail in the following section on target suitability.

However, a significant drawback of this literature is highlighted by research conducted by Bannerjee et al. in 2021. This research revealed a notable discrepancy between the motivation

variables utilized by the majority of papers, primarily sourced from Zone-H self-report data, and the motivations expressed in the content of website defacements. They found that the motivations reported in the Zone-H data consistently differed from those expressed within the defacement content. In fact, nearly 52% of the time, the self-reported motivation for the defacement in the Zone-H data deviated from the motivation expressed within the defacement itself (Banerjee et al., 2021). This finding is further supported by other research that found similar inconsistencies, as well as by the administrators of the Zone-H website (Romagna & van den Hout, 2017). This finding underscores the need for caution when relying solely on self-report data and highlights the importance of considering alternative sources or methodologies to better understand the motivations behind website defacement. As scoping reviews aim to identify areas of concern and gaps in the literature, it is notable that six out of the 10 other articles in this section, and 46% of all the included studies, rely on self-report data from Zone-H. This reliance underscores the importance of further research to understand the disparities between motivations provided to Zone-H when reporting a defacement and those expressed within the content of the defacement image they leave behind. Addressing this discrepancy is crucial for ensuring the accuracy and validity of research findings in this field.

**Table 2.3. Offenders, RAT: Motivation**

| Author/s | Year | Key Findings |
|---|---|---|
| Aslan et al | 2020 | Three topical themes are clearly visible in defacers' discussions: political grievances, discussions specific to certain countries, and technical discussions. |
| Banerjee et al | 2021 | Images used in website defacements often don't match the reported motives behind the attacks. Nearly 52% of the time, the self-reported motivation for the defacement in the Zone-H data deviates from motivation expressed within a defacement.<br>Only a small portion of attackers are motivated by expressive reasons, like seeking revenge or making a political statement. |

**Table 2.3. Offenders, RAT: Motivation (continued)**

| Author/s | Year | Key Findings |
|---|---|---|
| Thomas J. Holt | 2009 | Ideological hackers often collaborate to deface websites.<br>Hackers typically acquire computer system knowledge through personal experience and peer mentoring.<br>The features of ideological hackers' targets vary greatly.<br>Turkish ideological hackers unite around a common objective they refer to as "the mission," which is strongly influenced by Islam. |
| Holt et al | 2020. a | Ideologically motivated defacers deliberately select their targets to draw attention to their cause.<br>Ideological defacers are more inclined to utilize unknown vulnerabilities in their attacks compared to defacers with other motivations. |
| Holt et al | 2020. b | Those who defaced websites for personal achievement, as a challenge, political reasons, or unknown motivations were notably less inclined to exploit known vulnerabilities compared to those who hack for entertainment.<br>SQL injections were significantly more frequently employed by defacers who hacked for enjoyment or aimed to be recognized as the best in their field. |
| Maggi et al | 2018 | Around 53% of defacers operate individually, without identifying themselves as part of a team. The rest belong to one or more groups. A large majority (80%) stick with the same affiliation(s) throughout their "career," while only 20% switch from one group to another.<br>Defacement campaigns vary in their longevity and intensity.<br>Attackers compromise and deface websites for diverse reasons, ranging from enhancing their personal reputation to, notably, advocating for a particular ideology, religion, or political stance. |
| Romagna & van den Hout | 2017 | Hacktivist website defacers are driven by various ideological and psychological factors for their actions. While socio-political motivations may seem most significant, other triggers like seeking thrills and boosting self-esteem also contribute to their behavior.<br>These defacers often exploit known and relatively simple vulnerabilities and techniques. They utilize publicly available tools but are also capable of developing their own.<br>Their choice of targets appears to be influenced by how easy they are to hack and/or the level of attention the defacement is likely to garner. |
| Woo et al | 2004 | Roughly 70% of website defacements can be categorized as pranks, while the remaining incidents are driven by political motives.<br>Contrary to the portrayal of hackers as isolated individuals, they are actually part of large social networks. They often leave calling cards, greetings, and taunts on web pages to showcase their motivations for hacking. |

**Table 2.3. Offenders, RAT: Motivation (continued)**

| Author/s | Year | Key Findings |
|---|---|---|
| Balduzzi et al | 2018 | Defacement campaigns by ideological hackers are often triggered by real-world events, as these hackers tend to react to current events. These events typically revolve around geopolitics and regional politics, serving as catalysts for defacement activities.<br>Defacers often organize themselves into hacking teams to carry out their activities effectively. |
| Das et al | 2017 | The primary motivation behind website defacement is often personal entertainment.<br>In December 2012, file inclusion emerged as the most commonly used attack strategy. |
| Holt et al | 2017. a | Turkish hackers driven by ideological agendas often align with the broader values of the hacker subculture. However, their targets for attacks are typically influenced by religious or political beliefs.<br>Regardless of their motivation, hackers typically acquire knowledge about computer systems through personal experience and peer mentoring. |

**Suitable Targets.** While some articles in the section above mention aspects of a suitable target (Holt et al., 2020a; Maggi et al., 2017; Romagna & van den Hout, 2017), five additional studies, described in Table 2.4, specifically focused on target suitability variables. It is important to note that this scoping review aims to differentiate aggregate statistics or features of victimization rates from studies that seek to understand more about the behaviors and practices of victims of website defacement. Thus, studies that described the behaviors of targets of website defacement were discussed separately from studies discussing which targets were more likely to be victimized. However, even in descriptive statistics, there is disagreement in the literature on this topic. For instance, a study in 2017 revealed that 36.8% of defacements targeted US-based websites, which is about 11 times higher than the average rate of defacement for other countries (Das et al., 2017). This is likely due to the US's significant control over web hosting, with 40% of servers and hosting 43% of the world's top million websites (SolarWinds, 2012; W3Techs, 2024). Conversely, two years later, another study found that Asian nations were nearly six times

more likely to experience an increase in the count of website defacements than other nations, attributing this effect to likely country-specific hacker rivalries in the region (Howell et al., 2019). This study also found that Muslim-majority countries were nearly three times less likely to experience defacements than non-Muslim-majority nations (Howell et al., 2019). Thus, while the location of a website is often a measure of target suitability, the disagreement in the literature regarding the distribution of defacements among different countries suggests variations in the perceived suitability of targets for website defacers, which highlights the importance of understanding the factors that influence defacers' target selection processes (Howell et al., 2019).

Furthermore, the study by Howell and colleagues also examined non-demographic aspects of a country that make its websites suitable targets for defacers. Interestingly, they found that political defacement frequency was not influenced by a country's socioeconomic or internet infrastructure characteristics (Howell et al., 2019). Furthermore, they discovered that the political motivation of defacers serves as a proxy for target suitability, as these defacers are driven by their perception of a target's value and are not deterred by other factors, unlike recreational defacers who are more opportunistic in their target selection (Howell et al., 2019). In further pursuit of understanding suitable targets, Holt et al. (2022) sought to learn more about the targeting practices of website defacers who were "Jihadi inspired." By subsetting the Zone-H self-report data to only include defacers whose alias included "Jihadi terminology," "ties to the Jihadist movement," or mirrored the names of known Jihadist groups, they found that contrary to what is generally regarded as a suitable target for terrorists in the real world, Jihadi defacers were not significantly more likely to deface military, educational, or government websites. Rather, websites ending in .org were the only suitability factor found to be associated with these actors' preferences (Holt et al., 2022).

Interestingly, only two studies have examined whether and when the targets of website defacement react to website defacement. These studies revealed shockingly low response times, with 43 percent of defacements remaining unresolved after one week, and over 37 percent still in place after two weeks (Bartoli et al., 2009). Moreover, less than a quarter of the defaced websites were restored within 24 hours (Bartoli et al., 2009). Interestingly, the severity or scale of a defacement also influenced the speed of restoration, with mass defacements being resolved more quickly than single defacements (Bartoli et al., 2009). Additionally, websites with higher PageRank, or top-level domains, exhibited faster reaction times to restore their websites post-defacement. Supporting these findings, Das et al. (2017) observed that approximately four years after the initial defacement, 57% of websites remained defaced and inoperable.

While there is a pressing need to study and understand the preferred targets of defacers, particularly among different groups of defacers, the current and future findings could significantly contribute to the enhancement of cyber defenses. However, it is noteworthy that the final aspect of the Routine Activities Theory has received the least examination in the defacement literature.

**Table 2.4. Offenders, RAT Suitable Targets**

| Author/s | Year | Key Findings |
|---|---|---|
| Bartoli et al | 2009 | In our sample, about 43% of the defacements lasted for at least one week, with over 37% still in place after two weeks. However, less than 25% of the sample managed to restore the site within the first 24 hours.<br>The response time to mass defacements is typically faster compared to single defacements.<br>Pages with a higher PageRank value tend to have a quicker reaction time to defacements. |
| Das et al | 2017 | Websites hosted in the United States were defaced at a rate 11 times higher than the average defacement rate per country, making up 36.8% of the sample. Approximately four years after being defaced, around 57% of the websites were still not operational. |

**Table 2.4. Offenders, RAT Suitable Targets (continued)**

| Author/s | Year | Key Findings |
|---|---|---|
| Holt et al | 2022 | Jihadi cyberattacks were rare during the five-year period analyzed, accounting for only 1% of all attacks in the dataset (24,561 out of 2.2 million) being attributed to a jihadi-affiliated name or handle.<br>The only significant factor associated with jihadi attacks was that the targeted website was affiliated with an organization. Surprisingly, military, government, and educational institutions were not significant targets for jihadists in cyberspace, unlike in physical attacks.<br>Jihadist defacers were more inclined to target organizational websites and employed specific attack methods compared to other defacers.<br>They were also more likely to utilize both known and unknown vulnerabilities for their attacks, while showing significantly less reliance on SQL attacks, unlike other defacer motivations. |
| Holt et al | 2020. b | Homepages of websites were notably less impacted by defacements from attackers who hack for entertainment. However, they were more frequently targeted by attackers driven by challenges, political motives, and revenge.<br>The results offer partial confirmation for the principles of visibility, inertia, and accessibility within routine activity theory, which help explain attacker motivations and target suitability. It is evident that motivation significantly influences which targets are deemed suitable for attack. |
| Howell et al | 2019 | The frequency of political defacements doesn't seem to be influenced by a country's socioeconomic characteristics or internet infrastructure.<br>Political motivation can serve as a proxy for target suitability. Unlike opportunistic attacks, political ones are specific and may stem from ideological defacers' assessment of a target's significance, disregarding other elements of target suitability. Non-ideological defacers, on the other hand, tend to be more opportunistic and will target any vulnerable site.<br>Asian nations are nearly six times more likely to see an increase in website defacements of top-level domains compared to non-Asian nations. This is likely due to country-specific hacker rivalries prevalent in Asia.<br>Muslim-majority countries are nearly three times less likely to experience defacements of top-level domains compared to non-Muslim majority nations. |

**Capable Guardian.** As mentioned, Table 2.5 presents the details of the two papers to discuss the role of capable guardianship in the website defacement literature. Unlike the aspect of suitable targets, which was often examined in concert with motivated offenders, it appears that capable guardianship, while hotly contested in other forms of cybercrime research, has been largely unstudied in the context of website defacement. Howell and colleagues' (2019) research

studied the impact of capable guardianship to deter website defacements against top-level domains, which Zone-H classifies as Special Defacements, often government, educational, and high-profile company websites. They found that while capable guardianship, operationalized as a strong military and CERT (Computer Emergency Response Team) presence in a country, deters recreational defacers, it does not deter hackers who are ideologically motivated (Howell et al., 2019). The second study analyzed the impact of security on defacement on Iranian websites by comparing defacements between two time periods (2000-2001 and 2005-2007). The researchers found that while Iranian websites, especially government websites, have improved their security systems, many other Iranian websites are still using weak security systems (Shirali-Shahreza & Shirali-Shahreza, 2009). Furthermore, they identified that failure to use updated operating systems and a lack of firewalls were the key reasons behind these compromises (Shirali-Shahreza & Shirali-Shahreza, 2009). However, the lack of transparency regarding the data sources and methodologies used in this study raises concerns about the validity and reliability of its findings. Without clear documentation of how the data was sourced and analyzed, it becomes difficult to assess the rigor of the research and the extent to which its conclusions can be generalized. As demonstrated by the lack of research, there is a clear need for more studies that examine features of guardianship and the perception of its presence among website defacers.

**Table 2.5. Offenders, RAT Capable Guardian**

| Author/s | Year | Key Findings |
|---|---|---|
| Howell et al | 2019 | The overall frequency of website defacements is deterred by capable guardianship, such as having a strong military presence. Additionally, it is influenced by several measures of target suitability.<br>Capable guardianship deters recreational defacers, but not those who are politically motivated. |

**Table 2.5. Offenders, RAT Capable Guardian (continued)**

| Author/s | Year | Key Findings |
|---|---|---|
| Shirali-Shahreza & Shirali-Shahreza | 2009 | Iranian websites commonly exhibit low security measures, with many lacking firewalls. Additionally, they often rely on weak operating systems, such as outdated versions of Windows.<br>Although there has been an improvement in the security systems of Iranian government websites in recent years, other Iranian websites still maintain inadequate security measures. |

### *2.6.2. Life-Course Criminology*

Moving away from the Routine Activities Theory, five studies have contributed to improving our understanding of defacers' behaviors over time and have shed light on the life-course and change in the criminal careers of these hackers, even if only some of the studies use this theoretical language. These studies are displayed in Table 2.6. The earliest of these studies aimed to learn more about the variety-seeking behavior of hackers as their careers progressed. Ooi (2012) found that as the time between hacks increases, defacers are more likely to choose different targets and attack strategies. This study also revealed that defacers tend to prefer seeking variety in general, launching more attacks using new methods against targets in different regions or with differing operating systems (Ooi, 2012). Building on this research, others sought to observe differences in the careers of website defacers. Burruss et al. (2021) identified two distinct groups of website defacers based on attack frequency: a larger low-frequency group and a smaller high-frequency group. Furthermore, this study found that a defacer's use of Twitter (now X) and political messaging in their defacements made them more likely to be part of the high-volume group, while use of YouTube or animation in defacement content led to a greater likelihood of belonging to the low-frequency group (Burruss et al., 2021). Subsequent research utilizing group-based trajectory modeling found that six distinct groups of defacers exist based on their hacking frequency over the entirety of their career (van de Weijer et al., 2021). These

groups were identified as: low sporadic, high sporadic, low declining, high declining, low chronic, and high chronic (van de Weijer et al., 2021). However, the models were unable to predict the characteristics of defacers that made them more likely to belong to a specific group. Additionally, this research found that a small population of defacers accounted for the majority of defacements against websites (van de Weijer et al., 2021).

Somewhat differently, studies have significantly contributed to our understanding of the short-term impacts on defacers' careers. Maimon and colleagues distributed gossip related to law enforcement activities in cyberspace to the inboxes of defacers active on Facebook. They found that this intervention resulted in a reduction in the proportion of hackers who reoffend, the frequency at which they reoffend, and the severity of attacks they generate one week and one month after the intervention (Maimon et al., 2021). However, posting these messages to the Facebook profiles of these defacers, where others could see, was ineffective at deterring attacks (Maimon et al., 2021). Finally, Aslan and colleagues utilized social media to understand the sentiments found in the postings of defacers on Twitter (now X). They found that these sentiments both preceded and followed successful defacements. Thus, for some defacers, monitoring their social media could serve as an early warning system for potential web defacement attacks (Aslan et al., 2020). While these particular studies may not fit easily within the traditional framework of life-course theory, they nonetheless offer valuable insights into the changes within the careers of website defacers. These insights complement and bolster the findings of studies examining specific trajectory groups, providing a more comprehensive understanding of cyber-offender behavior over time, and were discussed here for this very reason.

**Table 2.6. Life Course Studies**

| Author/s | Year | Key Findings |
|---|---|---|
| Aslan et al | 2020 | Sentiments expressed in Twitter postings often precede and follow successful attacks for many defacers, constituting approximately 24% of the sample. However, for most defacers, this correlation wasn't observed due to insufficient data. This indicates the potential for early warning or even pre-attack alerts based on Twitter sentiment analysis. |
| Burruss et al | 2021 | There are two distinct groups of website defacers: low-volume defacers, comprising 69%, and high-volume defacers, comprising 31%.<br>Social media seems to be linked with website defacement. Twitter has a positive impact, particularly for the high-volume defacer group, while YouTube has a negative impact.<br>Hackers utilizing political content and music were associated with an increase in counts of website defacements, whereas the use of animation was associated with a decrease. |
| Maimon et al | 2021 | Sending gossip related to law enforcement agencies' activities in cyberspace directly to hackers' Facebook inboxes led to a decrease in the proportion of hackers who reoffend, as well as in the frequency and severity of their attacks one week and one month after receiving the intervention.<br>However, posting this gossip to their personal pages, where others could see the message, did not effectively deter attacks. |
| Kok Wei Ooi | 2012 | Hackers exhibit a propensity to seek variety when selecting their victims, considering factors such as region, hacking method, and types of operating systems.<br>Defacers, in particular, tend to initiate more attacks using novel hacking methods or target regions or operating systems that they haven't previously targeted.<br>Furthermore, defacers are more inclined to seek variety in their attacks as the time interval between the previous and current attack increases. |
| van de Weijer et al | 2021 | Various trajectory groups of defacers have been identified, totaling six: low sporadic, high sporadic, low declining, high declining, low chronic, and high chronic.<br>However, despite these distinct groups, predicting membership within them proved challenging.<br>Interestingly, a small portion of defacers constituted the majority of defacements against websites, underscoring the significance of a relatively small population in terms of the frequency and impact of attacks. |

### *2.6.3. Social Learning Theory*

While other research on website defacement acknowledges the tendency of defacers to join teams based on ideology and other similarities, this aspect is often not the primary focus of

investigation (Balduzzi et al, 2018; Holt, 2009; Holt et al., 2017; Maggi et al., 2017; Woo et al., 2004). For instance, Maggi et al. (2017) in their exploration of defacement campaigns found that 53% of the defacers were “lone wolves” and never joined a team, while the remaining defacers belonged to one or more. Furthermore, they found that most defacers (80%) are loyal to their team throughout their defacing career, whereas 20% of defacers migrate from one group to another. Furthermore, even ideologically motivated defacers formed teams as it was found that these defacers joined together to deface websites and that many learned how to do so through peer mentoring (Holt, 2009; Holt et al.,2017). However, as mentioned, these aspects were not the primary findings or research objectives of their studies. In fact, only two studies explicitly sought to understand how the team membership of defacers changes and impacts their careers as hackers. These studies are displayed in Table 2.7.

Directly seeking to learn more about how defacers form, leave, and join teams Perkins et al. (2023) employed the use of social network analysis on population data of a defacing forum known as Zone-Xsec. This forum notably provides defacers with the ability to provide not only their personal alias but also their team affiliation. Perkins et al. found that the social ecosystem of defacers is widely connected but centralized around several hacker groups. Furthermore, while they found that defacers maintain intragroup cohesion, they have weak and transitory intergroup connectivity. This was further shown when examining the change over time of these social bonds which revealed highly fragmented and sporadic connections between defacers (Perkins et al., 2023). In a different approach, Maimon et al, directly drawing on social learning theory, sought to understand how the social connectedness of defacers influenced their attack frequency, based on the assumption that defacers with greater connectivity to defacers learn more from others and better defacers themselves. Ultimately, Maimon et al.’s original assumptions were confirmed as

they found that defacers use of social media platforms like Twitter (now X) and Facebook significantly increased the frequency at which those defacers' defaced websites compared to those without social media engagement.

**Table 2.7. Social Learning Theory Studies**

| Author/s | Year | Key Findings |
|---|---|---|
| Maimon et al | 2017 | The utilization of social media platforms, particularly Twitter and Facebook, by defacers significantly amplifies the frequency of web defacement attacks they initiate. |
| Perkins et al | 2023 | Defacers operate within a well-connected ecosystem that revolves around several hacker groups.<br>Within these groups, defacers demonstrate strong cohesion among members but exhibit weak and transient connections between different groups.<br>Taking a longitudinal perspective, it becomes evident that the connections between defacers are highly fragmented and sporadic over time. |

### *2.6.4. Other*

The remaining articles take either a purely descriptive or unique approach to studying website defacement. While their findings do not easily fit within the narrative of the other articles, their findings are still important for our understanding of website defacement. They are displayed in Table 2.8.

The earliest of these papers were produced by Han and various colleagues in 2016 and 2019, with the latter building upon the former. In these studies, Han focused on the content of defaced webpages and found that machine learning algorithms were able to consistently narrow the potential suspects of a defacement to a few potential defacers (Han et al., 2016, 2019). This is because the content of a hacker's defacement acts almost like a digital thumbprint, even if the images change over time (Han et al., 2016, 2019). Such information can be useful for attributing defacements that are not claimed by defacers and posted to Zone-H or other forums.

Another study by Zayid and colleagues also utilized machine learning models to delve into the characteristics of defacements. While the models could not predict future defacements, their models were able to make accurate predictions of the missing features of motivation and hacking method in 99% of cases when given the other descriptive features of the data (Zayid et al., 2023). Furthermore, they identified SQL injection as the most common attack strategy used by defacers and estimated that only 0.00249% of defacements in their sample were from Islamic-far-extremists or Jihadist defacers. (Zayid et al., 2023).

Lastly, Moneva and colleagues (2022) studied revictimization of websites from the perspective of attackers. They discovered that repeat victimization is also observed in cyber places, particularly in websites. They revealed that cases of repeat victimization were found to be committed disproportionately by prolific offenders (Moneva et al., 2020). Furthermore, they found that offenders rarely defaced the same domains they had previously targeted, with a defacer returning to deface the same website in only 0.3% of cases (Moneva et al., 2022).

**Table 2.8. Other Studies**

| Author/s | Year | Key Findings |
|---|---|---|
| Han et al | 2016 | The contents of a defacer's image, even when they change, often contain enough unique features to identify who defaced certain pages. Therefore, defacement content can be likened to a digital thumbprint, enabling identification of the perpetrator. |
| Han et al | 2019 | Hacker profiling through cluster analysis serves as a fundamental and crucial step in cybercrime investigations for attribution.<br>However, the similarities among defacements tend to evolve over time, making it more challenging to pinpoint a likely defacer, especially when considering a larger number of past defacements.<br>Nevertheless, the Case-Based Reasoning (CBR) system remains effective in significantly narrowing down potential offenders, even when analyzing data over an extended period. |

**Table 2.8. Other Studies (continued)**

| | | |
|---|---|---|
| Moneva et al | 2020 | Repeat defacements are predominantly committed by prolific offenders who engage in a disproportionate number of attacks. Interestingly, offenders rarely target the same domains they have previously defaced, with such occurrences only accounting for 0.3% of the time. This indicates a low rate of revisiting previously targeted domains.<br>The phenomenon of repeat victimization is also observed in defaced cyber places, such as websites, highlighting the tendency for certain locations to be targeted repeatedly. |
| Zayid et al Pre-print / not peer reviewed | 2023 | After model training, it is possible to make highly accurate predictions regarding the target reason or hack mode with 99% certainty, even with a relatively small dataset. It is important to note that this machine learning model predicts the value of missing features based on other features of defacement and does not forecast future defacements.<br>SQL injection stands out as the most prevalent attack strategy among defacements.<br>Interestingly, there is a notable absence of Islamic-far-extremist and jihadist defacement and hacktivism, indicating a very weak extremist contribution in terms of defacement, with an occurrence rate as low as 0.00249%. |

### *2.6.5. Other Methodology*

In this section, four papers, that aimed to enhance our understanding of website defacement, albeit not by directly studying defacers, are presented. The results are displayed in Table 2.9. The first study, conducted by Aggarwal and colleagues, utilized reinforcement learning modules alongside Nash equilibrium metrics to simulate the interactions between hackers and site administrators across numerous iterations, with variations in how the model learned from past decisions and outcomes. Their findings suggested that website defenders exhibited higher success rates in defending websites, regardless of their level of attention to recent outcomes. This could be attributed to attackers' unfamiliarity with the network and what vulnerabilities might compromise the website (Aggarwal et al., 2015). However, unlike

defenders, hackers who paid closer attention to recent outcomes tended to be more successful in their exploits compared to those who were less aware (Aggarwal et al., 2015).

The remaining three studies utilized surveys of college students to make inferences on the decision-making of hackers to deface websites. The first of these studies, conducted by Holt and colleagues in 2017, examined behavioral and attitudinal correlates of willingness to engage in website defacements using a sample of over 1000 college students from the US and Taiwan. They discovered that individuals' political attitudes toward marginalized groups and their support for cybercrime were associated with increased willingness to engage in website defacement (Holt et al., 2017b). Furthermore, they found that a significant political factor contributing to the willingness to deface a website was the number of attacks an individual was willing to perform in the real world (Holt et al., 2017). Findings that demonstrate support for violent political action bridging the digital divide. Adam Bossler conducted two similar studies in 2019 and 2021, utilizing the results of a survey of around 700 college students, to examine techniques of neutralization and responses to perceived sanctions. Bossler found that students were not deterred from their willingness to engage in cause-based cyber-attacks by anticipated formal sanctions but were deterred by perceived informal sanctions (Bossler, 2019). Additionally, Bossler concluded that ideologically driven hackers would likely be more challenging to deter than economically focused hackers through the use of formal sanctions due to their dedication and belief in their righteous hacking mission (Bossler, 2019). In his later study, Bossler observed that while the majority of participants would not commit any cyber-attacks, respondents' willingness to engage in cyber actions against both domestic and foreign countries increased as their scores on the techniques of neutralization scale increased (Bossler, 2021). Moreover, he

found strongest support for "condemnation of the condemners" and "claim of entitlement" among the other techniques of neutralization.

While these studies offer interesting conclusions, the reliance on surveys of college students to understand the behaviors and motivations of website defacers raises valid concerns regarding the generalizability of the findings. While these survey-based papers contain nearly identical messages critiquing those who believe that surveying college students leads to limited generalizability of findings, the question remains, why study college students when there is ample opportunity to study defacers directly. While surveys of college students are commonly used in research, particularly in psychology, it is difficult to believe that the motivations and thought processes of undergraduate students mirror those of actual hackers, especially ideological hackers in regions like the Middle East or Indian sub-continent.

Knowing defacers' desire for attention and apparent willingness to share their motivation for hacking, rather than asking others as a proxy for these hackers, why were defacers not surveyed? Indeed, some studies have conducted interviews or engaged with defacers on a smaller scale, but larger-scale direct engagement with defacers could provide more comprehensive and accurate insights into their motivations and behaviors. Perhaps the results of these studies are generalizable to defacers at large, but until research directly targeting defacers is conducted, the applicability of findings from surveys of college students to real defacers remains uncertain. Given these concerns, the results of these studies should be considered separately from those that study actual website defacers.

**Table 2.9. Other Methodology**

| Author | Year | Key Findings |
|---|---|---|
| Aggarwal et al | 2015 | The findings reveal that both attackers' and defenders' actions are influenced by the attention they pay to their recent outcomes. Specifically, if an attacker pays more attention to recent outcomes, they are more inclined to perform attack actions. |

**Table 2.9. Other Methodology (continued)**

| | | |
|---|---|---|
| Aggarwal et al (continued) | 2015 | However, paying more attention to recent outcomes does not seem to affect a defender's actions.<br>Interestingly, defenders appear to achieve higher success rates in defending websites regardless of how much attention they pay to recent outcomes.<br>Moreover, when hackers pay more attention to recent outcomes, they tend to be more successful compared to when they do not. |
| Adam M. Bossler | 2021 | Scoring higher on the techniques of neutralization scale significantly raised the likelihood of respondents being willing to engage in cyber actions against both domestic and foreign countries.<br>Among these techniques, the strongest support was found for the techniques of condemnation of the condemners and claim of entitlement.<br>The majority of college students in this sample indicated they would not commit any forms of cyber-attacks against either their home countries or a fictitious country. |
| Adam M. Bossler | 2019 | Anticipated formal sanctions, such as legal penalties, did not dissuade students from expressing willingness to engage in cause-based cyber-attacks. However, perceived informal sanctions, such as social disapproval or personal consequences, did have a deterrent effect.<br>Ideologically driven hackers may prove more difficult to deter compared to economically motivated hackers when faced with formal sanctions. This is because ideologically driven hackers are often deeply committed to their cause and strongly believe in the righteousness of their actions. |
| Holt et al | 2017. b | Political attitudes toward marginalized groups and support for cybercrime are key factors that increase individuals' willingness to participate in website defacement. Surprisingly, technological skill and involvement in cybercrime may not be as crucial as previously thought in predicting engagement in cyberattacks.<br>Another significant political factor observed across all models was the number of real-world attacks an individual was willing to carry out. This highlights that the inclination to resort to violence in support of political objectives transcends the digital realm, cutting across what's often referred to as the "digital divide." |

## 2.7. Discussion

### *2.7.1. Summary of Evidence and Conclusions*

The study of website defacers has evolved significantly over the years, from initial descriptive statistics to more sophisticated statistical models and theoretical frameworks. Despite

this progress, our understanding of website defacers is still limited, and the literature is still in its infancy. Therefore, scoping reviews serve as a valuable methodology for synthesizing current findings, identifying prevailing theories, and addressing knowledge gaps in our understanding of website defacers.

In this context, the present study aimed to uncover dominant theories in the literature and address potential gaps in our understanding of website defacers. Given the absence of previous systematic reviews in this area, this review represents a necessary step toward advancing the literature and enhancing our comprehension of these hackers. The analysis was structured to focus on two primary areas of investigation: offenders and their victims. However, due to the overwhelming focus on studying offenders in the literature, sub-themes were separately discussed within this section. Papers with conclusions spanning across sub-themes were discussed separately in the corresponding sections. Additionally, a distinct section was dedicated to discussing articles contributing to the literature that sourced their data from neither victims nor perpetrators of defacement, primarily through college student surveys, to avoid confusion given the logical differences between these articles and the remainder of the literature. This approach enabled a nuanced and comprehensive examination of the interconnected facets of website defacements, allowing for a thorough exploration of research findings.

This investigation has yielded several important observations from the included studies. Firstly, there is a significant skew in research focus towards the hackers involved in website defacement. While our understanding of the offenders has significantly improved over the years, in contrast, our knowledge of the victims remains limited. At present, our understanding of victims of website defacement appears to be confined to their possession of weakened security measures and their slow response following security breaches. Such limited insights into victims'

experiences would be considered inadequate, perhaps even laughable, in the context of victimology research in other areas of criminology. Therefore, future research efforts should prioritize understanding the victims of this crime. However, this emphasis on victim-focused research should not detract from continued studies of offenders. There is still much to learn about this group, and ongoing research into their motivations, behaviors, and tactics remains crucial for developing effective strategies to prevent and mitigate website defacement incidents.

Specifically, our review of the literature focused on the offender found that the conclusions of the literature where dominantly studied through the lens of Routine Activities Theory, with over half of the articles studying offenders to operationalize this theory. Because of this, the main strength of the literature is its rich contribution to our understandings of how different motivations impact the behavioral tendencies of website defacers. The literature has shown that website defacers are far from monolithic but instead possess a wide variety of sometimes overlapping motivations. These motivations influence not only the volume at which defacers successfully attack websites but also what hacking methods they use to gain unauthorized access to the website they attacked.

While researchers have extensively examined the motivated offender aspect of Routine Activities Theory, less attention has been given to examination of suitable targets and most notably the role of a capable guardian. Interestingly, what targets website defacers find suitable is largely dependent on the motivation of the attacker, with most defacers finding any vulnerable website suitable, while ideological defacers preferred to attack websites they viewed as adversarial to their beliefs. However, this review found only two studies that sought to understand the role of capable guardianship on the actions of website defacers, finding mixed

effects based on the motivation of the offender. Thus, it is crucial for future research to bolster our knowledge of how website defacers perceive and respond to a capable guardian.

Other perspectives, such as Social Learning Theory and the examination of defacers' criminal careers akin to Life-Course Criminology, have also started to gain traction. This research demonstrates that social relationships with other defacers increases the offending frequency of defacers, aligning with the core tenets of social learning theory. Additionally, it reveals that defacers form close social bonds and learning relationships in the form of hacking teams. Other research has shown that the career activity of defacers varies based on attack frequency, but has had limited success in concluding what characteristics of a defacer increases the likelihood of group membership. This presents an opportunity for further research to expand our knowledge base on defacers' social bonds and criminal trajectories.

However, this research also faces methodological challenges that need to be addressed. Firstly, there is an overreliance on self-reported data available for purchase from the Zone-H website, with nearly half of the included studies using this shared data source. Additionally, two studies and Zone-H themselves have shown evidence that this data may not accurately measure the motivations of website defacers, which raises concerns about the reliability of the literature focused on offender motivations. This is a troubling result for literature so focused on the motivations of these offenders. Secondly, the results of the literature are primarily descriptive, offering valuable information on the behaviors of different types of defacers but lacking in causal analysis. While further exploration of defacers' behaviors is necessary, there is also a pressing need to understand how defacers respond to different treatments. The limited research to this effect has been primarily qualitative. While qualitative research can provide useful findings from the experiences of defacers, the sample sizes for these studies have been extremely small. This

research has aided our understanding of how ideological defacers can become motivated to offend by current events; yet, future research should aim to increase sample sizes for interviews with defacers or adopt procedures similar to Maimon et al.'s (2021) study, which examined the effects of treatments on randomly selected groups of defacers.

Lastly, it is worth noting that a limited amount of research has attempted to use non-defacement data, such as data derived from college students, as a proxy to study active hackers. As discussed earlier, the validity and applicability of findings from such studies is likely questionable. Future research should prioritize studying defacers directly rather than relying on proxies for them, especially considering the ample opportunity to engage with actual offenders.

In summary, this review has offered a comprehensive overview of studies examining website defacement. Moving forward, future studies should continue the trend of utilizing more innovative methods and robust analytic strategies. Additionally, there is a need to expand theoretical frameworks and, perhaps most importantly, increase focus on understanding the experiences and impacts on the victims of website defacement. By addressing these areas, the field can advance our understanding of website defacement and contribute to more effective prevention and mitigation strategies.

### *2.7.2. Limitations*

While this scoping review provides valuable insights into the literature on website defacement, there are several limitations that should be acknowledged. Firstly, scoping reviews inherently have a broad focus, though this is necessary for investigating the available knowledge on a topic such as website defacement. However, we followed best practice guidelines outlined in the PRISMA-ScR framework (Tricco et al., 2018) to mitigate this limitation.

Secondly, in most cases scoping reviews are to have two reviewers screen all studies at all stages of the process. However, given the lack of availability for a full-time second reviewer dual screening and coding was only feasible for a random sample of studies to check for reliability. While there were some initial disagreements, eventually these were resolved to arrive at consensus. Any future reviews should consider utilizing multiple reviewers dedicated to full involvement throughout the process.

Thirdly, this review could potentially have excluded an article as it does not use controlled vocabulary. While efforts were made to address this through asking experts and forward and backward searching of references, which led to an additional inclusion of three articles, it is possible that some relevant articles were missed.

Fourthly, the review was limited to English-language literature, although this restriction removed only one article in total, written in Korean. Future research would do well to investigate the literature written in other languages as well as to include searching non-English language databases.

Lastly, technical papers focusing on coding aspects of website defacement were excluded to maintain focus on the criminological aspects of the phenomenon. Despite the author's ability to code and experience with SQL injection techniques, this was necessary to limit the number of articles to a manageable level and to preserve the focus of the review to those involved in this crime, instead of discussing the plethora of methods used to commit this crime. Furthermore, his opinion is that such technical discussions largely would not add to the criminological findings on offenders and victims but would likely confuse many who sought to read this review. However, it is possible that some articles excluded could have contributed to our understandings of victims beyond technical discussions of code exploits.

Despite these limitations, this scoping review serves two important purposes: guiding future research in the field of website defacement and providing the first comprehensive overview of the existing literature. Despite its limitations, the review aimed to be rigorous and contribute value to the field.

### *2.7.3. Funding*

There were no sources of funding for this scoping review.

# Chapter III: Predicting New Hackers' Criminal Careers: A Group-Based Trajectory Approach

## 3.1. Abstract

The current study employs group-based trajectory modeling to assess the longitudinal attack patterns of new hackers involved in website defacement. Specifically, we track the activity of 241 emergent hackers for one year following their first verified website defacement. In doing so, we find four distinct criminal trajectories: low threat (29.0%), naturally desisting (26.5%), increasingly prolific (22.3%), and persistent threat (22.1%). Hackers classified as low threats engage in few defacements, whereas persistent threats engage in high-frequency attacks. Those labeled as naturally desisting begin their careers with velocity but become less prolific with time. Conversely, those classified as increasingly prolific engage in more attacks as they advance in their criminal careers. Using a series of regression models, we find that digital artifacts and open-source intelligence are predictive of group involvement. The findings presented in this study contribute to our theoretical understanding of the developmental trajectories of hackers, while providing valuable insights in fostering targeted intervention strategies aimed at effectively mitigating and preventing cyber-attacks.

## 3.2. Introduction

The Internet has assumed a pivotal role in the economy and the international system, establishing cyber-breaches as the foremost security concern for both government and business operations (Cawthra et al., 2019). Despite hackers being the primary instigators of most cyber-breaches, there has been limited research into their behavioral patterns. While scholars, including those in economics (Tsiakis & Stephanides, 2005), psychology (Firdaus et al., 2022), and criminology (Howell et al., 2022) acknowledge the importance of human behavior in adversarial

operations and employ decision theories to model behavioral patterns, a vast majority of these studies fall short in providing empirical tests using data derived directly from active malicious hackers.

A division among sub-disciplines, where computer scientists prioritize technical investigations while social scientists frequently lack the technical expertise to extract pertinent data regarding active offenders (Maimon & Louderback, 2019), has contributed to a fragmented understanding within the cybersecurity industry. Consequently, the disconnect between disciplines underscores the need for more comprehensive, integrated research that not only recognizes the human aspect of adversaries but also utilizes empirical assessments based on data from active malicious hackers. Such an approach can significantly enhance our understanding of cyber threats and inform more effective cybersecurity strategies.

The current study attempts to bridge this divide, utilizing cyber-intelligence insights and theories of human behavior to inform technical cybersecurity strategies. We argue that by fostering a more nuanced understanding of threat actors, such as hackers, we can provide a more realistic portrayal of the threat landscape, which can consequently aid in enhancing security posture. Our methodology comprises the extraction and analysis of active offender data from a subset of malicious hackers initially identified on Zone-H, the world's most popular hacking archive (http://www.zone-h.org/). In the following section, we delve deeper into an exhaustive review of studies pertinent to this topic. Notably, this study stands out as the pioneering research endeavor that systematically maps the criminal trajectories of new hackers, leveraging open-source intelligence (OSINT) and other digital artifacts to forecast future attack trends. Our investigation is driven by two fundamental research questions:

1. Are there identifiable patterns in the criminal trajectories of novice hackers within a year of their initial attack?
2. Can the use of OSINT and other digital artifacts facilitate the prediction of cyber-criminal trajectories?

Our study reveals the presence of four distinct trajectories among hackers and provides compelling evidence for the predictive capabilities of utilizing OSINT and other digital artifacts to forecast longitudinal attack trends. By demonstrating this capacity, we underscore the significance of adopting a life-course criminology perspective (Sampson & Laub, 1990, 2018) to gain a comprehensive understanding of hacker behavior. Through the process of plotting and predicting the behavioral patterns of novice hackers, we offer valuable insights into the factors influencing their involvement in cybercrime, their persistence or desistence in criminal activities, and the potential turning points that may redirect their behavior. Additionally, by analyzing the progression of attacks from initial defacement activities, we can identify common pathways or stages that hackers tend to traverse. This knowledge serves as a solid foundation for the development of targeted interventions and prevention strategies aimed at disrupting and mitigating cyber threats. By comprehending the dynamic nature of hacker trajectories, proactive measures can be implemented to address critical transition points and foster positive behavioral changes within the hacker community.

## 3.3. Theoretical Framework

### *3.3.1. Life-Course Criminology*

The field of criminology has witnessed remarkable progress in recent years in advancing our understanding of individuals' involvement in criminal behavior over their lifetimes. This progress has been facilitated by the application of the life-course criminology framework, which

offers a comprehensive perspective on the dynamic interplay between personal characteristics, social factors, and environmental influences that shape individuals' engagement in criminal activities (Sampson & Laub, 1990, 2018; Laub et al., 2018, Laub & Sampson, 2019). Researchers have effectively utilized this theoretical framework to investigate various types of crime and have successfully plotted and predicted criminal trajectories, revealing that a small proportion of chronic offenders are responsible for most criminal offenses (Benson, 2013; DeLisi & Piquero, 2011; Elder et al., 1985; Laub & Sampson, 2006, 2019; Laub et al., 2018; Nagin, 1999, 2005; Piquero, 2008).

Furthermore, researchers have identified critical life events that act as turning points in individuals' trajectories, redirecting them away from a life of crime and toward conformity. These turning points often include significant events such as marriage, parenthood, and career attainment, which bring about increased responsibilities, commitments, and social bonds. Such life events have the potential to reshape individuals' priorities, motivations, and social connections, ultimately reducing their involvement in criminal activities (DeLisi & Piquero, 2011; Laub & Sampson, 2006, 2019; Laub et al., 2018; Nagin, 1999, 2005; Piquero, 2008; Sampson & Laub, 1990, 2018). Understanding the factors associated with the persistence or desistence of criminal behavior provides valuable opportunities for the implementation of targeted interventions and preventive strategies at specific developmental stages (Laub et al., 2018, 2019; Nagin, 1999, 2005).

The practical application of research on criminal trajectories to design targeted interventions for crime prevention has been a subject of both interest and implementation (Van der Stouwe et al., 2014). Initiatives rooted in life-course criminology have attempted to identify critical turning points and offer support to individuals, particularly in the juvenile justice system,

aiming to redirect them away from criminal activities and toward positive life events (Mulvey et al, 2004). While some individuals have responded positively to such interventions, yielding reduced criminal behavior and improved outcomes (Van der Stouwe et al., 2014), it is essential to recognize that the effectiveness of these programs can vary widely. Factors like individual willingness, intervention program quality, and socio-economic context play crucial roles. Ethical considerations and potential unintended consequences also warrant ongoing scrutiny. Therefore, while research on criminal trajectories provides a valuable theoretical foundation, the practical implementation of targeted interventions requires thoughtful evaluation and adaptation to specific contexts, with a keen awareness of the potential limits and ethical considerations involved (Mulvey et al., 2004; Van der Stouwe et al., 2014).

### *3.3.2. Life-Course Criminology and Malicious Hacking*

The life-course criminology framework, although originally developed to understand criminal behavior in offline environments, can be extended to the study of cybercrime (Weulen Kranenbarg et al., 2018). Like traditional criminal behavior, malicious hacking follows distinct trajectories, wherein a small number of persistent offenders are responsible for a significant majority of cyber offenses (Burruss et al., 2021; van de Weijer et al., 2021). The application of the framework to understand these trajectories would enable researchers to identify chronic offenders and acquire valuable insights into the factors that contribute to their sustained involvement in online criminal activities. Moreover, the concept of turning points can be extended to the study of hackers, offering an avenue for the development of targeted interventions and prevention strategies aimed at deterring hackers from engaging in malicious activities. By identifying the life events or transitions that act as triggers for transformative

change, researchers can strategically intervene at crucial junctures to redirect individuals' behavior and foster desistence from cybercrime.

However, studying cybercriminal behavior poses unique challenges due to the anonymity that hackers enjoy in the digital realm (Howell & Burruss, 2020). This anonymity hinders the gathering of offense records and the measurement of traditional turning points commonly observed in the physical world, such as marriage or employment (Weulen Kranenbarg et al., 2018). Consequently, our understanding of the longitudinal behavioral patterns of cybercriminals is severely limited, representing a significant knowledge gap in the field. To address this gap, research is needed to explore the developmental trajectories and factors influencing the persistence and desistence of malicious hackers. Our study aims to fill this void by utilizing a sample of verified, malicious hackers, providing valuable insights into the longitudinal trajectories of emergent hackers and shedding light on the factors that drive their continued engagement in cybercrime.

## 3.4. Literature Review

### *3.4.1. Hackers*

Hackers are adept at exploiting vulnerabilities to gain unauthorized access to computer systems and internet technologies (Grabosky, 2016). This unauthorized access provides them with the means to engage in a range of criminal activities. For instance, malicious hackers may employ their unauthorized access to engage in spamming, inundating individuals with unsolicited and often fraudulent emails (Perkins et al., 2022). Additionally, hackers may utilize their access to launch attacks on other computers or networks, disrupting services and compromising sensitive information (Grabosky, 2016). Another common misuse of unauthorized access is the integration of compromised systems into larger botnet networks, which are used to

carry out coordinated attacks (Mirkovic & Reiher, 2004). The illicit activities enabled by hackers' exploitation of vulnerabilities highlight the need for robust cybersecurity measures and a thorough understanding of hacker behavior to effectively mitigate the risks posed by cybercrime.

Research has demonstrated that these risks are amplified when hackers form online communities and collaborate as part of organized teams (Perkins et al., 2023). These hacker communities, known as hacking groups or collectives, provide platforms for hackers to share knowledge, tools, and resources, as well as engage in sophisticated and coordinated cyber-attacks (Décary-Hétu et al., 2012; Lu et al., 2010). Through collaborative efforts, these groups can develop advanced hacking techniques and execute large-scale attacks with severe consequences. Moreover, these communities foster a sense of belonging and identity among hackers, glorifying their actions and encouraging further involvement in cybercriminal behavior (Jordan & Taylor, 1998; Taylor, 1999). Participation in hacker communities has been found to be a significant predictor of engagement in malicious hacking (Jordan & Taylor, 1998; Morris & Blackburn, 2009; Taylor, 1999).

Given the clear and crucial need to study hacking behavior, extensive research is currently being conducted to investigate hackers' methods, motivations, and organizational structures (Burruss et al., 2021; Holt et al., 2019; Holt et al., 2020; Maimon et al., 2017; Ooi et al., 2012; Woo et al., 2004). This research reveals a wide range of behaviors and motivations among hackers, differentiating them from traditional criminals and from each other (Burruss et al., 2021; Holt et al., 2019; Holt et al., 2020; Leukfeldt, 2017; Maggi et al., 2018; Ooi et al., 2012; Woo et al., 2004). These motivations influence hackers' decision-making processes, particularly regarding attack frequency and target selection (Woo et al., 2004; Holt et al., 2019; Holt et al., 2020; Burruss et al., 2021; Leukfeldt, 2017).

Some hackers are primarily motivated by financial gain, exploiting vulnerabilities for personal profit, while others find motivation in ideological reasons such as political activism or challenging authority (Holt et al., 2019; Holt et al., 2020; Burruss et al., 2021; Leukfeldt, 2017). Additionally, there are individuals who engage in hacking for the thrill and the status it brings within their community (Ooi et al., 2012). These diverse motivations greatly influence hackers' persistence in engaging in illicit activities and their selection of targets. Financially motivated hackers, for instance, prioritize opportunities that offer substantial financial rewards, while ideologically driven hackers may focus on organizations they perceive as oppressive or unethical (Holt et al., 2019; Holt et al., 2020; Howell et al., 2020).

Indeed, the concept of a "generic hacker" perpetuated in popular culture is misleading and fails to acknowledge the wide range of motivations, skills, and behaviors exhibited by individuals involved in hacking activities. In light of this recognition, researchers frequently employ a categorization approach that is based on various sub-types of hackers (Landreth, 1985). This approach allows for a more nuanced analysis of the hacking community and facilitates targeted investigations and interventions. By identifying different sub-groups of hackers, researchers can explore the specific motivations, skillsets, and patterns of behavior within each category (Zhang et al., 2015). These sub-types can vary widely, encompassing hacktivists who engage in cyber activism for political or social causes, state-sponsored hackers involved in espionage or cyber warfare, organized cybercriminal groups seeking financial gains, or even individual hackers driven by personal curiosity or a desire for recognition (Burruss et al., 2021; Landreth, 1985; Zhang et al., 2015).

Although classification attempts have contributed to our understanding of hacker behavior, there is still a lack of comprehension regarding their long-term patterns and limited

research on generalizing findings to different hacker populations. To address these gaps, the current study takes a data-driven approach by utilizing OSINT to examine a specific cohort of verified malicious hackers who specialize in website defacement. By analyzing longitudinal trends in hacking activity, we aim to develop a novel categorization framework that provides insights into the behavior of these hackers over time. This research seeks to offer a deeper understanding of the dynamics and characteristics of this specific hacker group.

### *3.4.2. Website Defacement*

Website defacement, conducted by hackers called defacers, involves vandalizing websites by exploiting security vulnerabilities to gain unauthorized access and modify content (Maimon et al., 2017; Ooi et al., 2012; Woo et al., 2004). This digital vandalism damages the targeted website's reputation and credibility, eroding trust and potentially leading to decreased website traffic and negative impacts on associated businesses (Maimon et al., 2017). Financially, it can result in investigation costs, restoration expenses, and the potential for legal repercussions if sensitive data is stolen or exposed (Ooi et al., 2012). Moreover, website defacement undermines trust in the online ecosystem, discouraging e-commerce activities and deterring potential investors (Howell et al., 2020). Finally, defacement can be used as a tool for conveying political or ideological messages, potentially causing social and political tensions and reputational harm (Ooi et al., 2012).

Understanding the behavior of defacers is essential due to the detrimental impacts associated with their actions. Defacers possess distinct characteristics that set them apart from other hackers, such as their willingness to disclose their identities and activities through their hacker monikers (Woo et al., 2004). They actively seek attention and reputation within the hacking community by reporting their exploits on platforms like Zone-H and leveraging social

media platforms. Notably, social media engagement has been found to be associated with hacking behavior, as individuals who use platforms like Facebook and Twitter tend to exhibit higher frequencies of attacks (Maimon et al., 2017).

Motivation also plays a significant role in the behavior of defacers. They launch attacks for a range of reasons, spanning from seeking recognition and acceptance within the hacking community to the excitement and challenge of compromising target sites. Additionally, various sociopolitical factors may also motivate their actions (Ooi et al., 2012; Perkins et al., 2023; Woo et al., 2004). These motivations are closely correlated with the frequency of attacks and the selection of targets (Holt et al., 2020; Howell et al., 2019).

While it is widely recognized in the present research that defacers with distinct characteristics are likely to display varying attack patterns, there remains a significant gap in the literature when it comes to categorizing groups based on these patterns. Only two studies have tried to address this issue. The first study, conducted by Burruss et al. (2021), employed finite mixture modeling to classify 119 hackers into two groups based on their attack frequency. The findings of this study revealed the existence of a large group of occasional defacers and a much smaller group of frequent defacers (Burruss et al., 2021). However, an important limitation of this study is that it did not examine behavioral patterns over time to determine the predictive value of various observable characteristics on longitudinal attack trends. By solely focusing on attack frequency and categorizing defacers into two groups, the study overlooks the potential for dynamic changes in their behavior over extended periods. It is plausible that defacers may evolve, transitioning between the two identified groups, as they advance in their criminal careers. Moreover, the study only considered defacements with English content, casting doubt on the generalizability of the findings.

Addressing these limitations, van de Weijer et al. (2021) conducted a comprehensive study examining the attack patterns of over 66,000 defacers over a seven-year duration. Their research successfully identified six distinct groups of defacers, namely low and high sporadic defacers, low and high declining defacers, and low and high chronic defacers. Notably, the study revealed that most of the variation in attack trajectories occurred within the first year, with minimal changes observed thereafter. This longitudinal investigation overcame the limitations of the Burruss et al. (2021) study by utilizing a dataset spanning multiple languages and capturing the dynamic nature of hacking behavior.

However, despite its significant contributions, the study conducted by van de Weijer et al. (2021) had its own shortcomings. One notable limitation is the failure to utilize available data to predict group involvement. While understanding the trends and characteristics of defacers is undoubtedly valuable for academic purposes, the development of proactive mitigation and prevention strategies requires the formulation of statistical models capable of forecasting events before they occur. By neglecting this crucial aspect, the study missed an opportunity to contribute directly to the formulation of effective policy solutions. The current study seeks to fill these gaps in the literature.

### 3.5. Current Study

The current study contributes to the existing literature in two key areas. Firstly, it examines the presence of identifiable patterns within the criminal trajectories of novice hackers during the first year following their initial attack. By closely analyzing the behavior of newly emerged hackers during this critical period, the study aims to uncover patterns and trends that offer insights into the continuation or cessation of their criminal activities. This examination of

the early stages of engagement in cybercrime provides a deeper understanding of the factors that contribute to the persistence or desistence of hackers.

Secondly, the study explores the potential of utilizing OSINT and other digital artifacts to predict cyber-criminal trajectories. By leveraging these data sources, the study aims to develop a predictive model capable of forecasting the future trajectories of hackers. This predictive capability holds significant value in identifying individuals who are likely to exhibit persistent criminal behavior or undergo changes in their criminal activities over time. Taken together, the study is guided by two overarching research questions:

1. Are there identifiable patterns in the criminal trajectories of novice hackers within a year of their initial attack?
2. Can the use of OSINT and other digital artifacts facilitate the prediction of cyber-criminal trajectories?

The relevance of life-course criminology for understanding hacker behavior is evident in this study. This perspective acknowledges that criminal behavior is not fixed, and that individuals' experiences and circumstances evolve over time, impacting their criminal trajectories (Sampson & Laub, 1990, 2018). By plotting and predicting the behavioral patterns of novice hackers, valuable insights can be gained into the factors that contribute to their involvement in cybercrime, their persistence or desistence, and the potential turning points that may redirect their behavior. Additionally, by analyzing the progression from initial defacement activities, common pathways that hackers tend to follow can be identified. This knowledge facilitates the development of targeted interventions and prevention efforts that can be implemented at critical junctures along their criminal trajectories (Maimon et al., 2021).

## 3.6. Methods

### *3.6.1. Data*

Our data on defacement activity comes from Zone-H. Created in 2002, Zone-H is a publicly accessible website that archives information about successful website defacements (Maimon et al., 2017). Zone-H has worldwide recognition among hackers, and it is the most popular website of its kind. As a result, the site has over 168,000 active users and has logged over 15 million verified attacks against websites hosted all over the world (Zone-H, 2019 & Howell et al., 2019). When hackers deface a website, they report the defacement to Zone-H. Once Zone-H verifies the legitimacy of the attack using automated software, it is permanently housed in their archive. The archive stores a mirror image of each defacement, in addition to the hacker's moniker, the defacement date, and other information regarding the attacked site. Nearly all past studies on website defacement use this archive as the primary data source (e.g., van de Weijer et al., 2021; Burruss et al., 2021).

### *3.6.2. Sample*

To ensure a robust dataset for the study, a Python web scraper was developed and deployed to extract information from the Zone-H archive. Through this process, we identified a total of 778 unique hacker monikers associated with defacement activity. It is important to clarify that our focus is on plotting and predicting the criminal trajectories of new hackers. In this context, the trajectory is initiated by the first defacement verified by Zone-H. While this initial defacement may not represent the individual's first attack, it serves as the starting point for their associated moniker. Thus, it provides an approximation of the beginning of their hacking careers, as it is the earliest identifiable attack linked to their moniker. Given the anonymity of hackers' true identities, this approach allows us to establish a reference point for analyzing their activities.

While acknowledging the limitation of using a single moniker for analysis, it is important to note that many defacers tend to adopt a consistent moniker to build and establish their reputation within the hacking community (Burruss et al., 2021; Maimon et al., 2021; Ooi et al., 2012; Woo et al., 2004). This practice of maintaining a single identity reduces the likelihood of moniker changes. However, we delve deeper into this limitation in a subsequent section and propose potential avenues for future research to address this issue.

The study implemented specific criteria for selecting a sample of hackers for analysis. Individuals who had logged over 50 pages of defacements (equivalent to 1,250 attacks) or whose first attack occurred after February 14th, 2019, were excluded from the sample. A limitation of the Zone-H archive, which only displays 50 pages of defacements per hacker, made it impossible to determine the exact date of the first attack for those exceeding this limit. It is worth noting that hackers who log over 1,250 defacements in a year are considered outliers (Burruss et al., 2021). Therefore, including such outliers would have distorted the data and potentially biased the results. Additionally, since the data collection period concluded on February 15th, 2020, hackers who initiated their first attack after February 14th, 2019, did not have the necessary data points for inclusion in the analysis. As a result, the final sample consisted of 241 malicious hackers for analysis.

It is important to recognize that the self-imposed parameters in the study, while necessary for analysis, do have limitations on the generalizability of the findings. These restrictions narrow the scope of the study and may not capture the entirety of hacker behavior. The implications of this limitation are thoroughly examined and discussed in the corresponding section, where the study's boundaries are acknowledged, and potential avenues for future research are proposed.

This discussion enables a more comprehensive understanding of the study's outcomes and the context in which they can be interpreted.

### *3.6.3. Dependent Variable*

The primary objective of this study is to examine the prevalence of defacement activity over the course of one year. To achieve this, we analyzed data collected on defacement incidents and used the information to plot and predict the criminal trajectories of 241 novice hackers. For each hacker, we generated 52 binary variables, representing the weeks following their initial attack. These variables indicate whether a hacker launched any attacks during each respective week. On average, we found that approximately 27.76% of the defacers successfully executed and reported their exploits to Zone-H in any given week. This provides valuable insight into the overall engagement and reporting behavior exhibited by these hackers throughout the study period.

This approach aligns with previous research conducted by van de Weijer et al. (2021) and offers several notable advantages. Instead of solely focusing on the frequency of attacks launched each week, the current study places a particular emphasis on examining longitudinal engagement (i.e., persistence) in hacking. By utilizing binary variables, the study can assess the prevalence of hacking activity across different weeks and various groups within the sample. This approach effectively addresses the issue of skewness commonly observed in datasets related to hacking activity, where a small number of chronic offenders are responsible for most cyber-attacks (Burruss et al., 2021). By categorizing the outcomes into binary variables, the study provides a more balanced representation of the prevalence of hacking behavior and facilitates the analysis of prevalence trends.

### *3.6.3. Independent Variables*

**Content Analysis.** Our research team conducted a thorough analysis and coding of the initial defacements for each of the 241 defacers by utilizing the attack images available in the Zone-H archive. The first defacement was specifically chosen as it signifies the commencement of their hacking activity. In addition, predicting trajectories based on the initial attack can offer valuable early warning signs to identify and potentially deter emerging hackers before they become more prolific in their activities. However, it is important to acknowledge that while manual coding of all defacements would provide deeper insights into potential turning points, it was not feasible due to the sheer volume of defacements.

The coding process for each variable was conducted qualitatively based on the content of the defacements. To ensure the reliability of our coding, we assessed the interrater reliability, which yielded scores ranging from 85% to 100%. Below is a more detailed description of each of the qualitive variables extracted from the defacement and used to forecast longitudinal patterns:

*Animation*: The presence or absence of animation in defacements can provide insights into the technical skills and creativity of the hackers. Defacements with animation may suggest a higher level of expertise and a desire to make a visually impactful statement, potentially indicating a more advanced or experienced hacker (Burruss et al., 2021). Defacements with the presence of animation were coded as "1," indicating the presence of animation. Defacements without animation were coded as "0."

*Contact Information*: The inclusion of contact information in defacements indicates a willingness to engage in further communication and potentially collaborate with other hackers or interested parties. Hackers who provide contact information may have stronger connections within the hacking community or seek recognition and collaboration, suggesting a higher level of

engagement and potential for future hacking activities. Defacements that included the hacker's contact information, such as email addresses, Telegram username, or handles for communication channels, were coded as "1." Defacements without contact information were coded as "0."

*Team Membership*: Content relating to team membership can be indicative of a hacker's affiliation with a hacking collective. Hackers who belong to teams may benefit from shared resources, knowledge exchange, and collaborative efforts, potentially leading to more coordinated and impactful hacking activities. Therefore, team membership can provide insights into the level of organization and potential future activities of the hacker (Perkins et al., 2023). To determine team membership, two indicators were considered. If a distinct group moniker separate from the defacer's alias was displayed in the defacement, it was considered as an indicator of team membership. Additionally, if a team roster was listed in the defacement, it was also considered as an indicator of team membership. Defacements with either of these indicators were coded as "1" for team membership, while defacements without these indicators were coded as "0."

*Political Content*: Defacements containing political content demonstrate the hackers' ideological or activist motivations. Political messaging in defacements can reflect the hacker's personal beliefs, motivations, or a desire to convey a particular message to a wider audience. Such defacements may indicate a hacker's inclination towards targeted attacks related to political causes or involvement in hacktivist movements (Holt et al., 2020; Howell et al., 2019; Woo et al., 2004). Defacements containing content related to government or public affairs, such as statements like "Justice for Palestine," "Death to American pigs," or "India, free Kashmir," were coded as "1." Defacements without such content were coded as "0."

*Religious Content*: Defacements containing religious phrases, messages, and imagery suggest that religious beliefs or affiliations may influence the hackers' motivations and actions. Religious content in defacements can reflect the ideological or symbolic significance attributed to their hacking activities. It may indicate a specific agenda, or the involvement of hackers associated with religiously motivated hacking groups (Woo et al., 2004). Defacements containing such content were coded as "1." Defacements without such content were coded as "0."

**Open-Source Intelligence (OSINT).** To gather additional information on the hackers included in our study, we conducted OSINT searches using their aliases. This approach allowed us to explore the presence and activities of the hackers across various platforms, both licit and illicit, providing valuable insights into their visibility and impact within the hacker community. The use of a consistent hacker moniker across platforms further demonstrates their dedication to establishing and enhancing their online identity and reputation.

*Social Media:* Social media engagement has consistently shown associations with defacement behavior, as evidenced by previous research (Maimon et al., 2017), highlighting its importance in understanding the level of involvement and influence of hackers. We searched for the aliases on popular social media platforms, including Facebook, Twitter, Instagram, Telegram, and YouTube. Hackers who were identified on at least one of these platforms were assigned a score of "1," indicating their presence, while hackers who were not identified on any of these platforms were assigned a score of "0."

*Reported on Multiple Platforms (RMP):* The act of reporting defacements on multiple platforms reflects a hacker's intention to showcase their skills, attract attention, and establish their influence within the hacking community. This behavior may be associated with certain

attack trends and patterns. We searched for the aliases of the hackers on other defacement reporting websites, such as X-security and Defacer-ID. Hackers who were identified on at least one of these platforms were assigned a score of "1," indicating that their defacement activities were reported on more than one defacement platform. Conversely, hackers who were not identified on these platforms were assigned a score of "0."

### 4.6. Analytic Strategy

We employed a latent group-based trajectory modelling approach that enables tracking the attack prevalence of defacers over time to estimate new hackers' criminal trajectories (Nagin 1999, 2005). Group-based trajectory models are employed to explore how behaviors or outcomes develop over time and to identify distinct groups within a population that follow similar trajectories. Additionally, group-based trajectory models allow for the inclusion of time-stable covariates that may help predict group membership. This approach provides a powerful tool for understanding the diversity of developmental trajectories and the factors that influence them.

In our study, we utilize the principles of group-based trajectory modeling to differentiate between distinct groups of hackers based on their longitudinal attack prevalence. We aim to examine the influence of various time-invariant predictors (see section immediately above) on the likelihood of belonging to a specific group. Since our dependent variable is dichotomous (presence or absence of attacks), trajectories are estimated using logistic models. A hacker's initial defacement reported to Zone-H serves as the starting point for their trajectories, and we model their trajectories over 52 weekly time periods during their first year. The optimal number of groups is determined using the Bayesian Information Criterion (BIC), and the shape parameters of each group's trajectory are allowed to vary to identify the most appropriate trajectory shapes. All statistical analyses are performed in STATA, and we estimate the group-

based trajectory logistic models using the Stata plugin developed by Jones and Nagin (2013). This approach enables us to capture the diverse patterns of attack trajectories among hackers and assess the influence of relevant predictors on group membership.

## 3.8. Results

### *3.8.1. Descriptive Statistics*

Table 3.1 displays the descriptive statistics for the measures examined in our study. The data reveals that a significant portion of defacers were active on social media, with 73% having a presence on these platforms. Additionally, 50% of the defacers were found to report their defacement activities across multiple platforms. Furthermore, 39% of the defacers were identified as belonging to a team, indicating their affiliation within the hacker community. In terms of the content of their first defacements, 9% contained religious messages, 12% contained political messages, and 59% featured animation. Finally, 34% of the defacers left their contact information in their defacements. These statistics provide a snapshot of the prevalence of various characteristics among the defacers in our study.

**Table. 3.1. Descriptive Statistics**

*Descriptive Statistics.*

| Variable | Mean | SD | Min | Max |
|---|---|---|---|---|
| Defacement Content | | | | |
| Political Content | .120 | .326 | 0 | 1 |
| Religious Content | .091 | .289 | 0 | 1 |
| Team Membership | .394 | .490 | 0 | 1 |
| Animation | .585 | .493 | 0 | 1 |
| Contact Information | .344 | .476 | 0 | 1 |
| OSINT | | | | |
| Social Media | .734 | .442 | 0 | 1 |
| RMP | .497 | .501 | 0 | 1 |

*Note*. n = 241, OSINT = Open-source intelligence, RMP = Report on Multiple Platforms.

### *3.8.2. Bivariate Analysis*

Table 3.2 presents the bivariate correlation matrix for the independent variables in our study. The results demonstrate that most of the variable pairs exhibit weak correlations, with less than a third reaching conventional levels of statistical significance. Among the significant correlations, the strongest relationship is observed between political messages and religious messages (r = 0.33). This moderate-strength positive correlation indicates that a notable proportion of defacers incorporate both political and religious messages in their initial defacements. Both religious and political messages are correlated with leaving contact information (r = 0.13 and r = 0.16, respectively), suggesting that some defacers with ideological motives may include their contact information in their defacements. Additionally, there is a positive correlation (r = 0.14) between the presence of contact information and social media presence, indicating that these defacers seek increased visibility and attention. Furthermore, the positive correlation (r = 0.16) between animation and team membership suggests that there may be a tendency for hacking teams to use the team's logo as a branding initiative or to signify their collective identity. Overall, the bivariate correlations provide insights into the associations between the variables, highlighting the interrelationships among different aspects of defacement behavior.

**Table 3.2. Bivariate Correlations**

*Bivariate Correlations.*

| **Variable** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 1 | Team Membership | — | | | | | | |
| 2 | Religious Content | .010 | — | | | | | |
| 3 | Political Content | .093 | .326** | — | | | | |
| 4 | Animation | .162* | .033 | .027 | — | | | |
| 5 | Contact Information | .023 | .134* | .161* | .150* | — | | |
| 6 | Social Media | .062 | .060 | .107 | -.068 | .139* | — | |
| 7 | RMP | .114 | .059 | .040 | .082 | .012 | .016 | — |

*Note*. n = 241, RMP = Report on Multiple Platforms. *$p < .05$. **$p < .01$.

### *3.8.3. Group-Based Trajectory Models*

We estimated a series of group-based trajectory logistic models to analyze the hacking trajectories of the defacers in our study. Among the models tested, the one with four groups demonstrated the highest BIC score, indicating its superior fit to the data. Given the relatively small size of our dataset, selecting the model with the highest BIC score ensures the best performance. To determine the functional form of the regression line for each group, we examined various variations of linear and squared terms and identified a model in which all terms were statistically significant. This model most accurately captures the relationships between the predictors and the probability of group membership. Table 3.3 presents the AvePP and OCC scores for each group, providing insights into the average posterior probability and overall classification accuracy of the model.

**Table 3.3. Model Fit Statistics.**

*Model Fit Statistics.*

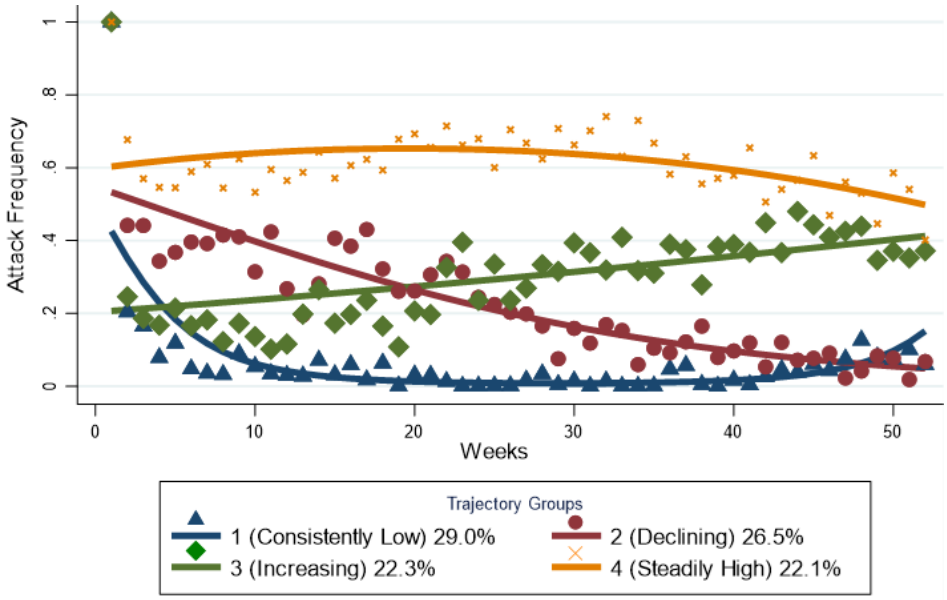
| Group | n | APP | OCC | OCC_pp | p | TotProb |
|---|---|---|---|---|---|---|
| 1 | 69 | 0.98 | 103.64 | 102.87 | 0.29 | 0.29 |
| 2 | 55 | 0.96 | 71.99 | 67.75 | 0.23 | 0.24 |
| 3 | 63 | 0.92 | 32.35 | 32.94 | 0.26 | 0.26 |
| 4 | 54 | 0.95 | 59.86 | 63.04 | 0.22 | 0.22 |

*Note*. APP = average posterior probabilities, OCC = odds of correct classification based on max post-probability, OCC_pp = odds of correct classification based on weighted post-probability, p = probability based on group assignment, TotProb = probability based on the sums of the posterior probabilities.

Figure 3.1 presents the results of our analysis, revealing the presence of four distinct groups among the defacers: the high-persistence group (persistent threats), the low-persistence group (low threat), the steadily increasing group (increasingly prolific), and the steadily decreasing group (naturally desisting). The trajectories of these four groups are depicted in Figure 1, along with their relative sizes in the sample. The low-persistence trajectory group,

group one, is the largest, comprising 29% of the sample and serving as the reference group for subsequent analyses. Group two, the declining trajectory group, accounts for 26.5% of the sample. Group three, the increasingly prolific group, represents 22.3% of the sample. Lastly, group four, the high-persistence trajectory group, consists of 22.1% of the sample.

**Figure 3.1. Defacer Trajectories**




Next, we present the results of our analysis on the time-stable covariates that may predict group membership in the criminal hacking trajectories. The findings are displayed in Table 3.4. In Model 1, the results suggest that members of the declining trajectory group were more likely to use social media and include animation in their first defacements (b=1.13 and 0.96, respectively). However, providing contact information decreased the likelihood of belonging to this group (b=-1.31). Moving to Model 2, the results indicate that for the increasing trajectory group, defacers who reported their defacements on multiple platforms were more likely to be part of this group (b=1.09). No other predictors were found to be significant for this group. Finally, in Model 3, the findings demonstrate that defacers in the high-persistence trajectory group were more likely to use social media, include animation in their first defacements, and

report on multiple platforms (b=1.12, 0.67, and 1.12, respectively). Conversely, defacers providing contact information were less likely to belong to the steadily high group (b=-0.82). These results provide insights into the associations between the time-stable covariates and group membership within the hacking trajectories, shedding light on the factors that may differentiate the various groups.

**Table 3.4. Group-Based Trajectories of Hackers.**

*Group-Based Trajectories of Hackers.*

| Variable | Model 1 | | Model 2 | | Model 3 | |
|---|---|---|---|---|---|---|
| | **b** | **se** | **b** | **se** | **b** | **se** |
| Defacement | | | | | | |
| Political Content | 1.42 | .54 | .70 | .92 | 1.20 | .83 |
| Religious Content | -0.83 | 1.20 | .65 | .77 | .73 | .75 |
| Team Membership | -0.09 | .43 | -0.53 | .43 | .35 | .42 |
| Animation | 0.96** | .42 | .47 | .43 | .67* | .44 |
| Contact Information | -1.31** | .47 | .31 | .45 | -0.82* | .45 |
| OSINT | | | | | | |
| Social Media | 1.13** | .47 | -0.02 | .45 | 1.12** | .49 |
| RMP | .72 | .41 | 1.09** | .41 | 1.12** | .41 |

*Note*. n = 241, OSINT = Open-source intelligence, RMP = Report on multiple platforms.
Model 1 represents the declining trajectory group. Model 2 represents the steadily increasing group. Lastly, Model 3 represents the consistently high trajectory.
*$p < .05$, one-tailed. **$p < .01$, one-tailed.

To examine the potential interaction effects between team membership and reporting on multiple platforms, we incorporated a multiplicative interaction term as a time-invariant covariate in our models. This analysis aimed to explore whether the combined influence of these predictors on group membership deviated from what would be expected based on their individual effects. Table 3.5 presents the results of this analysis, which reveal a significant and positive coefficient for the interaction term in predicting group involvement in the increasing trajectory group (b=1.54). This suggests that the combined influence of team membership and reporting on

multiple platforms has a distinct impact on hackers' involvement in the increasing trajectory group. Hackers who are part of a team and actively report their defacements on various platforms may benefit from enhanced opportunities for learning, collaboration, and recognition within the hacking community, leading to their increased persistence over time.

Although the interaction term did not demonstrate a significant effect on involvement in the other trajectory groups, its inclusion in the analysis yielded other intriguing findings. Particularly, in Model 1, we observed a significant positive association between political content and membership in the declining trajectory (b=1.89). This finding suggests that hackers who incorporate political content in their defacements are more likely to exhibit a declining trend in their hacking activities over time.

**Table 3.5. Group-based Trajectories of Hackers with Interaction Term.**

*Group-based Trajectories of Hackers with Interaction Term.*

| Variable | Model 1 | | Model 2 | | Model 3 | |
|---|---|---|---|---|---|---|
| | **b** | **se** | **b** | **se** | **b** | **se** |
| Defacement | | | | | | |
| Political Content | 1.89** | .93 | .68 | .94 | 1.38 | .89 |
| Religious Content | -13.32 | 1272.3 | .75 | .74 | .43 | .81 |
| Team Membership | -0.33 | .57 | -.27 | .59 | .08 | .60 |
| Animation | 0.97** | .43 | .45 | .42 | .74* | .44 |
| Contact Information | -1.34** | .50 | .42 | .42 | -.90** | .46 |
| OSINT | | | | | | |
| Social Media | 1.15** | .49 | .14 | .43 | 1.14** | .49 |
| RMP | .50 | .52 | .53 | .51 | .89** | .53 |
| Interaction | | | | | | |
| Team*RMP | .67 | .90 | 1.54* | .85 | .76 | .88 |

*Note*. n = 241, OSINT = Open-source intelligence, RMP = Report on multiple platforms.

Model 1 represents the declining trajectory group. Model 2 represents the steadily increasing group. Lastly, Model 3 represents the consistently high trajectory.

*$p$ < .05, one-tailed. **$p$ < .01, one-tailed.

### 3.9. Conclusion

The use of longitudinal research designs has significantly improved our understanding of traditional criminal offending and desistence (DeLisi & Piquero, 2011; Laub & Sampson, 2006, 2019; Laub et al., 2018; Nagin, 1999, 2005; Piquero, 2008). However, there is a limited application of these designs in the context of cyber-offending, specifically website defacement. This study aims to bridge this research gap by examining the criminal trajectories of new hackers during their first year of engagement in cyber-offending. Our analysis has yielded significant findings regarding the predictors of natural desistence, increased engagement, and becoming a persistent threat.

In terms of natural desistence, we observed that hackers who actively engage in social media platforms and incorporate animation in their defacements tend to exhibit a declining trend in their hacking activities over time. This suggests a developmental aspect to hackers' trajectories, with early-stage hackers seeking attention and validation through flashy defacements and social media recognition. As hackers gain experience and maturity, they may transition into more serious forms of hacking or pursue lawful paths.

Interestingly, our research also indicates that politically driven hackers are more likely to naturally desist. Although these hackers engage in frequent attacks at the beginning of their criminal careers, this phase is relatively short-lived. Given their motivation is tied to real-world events (Holt et al., 2020; Howell et al., 2019) it is possible that these eager new hacktivists lose interest or become disenchanted with the cause that initially drove them to engage in cyber-offenses. This finding highlights the dynamic nature of politically motivated hacking and suggests that the passion for a cause may fade over time, leading to a decrease in their criminal activities.

Conversely, hackers who post contact information directly on compromised websites are less likely to naturally desist from their hacking activities. By openly sharing their contact information in the virtual crime scene, these hackers receive recognition and validation for their audacity. This act may lead to acceptance and integration into the hacking community, providing opportunities for skill improvement and interaction with like-minded individuals, thus sustaining their defacement activities (Perkins et al., 2023).

Regarding the steadily increasing group, we discovered an interaction effect between reporting to multiple platforms and team involvement. This interaction can be attributed to the dynamics of reputation building within the hacking community. Hackers aim to establish themselves as skilled and respected individuals. Being part of a team and actively reporting their defacements on various platforms allows them to expand their visibility and showcase their expertise to a wider audience (Perkins et al., 2023). This increased visibility and recognition significantly contribute to reputation development, promoting increased engagement in malicious hacking.

For persistent threats, our findings indicate that social media engagement, reporting defacements to multiple platforms, and the use of animation in defacements are positively associated with persistent attack trends. Active participation in social media platforms enables hackers to establish a presence, gain recognition, and build connections within the hacking community (Maimon et al., 2017). Reporting defacements on multiple platforms enhances visibility and showcases expertise to a broader audience, contributing to reputation-building. Additionally, the use of animation demonstrates technical proficiency and creativity, further enhancing hackers' reputation within the community. On the contrary, posting contact information on compromised websites is negatively associated with membership in the persistent

threat trajectory. Persistent threats may prioritize maintaining a lower profile and minimizing exposure to law enforcement or other risks (Maimon et al., 2023). By keeping their identities and contact information private, hackers aim to avoid scrutiny, minimize the risk of apprehension, and thereby maintain their persistence in hacking activities.

### *3.9.1. Theoretical Implications*

Our study has significant implications for the theoretical understanding of cyber-offender behavior. By utilizing cyber-intelligence and adopting a life-course perspective, we contribute to the existing criminological literature by expanding our knowledge of cyber-offending trajectories and factors that influence them. Traditional criminological theories often focus on turning points in an individual's life, such as marriage, employment, or education, as influential factors in criminal desistance or persistence (Sampson & Laub, 1990, 2018). However, in the cyber realm, these conventional turning points may not be as applicable or easily measurable.

The findings presented in this study underscore the utility of OSINT as an alternative strategy for data collection in the study of cyber-offender behavior. By harnessing OSINT, researchers can gather information on hackers' activities, motivations, and trajectories from diverse online sources. This approach provides valuable insights into cyber-offender behavior that can complement and expand upon traditional criminological theories.

The incorporation of a life-course perspective in our study allows us to consider the developmental trajectories of cyber-offenders over time. This perspective recognizes that individuals may go through various stages and experiences that shape their involvement in cyber-offending (Sampson & Laub, 1990, 2018). By integrating a life-course perspective, we enhance the theoretical understanding of cyber-offending by emphasizing the importance of

contextual factors, such as social interactions, online environments, and hacking communities, in shaping hackers' behaviors and trajectories.

Furthermore, the implications of our study highlight the need for criminological theories to adapt to the unique characteristics of the cyber realm. The cyber environment presents distinct challenges and opportunities for understanding and addressing cyber-offending. The use of cyber-intelligence, including OSINT, offers a promising avenue for researchers to collect and analyze data in this domain. By incorporating cyber-specific factors into existing criminological theories and developing new frameworks tailored to the cyber context, we can advance our theoretical understanding of cyber-offender behavior.

#### *3.9.3. Policy Implications*

The findings of our study hold significant policy implications that can guide policymakers and practitioners in the realms of law enforcement and cybersecurity. The insights gained from our research can inform the development of targeted policies and interventions to address the challenges posed by threat actors and safeguard networked infrastructures.

One crucial policy implication is the necessity to allocate resources effectively to target high-risk hackers, particularly those within the increasing and persistent threat groups. Policymakers and cybersecurity authorities can establish specialized units tasked with monitoring and engaging with individuals identified as high-risk based on predictive factors. These units can judiciously allocate resources to proactively mitigate potential cyber threats posed by these individuals. By doing so, organizations can enhance their cybersecurity posture and respond more effectively to emerging threats.

Furthermore, our findings suggest the potential for redirecting the skills and talent of high-risk hackers toward ethical and constructive roles within the cybersecurity landscape.

Public-private partnerships can be established to create mentorship programs, offer ethical hacking courses, and provide employment opportunities for these individuals. Regrettably, to the best of our knowledge, no such intervention programs currently exist. However, this approach not only addresses the skill shortages in the field but also reduces the pool of persistent threat actors, contributing to a safer digital environment.

A community-centric approach to cybersecurity is another valuable policy implication. Policymakers and cybersecurity practitioners can engage with online platforms and hacking communities to encourage responsible behavior and foster positive norms. Collaboration agreements with online platforms can incentivize users to report vulnerabilities and security issues responsibly. Public awareness campaigns and educational initiatives, along with partnerships with respected figures within hacking communities, can promote a culture of ethical hacking practices, acting as a powerful deterrent against malicious cyber activities.

Lastly, our research highlights the importance of investing in cyber-intelligence capabilities, particularly OSINT. Policymakers should allocate resources to establish dedicated OSINT teams equipped with the tools and expertise required to monitor online activities, gather intelligence, and assess risks. This investment enables timely detection of emerging threats, identification of evolving cybercrime trends, and informs policy decisions, facilitating a proactive and adaptive cybersecurity strategy.

By incorporating these specific policy implications into current cybersecurity strategies, policymakers and practitioners can bridge the gap between research findings and actionable steps. These policies empower organizations to proactively address cyber threats, optimize resource allocation, and nurture responsible and ethical behavior within the cybersecurity community, ultimately contributing to a more secure digital landscape.

### *3.9.3. Limitations*

While this research contributes to theory and informs policy, it is important to acknowledge its limitations. Firstly, the reliance on data from the Zone-H archive is a limitation, as it may not fully capture the entirety of hacker behavior and could be subject to biases inherent in that source. To overcome this, future research should incorporate multiple data sources to provide a more comprehensive understanding of hacker behavior.

Another limitation of our study pertains to the focus on the first verified defacement reported by Zone-H as the starting point for trajectory analysis. While this approach provides a reference point and captures the initiation of a hacker moniker's criminal career, it may not necessarily represent the individual's true first attack. Additionally, using the moniker as a proxy for the individual may overlook potential changes in their identities or monikers over time. These limitations could be addressed in future studies by exploring alternative methods to capture the true identities and multiple monikers used by hackers throughout their criminal careers. By incorporating these alternative approaches, we can gain a more comprehensive understanding of the dynamics of cyber-offender behavior and its evolution over time.

The selection criteria applied to the sample also introduce limitations, as they exclude certain individuals based on the number of defacements or the timing of their first attack. While necessary to answer specific research questions and avoid outliers, these criteria may restrict the generalizability of the findings. Future studies should consider expanding the sample criteria to include a wider range of hackers and examine how results may differ across different subsets of the hacker population.

Our research, like other non-experimental studies, is also susceptible to omitted variable bias, which means that we may not account for all the unobserved factors that can influence

cyber-offender trajectories. Another limitation arises from how our variables are operationalized. For instance, the qualitative variables only capture content from the first defacement rather than all defacements. This limited scope restricts our understanding of potential turning points in hacker trajectories. Additionally, the possibility of hackers using different usernames across platforms, separate from their known hacker monikers, adds complexity to our analysis. To address these limitations and minimize omitted variable bias, future research should strive to incorporate additional variables and refine data collection techniques to ensure the reliability and validity of the findings.

# Chapter IV: Holidays and Hacking: Analyzing Website Defacement Patterns Through Routine Activities Theory.

## 4.1. Abstract

The traditional criminological literature has explored the impact of holidays as disruptions to the typical patterns of life on crimes against individuals and property, particularly in tests of the Routine Activities Theory. Despite a significant increase in cyber-attacks and assertions by the US Government about their escalation during holidays, academic research has not investigated how holidays influence cyber-offenses. This paper fills this gap by analyzing a dataset covering the hacking careers of 230 website defacers to understand holiday effects on website defacement. It also assesses claims outside academia that holidays reduce capable guardianship and increase cyber-attacks. Using multilevel modeling and adjusting for temporal differences, our findings reveal varied holiday effects on attack frequency, highlighting the complexity of cybercriminal behavior and questioning the validity of guardianship in cyberspace.

## 4.2. Introduction

Securing the digital realm has become increasingly critical due to the ever-evolving landscape of cyber-attacks. Each year, businesses face substantial financial losses stemming from a variety of security breaches. As the Internet takes on an increasingly significant role in the economy and the global landscape, advanced persistent threats (APTs) and hackers have emerged as the primary security concerns for numerous organizations (Cawthra et al., 2019). However, despite hackers' direct responsibility, due to their anonymity, there is limited research on their behavioral patterns and preferences (Karnow, 1994; Maimon & Louderback, 2019; Van Beveren, 2001). Criminological research into the causes and correlates of cybercrime is currently limited for two main reasons. First, a significant number of criminologists are unfamiliar with

computer technology and the cyber-environment (Maimon & Louderback, 2019). Secondly, researchers delving into cybercriminals struggle to source valid and reliable data. This is in part because hackers frequently conceal their identities and meticulously eliminate traces of their cyber intrusions (Howell et al., 2017; Maimon & Louderback, 2019). This anonymity coupled with hackers' adeptness at obscuring their activities make conventional data sources, such as the FBI's Internet Crime Complaint Center, prone to underestimating the true scope of cybercrime incidents (Howell et al., 2019).

In efforts to address the challenge of cyber-security, organizations have invested millions of dollars to establish highly secure computing environments designed to reduce the probability of a successful cyber-attacks against their digital systems (Ashibani & Mahmoud, 2017). However, these efforts in cyber-defense typically rely on conventional security policies and tools, whose true effectiveness in preventing cyber-attacks remains uncertain. In attempts to improve organizations' cyber security posture, several security experts, and even the Department of Defense Science Board, advocated for the adoption of proactive approaches to cyber security, and to engage in efforts for collecting tactic cyber intelligence to predict potential attacks (Gosler & Von Thaer, 2013; Mattern et al., 2014).

While enhancing the digital structure is crucial for cyber-defense, it is equally vital to understand the behavior and preferences of cyber actors. This understanding plays a pivotal role in crafting effective policies and improving decision-making processes for both governments and organizations, particularly in the context of predicting possible attacks. This research seeks to create a model that begins meeting this need and seeks to answer whether real-world events can serve as indicators for predicting website defacement attacks. A guiding principle for creating such a model is the Routine Activities Theory, which originates from the field of criminology.

This theory offers insights into the patterns and routines of offending that might influence the behaviors of cybercriminals.

## 4.3. Literature Review

### *4.3.1. Routine Activities in Brief*

The Routine Activities Theory (RAT), introduced by Cohen and Felson in 1979, offers a unique perspective in criminology by focusing on the circumstances surrounding criminal activities rather than the characteristics of offenders (Cohen & Felson, 1979). The core premise of this theory is that criminal activity requires a convergence in space and time of "likely offenders, suitable targets and the absence of capable guardians against crime" (Cohen & Felson, 1979). Conversely, the likelihood of preventing crime increases when any or more of these three conditions are not met (Jennings, 2015). But what are these three conditions defined as throughout criminological literature? Likely offenders are individuals motivated to commit a crime, suitable targets are entities or individuals vulnerable to being victimized, and capable guardians are those empowered to deter crime and protect potential targets (Cohen & Felson, 1979; Gotham & Kennedy, 2019). Thus, RAT provides an environment-focused explanation for understanding the root causes of criminal activities.

Since its inception, the Routine Activities Theory (RAT) has been extensively utilized in criminological research to explain a diverse range of criminal activities, including armed robbery, burglary, drug dealing, and various other offenses (Baird et al., 2019; Cohen & Felson, 1979; Cohn & Rotton, 2003; Farrell et al, 2005; Jennings, 2015; Khurana 2022a, 2022b; Lam, 2020; Nazaretian & Fitch, 2021; Rotton & Frey, 1985). Scholars have scrutinized each of RAT's three conditions to understand the specific influence of these dimensions, with particular focus on suitable targets and capable guardianship. This emphasis may be partly due to a primary

criticism of RAT, which assumes that offenders are rational actors (Kitteringham & Fennelly, 2020). While RAT has proven effective in understanding conventional crimes, its application to explaining less traditional crimes, such as cybercrimes, has been limited. Cybercrimes have received considerably less attention within the RAT framework compared to other types of criminal activities.

#### *4.3.2. Routine Activities in Cyberspace*

Although the Routine Activities Theory (RAT) and its related concept, Lifestyle Routine Activities Theory, are not commonly used to explain cybercrimes, they have demonstrated moderate success in shedding light on various forms of cybercrime (Guerra & Ingram, 2022; Maimon & Louderback, 2019). The bulk of research applying RAT to cybercrimes has predominantly centered on incidents involving victims of phishing, malware/virus infections, and hacking (Guerra & Ingram, 2022; Howell et al., 2019). This emphasis can be attributed to the inherent limitations of studying cybercrime mentioned in the introduction. However, one category of cybercrime offers an opportunity to examine all three dimensions of RAT: website defacement. Before delving into the application of RAT to website defacement, it is essential to offer a concise overview of this type of crime and the existing research pertaining to it.

#### *4.3.3. Website Defacement*

Website defacers (hereafter called defacers) are hackers that engage in what can be described as digital vandalism, in a cyber-crime known as website defacement. This involves exploiting vulnerabilities in a website's or internet server's digital infrastructure to gain administrative privileges, all the while preventing the rightful owners from using their own website. The defacer then alters the visual appearance of a webpage or an entire website, completely disrupting its legitimate use (Holt et al., 2017). While most defacement incidents

target the websites of private individuals or mid- to small sized companies, even major websites are susceptible to defacement attacks, known as "special defacement" incidents, affecting large businesses, healthcare systems, or governments. Despite occurring less frequently for these larger entities, they are not immune to the threat (Maimon & Howell, 2020). Defacement also poses substantial and costly consequences to its victims, such as financial losses due to the unavailability of the site and tarnished reputation due to perceived security weaknesses (Kanti et al., 2011).

Unlike more complex hacking methods like ransomware, Zero-Day exploits, and Distributed Denial of Service (DDoS) attacks, defacement attacks are relatively straightforward. Surprisingly, advanced technical skills are not necessary to engage in website defacement. Numerous tutorials outlining the process of infiltrating a server and altering website content are readily available online, often on social media platforms like Facebook and YouTube (Holt et al., 2017). Moreover, the tools for conducting these attacks are easily accessible and simple to deploy. Given its comparative simplicity, website defacement is often regarded as an entry-level form of hacking, potentially serving as a gateway to more complex cybercriminal activities (Seebruck, 2015).

#### *4.3.4. Routine Activities and Website Defacement*

Regarding RAT, substantial efforts have been directed towards comprehending the motivations that drive defacers to initiate and sustain a life of cybercrime. In fact, the main motivation of defacers is to gain a good reputation and recognition in their community, which can lead to their recruitment by a hacking team (Woo et al., 2004). In seeking to understand more about defacer motivation, one study reveals that 70% of defacers can be classified as pranksters,

but that motives extend beyond pranking, such as: peer acknowledgement, nationalism/ideology, and more (Woo et al., 2004).

Yet, the significance of understanding defacer motivation goes beyond classification, as their motivations play a pivotal role in determining the types of websites they target (Ooi et al., 2012). For instance, defacers with similar motivations tend to consistently select similar targets and employ similar methods (Holt et al., 2020a). Likewise, the research highlights distinct differences in behavior between ideologically motivated defacers and others. For instance, ideological defacers have distinctly different motivations (Romagna et al., 2017), contain different and more aggressive messages (Woo et al., 2004), and base their target selection on the potential attention generated by the attack, rather than solely on the ease of hacking a system (Romagna et al., 2017). Studies also indicate that volumes of defacement tend to rise following real-world events that provoke ideologically driven defacers (Holt et al., 2020b).

In terms of the targets that defacers deem suitable, most defacers likely value any accessible website as they build their reputation (Howell et al., 2019; Woo et al., 2004). Hacktivists, defacers with ideological motives, frequently direct their attention towards government and corporate websites associated with interests they oppose (Holt et al., 2020b; Romagna and van den Hout, 2017). Remarkably, hacktivists behaviors mirror those of activists in the real world; they possess more deliberate target selection and conduct attacks to both undermine disliked groups and to draw attention to their cause (Holt et al., 2019).

However, the aspect of capable guardianship within the RAT framework has received relatively little research attention in the context of website defacement. Only one study has investigated the connection between capable guardianship and defacement levels, revealing that the presence of capable guardians (measured by a country's military presence) meant less

recreational defacements against that country's websites, but did not deter politically motivated defacers (Howell et al., 2019). Consequently, there remains a considerable gap in comprehending the role of capable guardianship in the context of website defacement.

#### *4.3.5. Holidays as a Measure of Capable Guardianship*

The existing academic literature on crime and holidays primarily focuses on interpersonal physical violence, with early studies by Lester (1979, 1987a, 1987b) linking major holidays to increases in homicides due to heightened social interactions and alcohol consumption. Subsequent research extended these findings to include other violent crimes across different cultural contexts (Baird et al., 2019; Cohn & Rotton, 2003; Khurana et al., 2022a, 2022b; Kudryavtsev & Kuchakov, 2021; Rotton & Frey, 1985). However, the impact of holidays on criminal activity varies across different groups, as evidenced by studies showing differences in homicides among individuals with a history of mental illness and fewer terrorist attacks during Islamic holidays in the Middle East (Baird et al., 2009; Reese et al., 2017).

Only a couple of studies have examined economically driven crimes on holidays, revealing a decrease in property crimes attributed to increased guardianship at home during holidays when individuals are not at work (Cohen & Rotton, 2003; Lam, 2020). Lam's (2020) study further demonstrated that holidays celebrated at home had lower levels of burglaries and robberies compared to non-holiday periods and holidays celebrated outside the home. These findings highlight how holidays disrupt the typical convergence of motivated offenders, suitable targets, and capable guardians.

In addition to academic research, non-academic literature by cybersecurity professionals and journalists also supports the increase in crimes during holidays. For example, Pompon and colleagues (2018) found a surge in phishing attacks during winter holidays, corroborated by

Rodriquez & Okamura (2019), who observed increased attacks and victimization from phishing, fraud, and scams over Christmas. Moreover, a Defcon survey reported that 81% of malicious cyber actors prefer hacking during the winter holidays (Eaton, 2009), supported by substantial increases in ransomware attacks during the Christmas season (Mujezinovic, 2022; Tripwire, 2022; Wetzig, 2022). Journalists have also observed trends in website defacement incidents during the holiday season, such as the "traditional Christmas defacement spree" reported on platforms like the Zone-H website (Scwartz, 2005). However, cyber-attacks do not increase just over Christmas. Instead, governmental organizations like the US Cybersecurity & Infrastructure Security Agency and the FBI have issued warnings about increased cyber-threats during holidays in general, urging organizations to remain vigilant in their security during these periods (CISA, 2022). But what is it that makes the holidays attractive for hacking?

The consensus among government agencies, journalists, and cybersecurity professionals is that holidays leave organizations more vulnerable to cyber-attacks (Barret, 2021; CISA, 2022; Eaton, 2009; Kapko, 2022; Middleton, 2022; Sakellariadis, 2022; Sganga, 2021a, 2021b; Tung, 2021). This vulnerability arises from reduced IT staffing during holidays, limiting the ability to detect and respond to attacks promptly (Barrett, 2021; Eaton, 2009; Kapko, 2022; Middleton, 2022). Consequently, hackers have more time to escalate privileges and worsen the severity of attacks, with fewer cyber-defenders available to assemble and respond effectively (Barrett, 2021; Kapko, 2022). These observations align with the absence of capable guardianship outlined in the Routine Activities Theory framework.

In fact, businesses themselves acknowledge the impact of holidays on cybersecurity, with anonymous surveys revealing lower staffing levels and longer response times for cyber-attacks occurring during holidays (Kapko, 2022). Interestingly, larger companies experience even longer

delays, highlighting the challenges they face in mitigating cyber threats during holiday periods (Kapko, 2022). Despite this awareness, many businesses lack contingency plans to respond to cyber-attacks during holidays (Sganga, 2021b). While holidays appear evident of a lack of capable guardianship, this has yet to be expressly tested in the academic literature for any kind of hacking, let alone website defacement.

Therefore, this paper aims to address this gap by investigating the relationship between holidays and hacking volumes. By exploring this relationship, the research seeks to understand whether holidays serve as motivators for defacers to engage in cyber-offenses. Through rigorous analysis and modeling techniques, the study aims to provide valuable insights into cybercriminal behavior dynamics and the potential impact of holidays on hacking activity.

### 4.4. Current Study

The present research aims to examine how holidays influence the frequency of cyber-attacks perpetrated by website defacers. Website defacers were chosen as the focus of this study due to the wealth of data available from sources like Zone-H, whereas information on other types of hackers is limited or non-existent. Unlike many hackers who maintain a covert profile, website defacers tend to openly showcase their actions. This transparency allows for the tracking of their activities over time, a capability that is often unachievable with other hacker groups. This characteristic is particularly valuable for observing if events genuinely motivate hackers at the individual level, rather than relying solely on aggregate volumes or specific incidents as indicators of motivation or causal connections. To empirically investigate the relationship between reduced guardianship and increased cybercrime levels, the assumptions commonly held among cybersecurity experts and criminologists have been translated into the following hypotheses:

H1. Defacement levels of defacers increase in time periods corresponding to holidays.

H2. Holidays impact the defacement volumes of defacers differently, thus groups of defacers with similar characteristics will exhibit similar changes in attack volumes on holidays.

A third hypothesis that examines the effect of holidays does not stem from an assumption of a lack of capable guardianship, but rather the characteristic of the offender has been translated to the following hypothesis.

H3. There will be an increase in the volume of defacements from Middle Eastern defacers on dates corresponding to Middle Eastern holidays.

## 4.5. Methodology

### *4.5.1. Data*

The data on defacers' attack volumes is sourced from Zone-H (www.zone-h.com), a publicly accessible website renowned for compiling information about website defacement attacks reported by defacers. Established in 2002, Zone-H has gained global recognition within the defacer community and routinely receives notifications about attacks targeting websites hosted on servers worldwide (Howell et al., 2019). With over 1 million reported defacements annually, Zone-H stands as the most widely utilized platform of its kind within the defacing community (Zone-H, 2019).

When hackers successfully deface a website, they submit the relevant details to Zone-H. These reported attacks undergo verification by Zone-H through automated software before being permanently stored in their archive. Additionally, Zone-H collects supplementary information about reported defacements (Holt et al., 2020). Notably, Zone-H identifies whether an attack is launched against a significant website, which it categorizes as "special defacements." The designation of a defacement as special is determined by Zone-H administrators following its

report. Typically, these targeted websites comprise Top Level Domains, including government sites, educational institutions, and large corporations.

When defacers report a defacement on Zone-H, they are required to specify a motivation for their actions from a predefined list of options. Much of the existing research on defacement relies on this self-reported data from Zone-H to determine the content of the defacement rather than directly examining the defacement itself. This approach is favored for its simplicity and ability to handle large sample sizes. However, relying solely on self-reported data introduces potential variance in research outcomes due to several factors. Firstly, defacers retrospectively list their motivations, which may not accurately reflect the actual motives behind the defacement. Secondly, the stated motivation might not align with the limited options provided by Zone-H. In fact, Zone-H itself acknowledges the unreliability of this data, and other research studies have demonstrated the poor accuracy of this variable (Banerjee et al., 2021; Romagna & van den Hout, 2017; Zone-H). Considering these limitations, our study adopted a rigorous content analysis approach to examine defacements and construct our data on defacer characteristics. This methodology allows for a more nuanced and accurate understanding of the motivations driving defacement activities, circumventing the potential biases inherent in self-reported data.

However, the criminological literature that does use content analysis tends to be limited by analyzing only defacements written in English due to the language skills of the coders/researchers involved. This restriction narrows the scope of analysis and fails to provide a comprehensive view of the entire defacer landscape. To address this limitation, our study took a different approach by not excluding any defacer or defacement based on language. For defacements in Arabic, our coder, proficient in Arabic, personally translated each instance. For defacements in other languages, we utilized multiple online translation tools. This strategy

allowed us to capture the entirety of the defacement landscape, including hackers from various linguistic backgrounds. By adopting this inclusive approach, our study aims to provide a more thorough understanding of the motivations and characteristics of website defacers across different linguistic communities.

### *4.5.2. Sample*

The study's sample was constructed using a two-stage approach. In the first stage, a non-random sample was generated using a computer program, known as a scraper, to extract data from the Zone-H database. Initially, this extraction yielded information on 778 defacers. However, defacers were subsequently screened based on two criteria: 1). Defacer's defacement page on Zone-H had less than 50 pages, providing visibility to the beginning of the defacer's career. Due to a limitation in the Zone-H archive, which only displays 50 pages of defacements per hacker, it was impossible to determine the exact date of the first attack for those exceeding this limit, and the content of these defacements. Therefore, they were removed from the sample to capture the entirety of their criminal career. However, it's important to note that these prolific hackers are considered outliers, constituting a small portion of the defacing ecosystem and our initial sample (Burruss et al., 2021; van de Weijer et al, 2021). 2). Defacer's first defacement occurred before Feb 14th, 2019, since the initial data collection period seeking to gather the first year of activity began on February 15th, 2020. Most of the aliases were removed in this second stage. After this initial screening process, 251 defacers remained. A validation step involving cross-referencing these usernames on the Zone-H website revealed that six defacers could not be found, and one had no defacements. These seven defacers were removed from the dataset, resulting in a total of 244 defacers. Additionally, despite the restrictions, it was discovered that four defacers in the initial sample violated the 50-page assumption criterion. Consequently, the

sample was reduced to 240 defacers. Four years after the initial data collection period, on January 31st, 2024, the data was recollected to include more defacements and improve data quality. After this additional collection, the defacers were re-examined to check for compliance with the 50-page restriction, leading to the removal of 10 more defacers from the sample. This resulted in a final sample size of 230 defacers.

Due to the imposed parameters, the dataset includes defacers who commenced their activity in 2016 and before. This decision was made to prioritize a longer period for studying the onset, persistence, and desistance of offenders, while also increasing the potential number of holidays available for defacement. Importantly, the dataset was constructed longitudinally, recording the daily attack volume of defacements per defacer from their very first hack to their last reported defacement. As the Zone-H website only records individual hacks and not daily trends, the data retrieved by the scraper did not contain observations for days when no hack occurred. To address this, a Python script was developed to fill in the missing dates for each defacer and attribute them with zero hacks for that day. At the conclusion of the dataset creation process, there were 81,207 unique defacements from 230 defacers, spanning a total of 425,162 days of criminal careers.

While this dataset shares similarities with another paper written by this author (Hoffman et al., 2024), there are notable differences. Firstly, unlike the previous study where hacking volumes were collected on a weekly basis, in this dataset, hacking volumes were collected daily. This finer granularity allows for a more detailed analysis of daily variations in hacking activity. Secondly, the main dependent variable in this study is not a measure of weekly hacking prevalence but discrete count data on the number of defacements per day per defacer. This shift in the dependent variable provides a more precise measure of hacking activity at the daily level.

Thirdly, the data in this study has been structured as a longitudinal dataset rather than a perfectly balanced panel. This longitudinal structure enables the examination of changes in hacking activity over time for each defacer, providing further insights into the trajectory of their criminal behavior. Lastly, the data for each defacer extends beyond the initial one-year period to include the entirety of their reported criminal activity on Zone-H. This extended timeframe allows for a more comprehensive analysis of defacer behavior over the course of their criminal careers.

### *4.5.3. Dependent Variables*

The primary objective of this paper is to investigate the impact of holidays on the frequency of website defacement. To achieve this objective, we compiled data on every instance of defacement in each defacer's archive on the Zone-H website. This data allowed us to create a variable representing the total number of defacements occurring each day, ranging from the defacer's first recorded defacement to their most recent one. Subsequently, we derived a transformed version of this variable to gauge the hacking prevalence of defacers, indicating whether a defacer engaged in hacking activity on a given day throughout their career. Furthermore, this study examines the disparity between overall defacement levels and the frequency of special defacements, which target top-level domains. Given that these sites often belong to prominent companies and government entities, it is plausible that they receive heightened security measures during holidays compared to other websites. Therefore, we aim to assess whether the occurrence of special defacements exhibits a distinct pattern during holiday periods. A list of the dependent variables included in the final model are described below.

*Hack:* A continuous variable that signifies the total defacements per day for each individual defacer. This variable is the main dependent variable of our study.

*Did Hack:* A binary variable that signifies if a defacement occurred that day for each individual defacer. This variable is used in the initial logistic regressions in our study.

*Special:* A continuous variable that signifies the total special defacements per day for each individual defacer. This variable was created to test the difference in holiday effects between average and important websites.

*Did Special:* A binary variable that signifies if a defacement occurred that day for each individual defacer. This variable was also used in initial logistic regressions and to display differences between website categories.

### *4.5.4. Independent Variables*

**Content Analysis.** The data creation process involved a detailed examination and coding of the initial defacements for each of the 230 defacers in the sample. This examination utilized mirror images of the attacks available from the Zone-H archive. Selecting the first defacement was deemed crucial as it signifies the outset of their criminal careers. While conducting manual coding for all defacements would have provided deeper insights into potential turning points in a defacer's career, it was not feasible due to the sheer volume of defacements, which totaled over 81,000.

Focusing on the first defacement as the starting point for analysis was deemed appropriate as it marks the commencement of each defacer's criminal activity and serves as a consistent reference point for studying their hacking careers. However, considering alternative approaches, such as monthly sampling of content, could be beneficial for future research endeavors. This sampling method could help identify potential turning points in defacer careers while managing the extensive volume of data more effectively.

As previously mentioned, the coding process for the variables describing defacer characteristics was conducted qualitatively by analyzing the image content of the defacements. To ensure the reliability of this data creation process, we employed an interrater reliability metric. The scores obtained ranged from 85% to 100% for each variable. Below, a more detailed description of each of the variables created from the defacement content can be found.

*Ideological:* A binary variable signifying whether a defacer appears to be politically or religiously motivated from the content of their first defacements.

*Middle East:* A binary variable signifying whether a defacer appears to be Middle Eastern from the content of their first defacements.

*Team:* A binary variable signifying whether a defacer appears to be a member of a hacking team from the content of their first defacements, which was determined by mentioning their team in the defacement content, a common practice among defacers (Hoffman et al., 2024). Team membership displays involvement in the hacking community, commitment to a lifestyle of cyber-crime, and generally a higher skill level (Balduzzi et al., 2018; Maggi et al 2018).

**Variation in Defacer Careers.** One of the key objectives of this research was to address differences in the careers of the defacers in our sample, which encompassed a wide range of start dates and career lengths. Understanding this variation was pivotal in uncovering the true effect of holidays on defacement levels. Thus, an essential initial step in our investigation was to explore the diversity and patterns of criminal careers among the defacers in our dataset. To achieve this, we developed a range of variables to create graphs to visualize the variation in career behaviors exhibited by the defacers. Below, we present a selection of the graphs created during our analysis to illustrate the significance of controlling for career variation. In doing so, we aim to display the

importance of controlling for these career differences and to underscore the need for further research into the criminal careers of website defacers.

**Figure 3.1. Career Defacements**

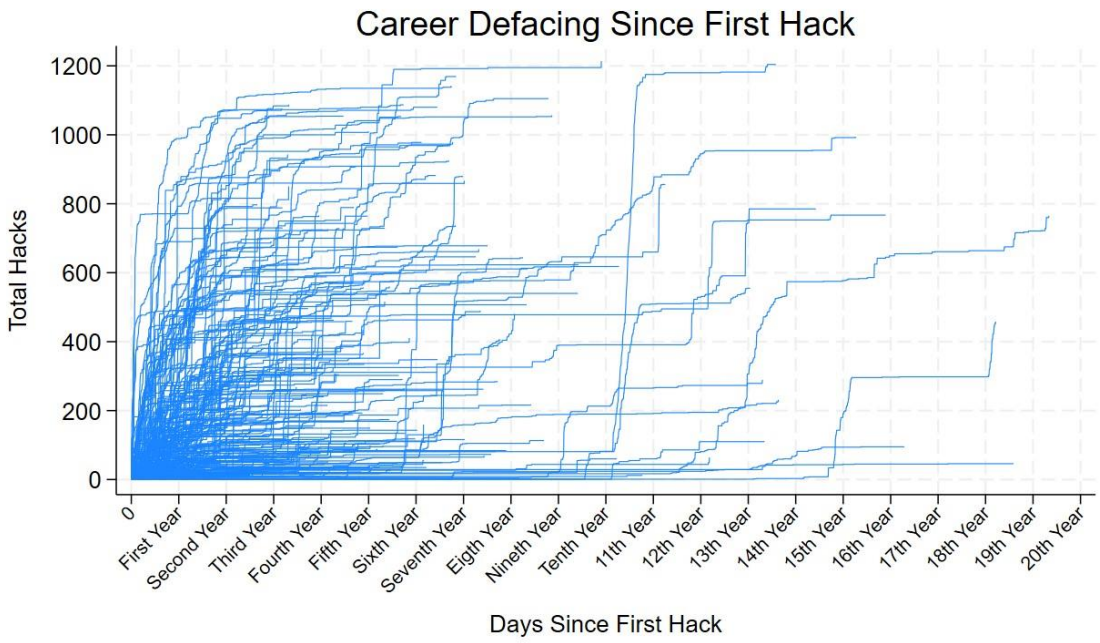
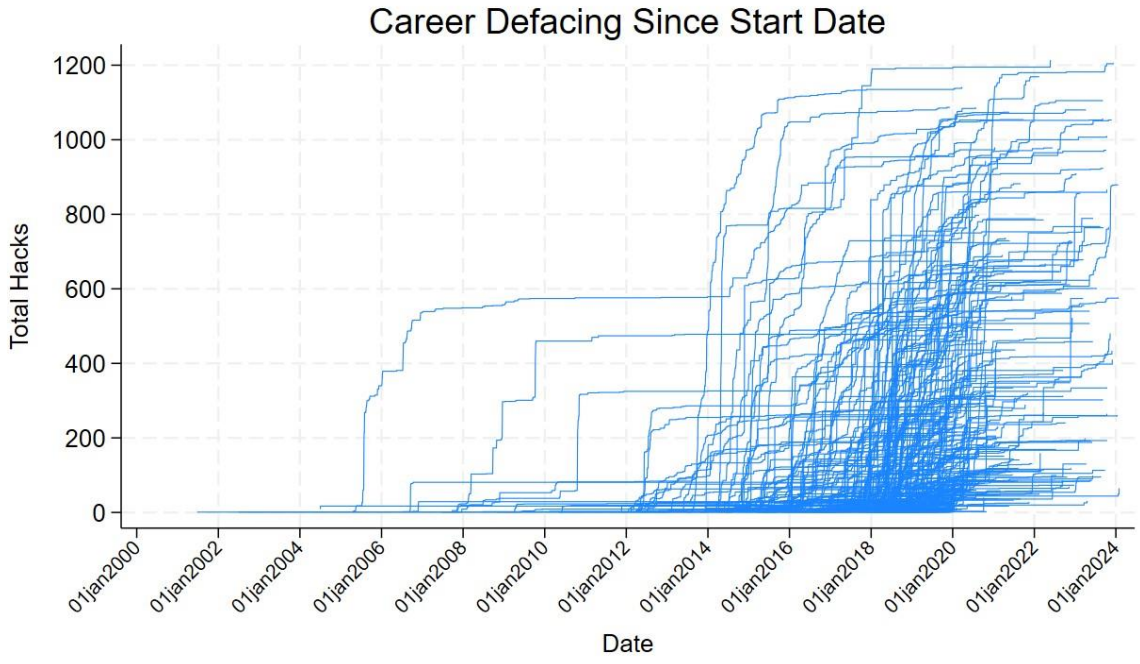



**Figure 3.2. Defacer Careers**



As depicted in Figure 1 and Figure 2, the trajectories of defacer careers exhibit significant variability. While overarching trends are discernible, indicated by denser areas of blue, there is notable divergence among individual defacers. Indeed, the shapes of defacer careers appear to be as diverse as their underlying motivations, with some initiating prolific and high-volume activities from the outset, while others gradually escalate over time or remain relatively inactive. Moreover, a closer examination of the horizontal lines reveals instances where defacers intermittently cease their offending behavior, interspersed with periods of sustained activity. This variability underscores the complexity of criminal careers among website defacers and underscores the importance of accounting for these differences when analyzing defacement behaviors. While our paper does not delve deeply into the analysis of criminal careers among website defacers, these visualizations highlight the necessity of controlling for such variations in understanding defacement behaviors. We hope that these findings will serve as a valuable contribution to the field and inspire further research in this area. Below, we outline the additional variables created to account for the diversity among defacers in their criminal tendencies and the trajectories of their criminal careers.

*Start Date:* Denotes the date of each defacer's first reported defacement. This variable adjusts for differences in the start dates of defacers. The earliest start date in our data was June 29th, 2001, while the latest start date was February 7th 2019.

*Days Since Hack1:* Measures the total number of days that have elapsed in the defacer's career for every observation within that defacer. For example, the observation measuring the day after their first attack would have a 1 for this variable, the next observation a 2, and so forth until the end of their career. This adjusts for the length of time defacers have been active offenders for each defacement.

*Tally*: A continuous variable measuring a "rolling count" of the total defacements a defacer has committed since their first active day. This variable helps adjust for differences in offending between defacers.

*Holiday Hack Tally:* A continuous variable that measures the total defacements that a defacer has committed on holidays since their first active day. This variable was made to adjust for the defacers who may have hacked on holidays previously from those who have not or in smaller numbers.

*No Hack Tally:* A continuous variable measuring a "rolling count" of the total days a defacer has not defaced since their first active day. This variable helps adjust for differences in offending between defacers who may spend loner periods between defacements.

*Hack Average:* a variable that measures the total number of defacements per hacker, divided by their length of career. This variable was created to control for defacers with more "time efficient offending behavior" and those who may be "prolific offenders."

*Holiday Count:* Measures a rolling count of the total number of holidays that have passed in a defacer's career. This variable was made to control for the opportunity that defacers had to hack on holidays as well as the time to learn if holidays presented opportunities for defacement.

*Big Gap:* A binary variable that measures if the observation for a defacer falls in an unusually long period of inactivity. Descriptive analysis showed that only 1% of gaps between offending were longer than 87 days, as such this variable denoted a big gap as a period of inactivity 88 days or longer. This variable measures differences in observations that may represent periods of lack of motivation or other unknown factors. Regardless of why defacers desist from offending for long periods, the daily observations within a "big gap" are different from those that do not fall within such a period.

**Holidays.** The main independent variable of interest are the variables measuring holidays. As mentioned, the holiday variable is being used to measure a lack of capable guardianship. However, it is essential to discuss the rationale behind using holidays as proxies for a lack of capable guardianship, as this decision involves using one variable to approximate another omitted variable. Ideally, we would have direct measures of guardianship for each website, such as the number and proficiency of IT staff present on any given day. However, obtaining such detailed data is highly impractical, if not impossible. Consequently, holidays serve as the most feasible proxy variable for gauging the potential decrease in capable guardianship.

As discussed, holidays are expected to coincide with a reduction in IT staff availability, thus resulting in decreased guardianship. However, it is crucial to acknowledge that this proxy variable is not perfect. While holidays generally align with decreased guardianship, the extent of this effect varies. Not every website experiences a complete absence of IT staff, and the reduction in staffing levels may vary among different organizations. Some may even choose not to reduce their IT staffing during holidays. Therefore, while the holiday variable is positively correlated with decreased guardianship, its effect is attenuated by these errors in measurement. This attenuation results in a smaller magnitude of effect for the holiday variable compared to a direct measure of guardianship. Consequently, the coefficients in our regression models may be smaller due to the use of this proxy variable.

*Holiday:* A binary variable detailing if the day observation is a holiday or not. Holidays included in this variable are Christmas, New Years, US Independence Day, Yom Kippur, Rosh Hashanah, Eid Al-Fitr, Labor day, Thanksgiving, start of Ramadan, and Eid Al-Adha. Each holiday also has its own separate variable.

### 4.6. Analytic Strategy

Our analysis utilized a multilevel model (MLM) to effectively control for various factors that could influence the impact of holidays on website defacement levels. MLM, also referred to as hierarchical or mixed-effects models, is a robust statistical technique designed for data exhibiting a hierarchical or nested structure, such as hacking events nested within individual defacers (Bryk & Raudenbush, 1988; Goldstein, 2011; Gordon, 2019; Nezlek, 2020; Preacher, 2021; Raudenbush & Bryk, 2002). This modeling approach enables estimation of predictor variable effects at both within-defacer and between-defacer levels, offering more accurate estimates and accounting for observations clustered within defacers by assigning each defacer its own random intercept in the regression model (Bryk & Raudenbush, 1988; Gelman & Hill, 2006; Luo et al., 2021; Preacher, 2021; Rasbash, 2023; Snijders & Bosker, 2012).

Therefore, based on the structure of our data and research goals, we opted for an MLM with random intercepts for hacker IDs while controlling for time using separate time-related variables in the regression. This approach provides not only a robust and comprehensive approach to analyzing the complex structure of hacking incident data, but also provides flexibility in modeling the effects of time while simultaneously accounting for the clustering of hacking incidents within defacers, leading to a more comprehensive understanding of the factors influencing hacking activity.

Incorporating random intercepts for hacker IDs allows the MLM to account for the hierarchical structure of the data and the clustering of hacking incidents within individual defacers. This ensures appropriate adjustment for the correlated nature of observations within defacers, leading to more accurate parameter estimates and reliable inference (Bryk & Raudenbush, 1988; Rasbash, 2023; Raudenbush et al., 2003). Additionally, controlling for time

effects with separate time-related variables in the regression model enables explicit modeling of temporal patterns and trends in hacking activity, capturing nuances such as seasonality and long-term trends (Gordon, 2019; Singer & Willett, 2003). While some may ask why we did not add a third level to the model by nesting time within defacers, as is typical in much MLM research, our data did not have an easy third level structure. Such models require data where individuals have many observations per day, such as in dairy research and "beeper studies" (Nezlek, 2020). Additionally, such models require substantially larger data sizes for reliable estimates, lengthy convergence times, and lack flexibility in modeling the effects of time-related variables, which in our case extend beyond individual days (Holodinsky et al., 2020; Gordon, 2019).

Furthermore, employing MLMs with random intercepts for hacker IDs and time-controlled regression models offers several advantages over using clustered standard errors alone. Clustered standard errors can adjust for the clustering of observations within defacers but do not explicitly model the hierarchical structure of the data (Bickel & Levina, 2008; Gelman, 2007; Singer & Willett, 2003). Consequently, models using clustered standard errors may produce biased results, particularly with unequal sample sizes between clusters, as observed in our data on hacker careers (Bickel & Levina, 2008; Gelman, 2007; Holodinsky et al., 2020; Singer & Willett, 2003). Moreover, neglecting hierarchical structures within the data can lead to underestimated standard errors, potentially inflating statistical significance (Holodinsky et al., 2020; Singer & Willett, 2003).

Therefore, an MLM with random intercepts for hacker IDs offers a sophisticated, powerful, and flexible approach for analyzing the complex structure of hacking incident data. It allows for the estimation of both within-defacer and between-defacer variability, as well as the simultaneous modeling of time effects, leading to more reliable and interpretable results (Bryk &

Raudenbush, 1988; Goldstein, 2011; Holodinsky et al., 2020; Rasbash, 2023; Raudenbush & Bryk, 2002). For our research, we employed MLMs for both logistic and negative binomial regression models to understand more about the volume and chance of defacement attacks on holidays. While both models were used to measure the effect of all holidays and individual holidays, the negative binomial regression model was utilized alongside a sensitivity analysis with restrictions for defacers on teams, individuals classified as ideological defacers, defacers who revealed themselves as Middle Eastern, and for defacers who were none of the previous three classes (labeled as unaffiliated). This analysis of separate groups within our sample can also be viewed as a random slope approach for these characteristics. Lastly, as mentioned, this research examines differences between defacement levels at large and the levels of special defacements across all models.

Because of the aims of the research, the paper prioritizes a negative binomial distribution model for four reasons. First, as we are primarily concerned with whether defacement volumes increase on holidays, these models are useful for testing the relationship between variables when the dependent variable contains skewed count data, which the number of hacks per day is. Second, these regressions assume that the dependent variable exhibits a known specific interval of time, in this case, days. Thirdly, negative binomial regressions also require that the probability of events are independent from each other, the likelihood of one hacker defacing a website is independent of others defacing a website given the millions of potential targets. Lastly, as our data is over—dispersed (variance greater than the mean) negative binomial models are better suited to analyze our data. While Poisson models require variance relatively equal to the mean, negative binomial models were designed to handle overdispersion.

Given the nature of our data, we conducted a series of rigorous tests to ensure the robustness of our analysis. Firstly, we performed an autocorrelation test using both the Durbin-Watson and Cumby-Huizinga tests to assess whether time series regressions were appropriate. The results of these tests indicated that we could not reject the null hypotheses of no autocorrelation.

Secondly, we explored time-dependent effects by graphing the frequencies of defacement incidents during months containing holidays. Our objective was to identify any noticeable spikes occurring on holidays and assess whether there were increased levels of defacement leading up to or lagging behind holidays, which might necessitate the use of leads or lags in our analysis. Throughout all the months containing holidays, we did not observe any significant increases leading to or lagging behind holidays. Consequently, we did not include the use of leads and lags in our analysis. Additionally, we examined the potential effect of the US holiday season (Thanksgiving to New Years) as a potentially cyclical pattern. However, we found no evidence of such an effect, and thus, we did not control for it in our models. Nonetheless, we examined the effect of multiday holiday periods to address any leads and lags, and found no further evidence for an effect. Regardless, we included monthly variables to control for any potential seasonality effects.

Thirdly, we assessed the presence of multicollinearity among predictor variables by calculating variance inflation factors (VIFs). The purpose was to determine whether any independent variables were correlated with others in the model. The results of this test indicated a lack of multicollinearity, with an overall mean VIF of 1.07. These rigorous tests ensure the reliability and validity of our analysis, providing confidence in the conclusions drawn from our research.

Thus, the generalized final models for the regressions are below:

Logistic Regressions:

$$\text{logit}(P(Yij=1)) = \beta 0 + \beta 1\text{Hack}ij + \beta 2\text{Christmas}ij + \beta 3\text{Team*Christmas}ij + \beta 4\text{NewYears}ij + \beta 5\text{IndependenceDay}ij + \beta 6\text{YomKippur}ij + \beta 7\text{RoshHashanah}ij + \beta 8\text{EidAlFitr}ij + \beta 9\text{LaborDay}ij + \beta 10\text{Thanksgiving}ij + \beta 11\text{RamadanStart}ij + \beta 12\text{EidAlAdha}ij + \beta 13\text{Ideological}ij + \beta 14\text{Team}ij + \beta 15\text{MiddleEast}ij + \beta 16\text{Startdate}ij + \beta 17\text{DaysSinceHack1}ij + \beta 18\text{HolidayHackTally}ij + \beta 19\text{Tally}ij + \beta 20\text{NoHackTally}ij + \beta 21\text{HackAvg}ij + \beta 22\text{HolidayCount}ij + \beta 23\text{BigGapNoMiss}ij + \sum k=14 \gamma k\,\text{MonthOfWeekdate}ij,k + \sum l=114 \delta l\,\text{YearOfWeekdate}ij,l + u0j$$

Negative Binomial Regressions:

$$\log(\mu ij) = \beta 0 + \beta 1\text{Hack/Special}ij + \beta 2\text{Christmas}ij + \beta 3\text{Team*Christmas}ij + \beta 4\text{NewYears}ij + \beta 5\text{IndependenceDay}ij + \beta 6\text{YomKippur}ij + \beta 7\text{RoshHashanah}ij + \beta 8\text{EidAlFitr}ij + \beta 9\text{LaborDay}ij + \beta 10\text{Thanksgiving}ij + \beta 11\text{RamadanStart}ij + \beta 12\text{EidAlAdha}ij + \beta 13\text{Ideological}ij + \beta 14\text{Team}ij + \beta 15\text{MiddleEast}ij + \beta 16\text{Startdate}ij + \beta 17\text{DaysSinceHack1}ij + \beta 18\text{HolidayHackTally}ij + \beta 19\text{Tally}ij + \beta 20\text{NoHackTally}ij + \beta 21\text{HackAverage}ij + \beta 22\text{HolidayCount}ij + \beta 23\text{BigGap}ij + \sum k=14 \gamma k\,\text{MonthOfWeekdate}ij,k + \sum l=114 \delta l\,\text{YearOfWeekdate}ij,l + u0j + vij$$

Where:

- $\mu ij$ is the expected count of website defacements for defacer $j$ on day $i$.
- $P(Yij=1)$ is the probability of a successful website defacement for defacer $j$ on day $i$.
- $\beta 0, \beta 1, \ldots$, are the coefficients associated with the respective predictor variables.
- $\gamma k$ and $\delta l$ are coefficients associated with the month and year indicators, respectively.
- $u_{0j}$ represents the random intercept for each defacer $j$.
- $vij$ represents the random error term at the observation level.
- Individual holidays are replaced with $\beta\text{Holiday}ij$ when testing the overall holiday effect.

The negative binomial regression represents the relationship between the predictors (such as hack events, holidays, defacer characteristics, and temporal factors) and the expected count of website defacements, while the logistic regression displays the relationship between the same predictors and the log-odds of a successful website defacement that day. Additionally, both models account for both within-defacer and between-defacer variability. The models include fixed effects for the predictor variables, random intercepts for each defacer, and categorical indicators for months and years.

### *4.6.1. A Note on Model Building*

Our research process underwent a rigorous model building procedure aimed at ensuring the validity and robustness of our analyses. Following the methodology outlined by multi-level modeling from the Centre for Multilevel Modelling and adhering to best practices, we conducted an exhaustive examination of various model specifications (Leckie, 2010; Rabe-Hesketh & Skrondol, 2008). This involved testing models with different configurations, including those with random intercepts, random slopes, and combinations of both for each variable in the model. By systematically introducing variables into the model, starting with a base model containing only the dependent variable and no independent variables, we aimed to capture the nuanced dynamics of website defacement behavior and elucidate the relationships between predictor variables.

Throughout this iterative process, we carefully assessed the presence of shared variance among predictor variables and scrutinized the relationships between them to detect any instances of multicollinearity or overlapping effects. Our objective was to create final models that accurately represented the complexities of the data while ensuring the interpretability and reliability of the results. While the detailed results of these intermediate models were not displayed in the final analysis due to the large volume of tables, they played a crucial role in

guiding the development and refinement of our final models. By systematically refining our models based on the insights gleaned from these intermediate analyses, we ensured the appropriateness and robustness of our final models for investigating the factors influencing website defacement behavior.

In addition to exploring various model configurations with random intercepts and slopes, we also considered including cubic and squared versions of the dependent variables to capture potential non-linear relationships. However, after thorough testing and evaluation, we found that the standard daily hack volume variable provided the most parsimonious and interpretable representation of the data, supported by statistical tests and model diagnostics. Consequently, we opted not to include the cubic and squared versions in our final models.

One notable finding from our model building process was the detection of some shared variance across variables in the final models, particularly between the predictor variable representing Christmas and its interaction term with team membership. As anticipated, interaction terms inherently capture shared variance, and in our analysis, the significance and magnitude of the Christmas variable diminished once the interaction term was introduced. This underscores the intricate interplay between hacking occurrences on Christmas and team membership, highlighting the nuanced factors influencing defacement levels during specific holidays is not solely attributable to the holiday itself.

Furthermore, we conducted analyses to assess the impact of removing variables representing years and months from the model. Our objective was to evaluate the covariance of months with holidays and ascertain whether previously undetected seasonality influenced our results. Interestingly, our findings revealed no significant differences in the magnitude or direction of the results after removing these variables. This suggests that the lack of seasonality

in our model may contribute to the stability of our findings and reinforces the robustness of our analytical approach.

Overall, our rigorous model building process involved careful consideration of variable relationships, detection of shared variance, and sensitivity analyses to ensure the reliability and validity of our results. These methodological steps contribute to the integrity of our findings and enhance the credibility of our research outcomes.

## 4.7. Results

### *4.7.1. Descriptive Statistics*

Table 4.1 presents descriptive statistics for the variables analyzed in our study. It is important to note that many of these variables represent a "rolling count" since a defacer's first hack. Traditional methods for calculating descriptive statistics may yield skewed results due to the repeated and varying values within defacers' careers, as well as the potential skewing effect of observations from defacers with longer careers. Therefore, variables capturing career effects were measured at the culmination of each defacer's career to present a clearer picture of the variation in career trajectories.

As indicated by these statistics, the careers of defacers exhibit significant variability. Particularly noteworthy is the wide range of career lengths among defacers. While the start date variable accounts for right-handed censoring in the data, some defacers had notably shorter careers than the minimum possible career length of almost five years, as determined by our sampling procedure. Furthermore, this variation in career length, as expected, drastically changes other time dependent features such as the average hacks per day of a defacer and the number of holidays that a defacer remains an active offender. Furthermore, it is crucial to acknowledge the importance of controlling for extended gaps in offending behavior, given the substantial

proportion of days in defacers' careers occupied by such gaps. While fewer than 1% of these gaps in offending lasted nearly three months, many defacers, especially those with longer careers, experienced extended periods of inactivity. Although not a primary focus of this research, further investigation into the factors influencing defacers' decisions to refrain from hacking for prolonged periods could enhance our understanding of hacker criminal careers.

The descriptive characteristics of the defacers in our sample also exhibit notable variation. For instance, over 16% of defacers displayed ideological motivations based on the content of their defacements, consistent with findings from similar studies. Additionally, approximately 40% of defacers were affiliated with hacking teams, providing them with opportunities to learn from others involved in cybercrimes. Lastly, close to 20% of defacers self-identified as being of Middle Eastern origin, as evidenced by the content of their defacements. These statistics offer insight into the diverse profiles of defacers included in our study.

**Table 4.1. Descriptive Statistics.**

*Descriptive Statistics*

| Variable | Mean | SD | Min | Max |
|---|---|---|---|---|
| **Defacer Characteristics** | | | | |
| Ideological | .165 | .372 | 0 | 1 |
| Team | .400 | .491 | 0 | 1 |
| Middle East | .196 | .398 | 0 | 1 |
| **Career Differences** | | | | |
| Career Length (days) | 1839.532 | 1210.726 | 239 | 7057 |
| Hacking Average | .226 | .230 | .002 | 1.544 |
| Holidays Elapsed | 58.446 | 37.409 | 7 | 204 |
| Non-Hacking Days | 1781.148 | 1189.271 | 209 | 6895 |
| Big Gap Period? | .684 | .465 | 0 | 1 |
| **Hacking Differences** | | | | |
| Hack Total (by day) | .191 | 2.486 | 0 | 386 |
| Total Career Hacks | 351.048 | 324.470 | 2 | 1219 |
| Any Hacks? (by day) | .035 | .187 | 0 | 1 |
| Special Total (by day) | .012 | .612 | 0 | 186 |

**Table 4.1. Descriptive Statistics. (continued)**

| | | | | |
|---|---|---|---|---|
| Total Career Special | 21.983 | 57.879 | 0 | 575 |
| Any Special? (by day) | .003 | .059 | 0 | 1 |
| Total Hacks on Holidays | 9.841 | 18.505 | 0 | 143 |
| Total Special Hacks on Holidays | .174 | .472 | 0 | 4 |
| **Holiday Differences** | | | | |
| Holiday | .027 | | 0 | 1 |
| Non-Holiday | .973 | | 0 | 1 |

*Note*. n = 230. The means of binary variables can be imagined as percentages (ex. 97.3% of days in the data are not holidays).

### *4.7.2. Bivariate Correlation*

Table 4.2 displays the bivariate correlation matrix for the independent variables analyzed in our study. The results reveal that most pairs of variables exhibit weak correlations, although many reach strong levels of statistical significance. This pattern primarily arises from the relationships among time-dependent variables, such as start date and the number of holidays elapsed during a defacer's career, where longer careers correspond to more potential holidays for hacking.

Among the significant correlations, the strongest relationship is observed between higher total career hacks and the propensity to hack on holidays, as well as higher averages of hacking incidents per day and the likelihood of attacking on holidays. Another noteworthy finding is the correlation between ideological content and Middle Eastern defacers (0.3405), indicating that many Middle Eastern defacers also exhibit ideological motivations for their actions. Overall, the bivariate correlation table provides valuable insights into the associations between the variables, shedding light on the interrelationships among different aspects of defacement behavior.

**Table 4.2. Bivariate Correlation Table**

| | Variable Name | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Holiday | — | | | | | | | | | | | |
| 2 | Ideolog-ical | .001 | — | | | | | | | | | | |
| 3 | Team | -.001 | .060* | — | | | | | | | | | |
| 4 | Middle East | .001 | .341* | -.075* | — | | | | | | | | |
| 5 | Start Date | .001 | .099* | .280* | .068* | — | | | | | | | |
| 6 | Days Since Hack 1 | -.001 | -.091* | -.163* | .005* | -.628* | — | | | | | | |
| 7 | Holiday Hack Tally | .000 | .034* | .102* | -.018* | .118* | .109* | — | | | | | |
| 8 | Tally | .001 | .011* | .064* | -.052* | .073* | . 259* | .543* | — | | | | |
| 9 | No Hack Tally | -.001 | -.092* | -.168* | .008* | -.639* | .999* | .088 | .223* | — | | | |
| 10 | Hack Average | -.000 | .101* | -.057* | -.057* | .338* | -.202* | -.392* | -.600* | -.227* | — | | |
| 11 | Holiday Count | .002 | -.065* | -.119* | -.001 | -.524* | .937* | .445* | .403* | .929* | -.059* | — | |
| 12 | Big Gap | .001 | .009* | -.074* | .038* | -.222* | .247* | -.064* | -.105* | .254* | -.335* | .206* | — |

*Note*. n = 230, *$p < .01$.

### *4.7.3. Regression Analysis*

In the final stage of our analysis, we employed multi-level regression models to assess the impact of holidays on defacement levels. Additionally, to explore potential interaction effects between team membership and major holidays, we included a multiplicative interaction term between Team and Christmas. We hypothesized that hackers who are members of teams might demonstrate greater dedication to hacking, potentially spending more time on their computers during holidays or benefiting from shared knowledge within their group regarding the impact of holidays on guardianship. As outlined in the analytic strategy section, we incorporated multiple time-based variables to control for trends and seasonality within the data. Although we simplified the tables presented in the text by omitting results for the variables measuring the effect of each month and year, we provided the variance of the random intercepts in the table, labeled as var(_cons[notifierx]), where notifierx represents the unique identifiers for each hacker. The complete results from the time-based variables, along with additional regression output, are available in the appendix where comprehensive tables are provided.

We employed both logistic regression (logit) and negative binomial multilevel models (MLMs) to thoroughly investigate various aspects of the data. Logistic regression, commonly used for analyzing binary outcome variables, allowed us to examine the likelihood of defacers engaging in hacking activities on holidays compared to non-holidays, while controlling for relevant covariates. This approach enabled us to understand the factors influencing the chance of defacement attacks during holiday periods. These models usually would display fewer observations than the following models as our Big Gap variable and one year in the data perfectly predicted negative outcomes. Rather than remove these variables from the analysis, we used the “asis” option to retain these observations. While this can introduce numerical instability,

comparing this model to logistic regressions without the option and without the variables in question yielded nearly identical results. Thus, we can be confident in the reliability of the results. Furthermore, we utilized negative binomial MLMs to explore the volume or frequency of hacking incidents, accounting for the overdispersion commonly observed in count data of defacement attacks. By incorporating negative binomial MLMs, we could investigate the factors associated with variations in the volume of hacking incidents across different defacers and time periods. This approach provided insights into the underlying mechanisms driving the frequency of defacement attacks, specifically evaluating whether holidays play a significant role, while considering the hierarchical nature of the data and the potential clustering of observations within individual defacers.

By combining these complementary analytical methods, we aimed to provide a more nuanced understanding of cybersecurity threats, uncovering the complex dynamics of hacking activity and identifying factors that shape both the likelihood and intensity of defacement attacks. This integrated approach enhances our ability to develop effective strategies for mitigating cyber risks and safeguarding digital assets against malicious activities.

**Logistic Regressions.** Starting with a model utilizing only the aggregated holiday variable, the results indicate that, for both all hacks and special defacements, the relationship with holidays is not statistically significant. Interestingly, none of the variables in the special defacement model exhibited statistical significance, including those related to various aspects of defacers' careers. However, when considering all defacements, the average hack variable was found to be significant for both defacement groups. This outcome is expected, given its association with the overall number of hacks.

Variables such as No Hack Tally and Holiday Hack Tally primarily served as controls for defacers with more prolific careers. Nonetheless, the significant finding that the number of holidays elapsed in a career correlates with an increase in defacements, while the number of hacks on holidays is associated with a decrease in defacement, is intriguing. While the effect of holidays elapsed may be a result of a longer career, perhaps defacers who have hacked on a holiday learned they would rather spend these days celebrating. Regardless of this speculation, these results may present opportunities for future research into the dynamics of defacer careers and the factors influencing hacking behaviors, particularly in relation to holiday periods.

**Table 4.3. Logistic, Overall Holiday Effect**

| VARIABLES | (1)<br>Did hack? | (2)<br>Did special? |
|---|---|---|
| Holiday | -0.0396 | -0.0667 |
| | (0.0541) | (0.166) |
| Ideological | 0.0879 | -0.0946 |
| | (0.0967) | (0.319) |
| Team | -0.100 | -0.326 |
| | (0.0710) | (0.229) |
| Middle East | -0.153* | -0.440 |
| | (0.0923) | (0.305) |
| Start Date | -0.000767 | 0.00229 |
| | (0.000990) | (0.00304) |
| Days Since Hack1 | -0.00156 | 0.00221 |
| | (0.00122) | (0.00383) |
| Holiday Hack Tally | -0.0351*** | -0.0275 |
| | (0.0110) | (0.0335) |
| Tally | -0.000882*** | -0.000205 |
| | (0.000122) | (0.000403) |
| No Hack Tally | -7.90e-05 | -0.000752 |
| | (0.000794) | (0.00257) |
| Hack Average | 1.613*** | -0.0508 |
| | (0.158) | (0.517) |
| Holiday Count | 0.0391*** | 0.0359 |
| | (0.0113) | (0.0344) |
| Big Gap | -54.70 | -20.44 |
| | (0) | (0) |

**Table 4.3. Logistic, Overall Holiday Effect (continued)**

| | | |
|---|---|---|
| var(_cons[notifierx]) | 0.224*** | 2.193*** |
| | (0.0260) | (0.309) |
| Constant | 28.62 | -53.48 |
| | (0) | (0) |
| Observations | 425,162 | 425,162 |
| Number of groups | 230 | 230 |

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

Testing the effect of various holidays independently reveals significant findings for certain holidays. Labor Day, for instance, significantly increased the likelihood of special defacements. Conversely, Eid al-Fitr was associated with a slight decrease in the likelihood of all defacement attacks. Notably, variables measuring career differences were not significant for special defacements. However, when considering all hacks, most of these variables exhibited significance. Overall, the results of the logistic regressions lend partial support to our first hypothesis that holidays increase defacement levels.

**Table 4.4. Logistic, Individual Holidays**

| VARIABLES | (1)<br>Did hack? | (2)<br>Did special? |
|---|---|---|
| Christmas | 0.0232 | -0.918 |
| | (0.220) | (1.013) |
| Team*Christmas | -0.190 | 0.490 |
| | (0.340) | (1.428) |
| New Years | -0.136 | -1.318 |
| | (0.173) | (1.011) |
| Independence Day | -0.00655 | -0.233 |
| | (0.173) | (0.595) |
| Yom Kippur | -0.217 | -0.206 |
| | (0.183) | (0.591) |
| Rosh Hashanah | 0.200 | -0.00509 |
| | (0.156) | (0.517) |
| Eid al-Fitr | -0.445** | -0.921 |
| | (0.194) | (0.717) |

**Table 4.4. Logistic, Individual Holidays (continued)**

| | | |
|---|---|---|
| Labor Day | 0.225 | 1.197*** |
| | (0.152) | (0.310) |
| Thanksgiving | -0.0348 | 0.244 |
| | (0.174) | (0.432) |
| Ramadan start | -0.0806 | -0.921 |
| | (0.165) | (0.717) |
| Eid al-Adha | 0.183 | -0.125 |
| | (0.156) | (0.512) |
| Ideological | 0.0905 | -0.0981 |
| | (0.0923) | (0.319) |
| Team | -0.116* | -0.323 |
| | (0.0677) | (0.229) |
| Middle East | -0.150* | -0.438 |
| | (0.0881) | (0.305) |
| Start Date | -0.000929 | 0.00288 |
| | (0.00100) | (0.00308) |
| Days Since Hack1 | 0.00386*** | 0.00286 |
| | (0.00123) | (0.00387) |
| Holiday Hack Tally | -0.00962 | -0.0330 |
| | (0.0109) | (0.0336) |
| Tally | -0.00165*** | -0.000215 |
| | (0.000122) | (0.000403) |
| No Hack Tally | -0.00496*** | -0.000978 |
| | (0.000788) | (0.00257) |
| Hack Average | 1.670*** | -0.0486 |
| | (0.151) | (0.517) |
| Holiday Count | 0.0128 | 0.0416 |
| | (0.0112) | (0.0345) |
| Big Gap | -70.24 | -22.26 |
| | (0) | (0) |
| var(_cons[notifierx]) | 0.201*** | 2.189*** |
| | (0.0234) | (0.308) |
| Constant | 27.42 | -62.25 |
| | (0) | (0) |
| Observations | 425,162 | 425,162 |
| Number of groups | 230 | 230 |

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

**Negative Binomial Regressions.** Similar to the logistic regressions displaying the chance of hacking on holidays, we use negative binomial multi-level models to display the increase and decrease in the volume of attacks on holidays. While the logistic regressions help provide an initial analysis, the following models help answer the research question on the effect of holidays on the volume of defacements.

However, the results of the model utilizing the aggregated holiday variable show no statistically significant relationship between holidays and the volume of attacks, whether targeting all websites or top-level domains specifically. Interestingly, being a member of a hacking team or being of Middle Eastern origin was associated with slightly lower volumes of attacks. Among the variables measuring aspects of defacers' careers, the average number of hacks was significant for all defacements but not special ones. This finding is expected given its correlation with the overall number of hacks and the lower likelihood of defacing a top-level domain. These variables, along with others such as the number of days since the first hack, serve as controls for defacers with more prolific careers. Overall, these results suggest that while individual characteristics of defacers may influence attack volumes, there is no clear evidence of a relationship between holidays and the volume of defacements.

**Table 4.5. Negative Binomial, Overall Holiday Effect**

| VARIABLES | (1)<br>hack | (2)<br>special |
|---|---|---|
| Holiday | -0.00804 | -0.0963 |
| | (0.0815) | (0.249) |
| Ideological | 0.140 | -0.248 |
| | (0.104) | (0.421) |
| Team | -0.140* | -0.279 |
| | (0.0760) | (0.304) |
| Middle East | -0.172* | -0.612 |
| | (0.0991) | (0.403) |
| Start Date | 0.00179 | -0.00143 |
| | (0.00152) | (0.00437) |

**Table 4.5. Negative Binomial, Overall Holiday Effect (continued)**

| | | |
|---|---|---|
| Days Since Hack1 | -0.00687*** | -0.0109** |
| | (0.00186) | (0.00550) |
| Holiday Hack Tally | -0.0202 | -0.0342 |
| | (0.0162) | (0.0507) |
| Tally | 0.000121 | 0.000861 |
| | (0.000181) | (0.000558) |
| No Hack Tally | 0.00815*** | 0.00843** |
| | (0.00116) | (0.00369) |
| Hack Average | 2.710*** | 0.285 |
| | (0.184) | (0.690) |
| Holiday Count | 0.0274* | 0.0442 |
| | (0.0166) | (0.0518) |
| Big Gap | -28.86 | -41.96 |
| | (4,083) | (9.953e+06) |
| Constant | -27.52 | 0.422 |
| | (23.21) | (0) |
| var(_cons[notifierx]) | 0.231*** | 3.874*** |
| | (0.0307) | (0.534) |
| Observations | 425,162 | 425,162 |
| Number of groups | 230 | 230 |

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

The results of testing the effect of various holidays separately reveal significant effects on defacement levels. Firstly, while Christmas alone did not show a significant effect, the interaction between Christmas and team membership had a notable positive effect (b = 1.297) on the level of defacements, but not special defacements. Labor Day was found to positively influence both overall defacement totals (b = 0.457) and special defacement totals (b = 1.818), with a particularly pronounced effect on the latter. Interestingly, these were the only holidays to have a positive influence on hacking totals. Conversely, Yom Kippur (b = -0.493), Eid al-Fitr (b = -0.781), and Thanksgiving (b = -0.428) were associated with decreases in general defacement levels. New Years (b = -2.091) and the start of Ramadan (b = -2.065) had particularly strong negative impacts on the levels of special defacements. These findings suggest that different holidays may have varying effects on hacking activity, highlighting the importance of

considering each holiday individually in analyzing cybercrime patterns, and provides partial support of our first hypothesis that defacement levels increase on holidays.

**Table 4.6. Negative Binomial, Individual Holidays**

| VARIABLES | (1)<br>hack | (2)<br>special |
|---|---|---|
| Christmas | -0.385 | -0.195 |
| | (0.348) | (0.898) |
| Team*Christmas | 1.297*** | 0.189 |
| | (0.498) | (1.771) |
| New Years | 0.215 | -2.091* |
| | (0.247) | (1.247) |
| Independence Day | 0.364 | -0.878 |
| | (0.252) | (0.788) |
| Yom Kippur | -0.493* | 0.942 |
| | (0.261) | (0.779) |
| Rosh Hashanah | 0.0396 | -0.559 |
| | (0.253) | (0.870) |
| Eid al-Fitr | -0.781*** | -1.319 |
| | (0.264) | (0.865) |
| Labor Day | 0.457* | 1.818*** |
| | (0.244) | (0.607) |
| Thanksgiving | -0.428* | -0.0765 |
| | (0.256) | (0.742) |
| Ramadan start | -0.330 | -2.065** |
| | (0.245) | (0.889) |
| Eid al-Adha | -0.184 | -0.795 |
| | (0.254) | (0.795) |
| Ideological | 0.137 | -0.234 |
| | (0.104) | (0.422) |
| Team | -0.146* | -0.289 |
| | (0.0758) | (0.305) |
| Middle East | -0.176* | -0.610 |
| | (0.0989) | (0.405) |
| Start Date | 0.00223 | -0.000815 |
| | (0.00154) | (0.00442) |
| Days Since Hack1 | -0.00630*** | -0.0103* |
| | (0.00188) | (0.00554) |
| Holiday Hack Tally | -0.0219 | -0.0375 |
| | (0.0162) | (0.0509) |
| Tally | 0.000110 | 0.000853 |
| | (0.000181) | (0.000559) |
| No Hack Tally | 0.00799*** | 0.00837** |
| | (0.00116) | (0.00370) |
| Hack Average | 2.716*** | 0.270 |
| | (0.183) | (0.693) |

**Table 4.6. Negative Binomial, Individual Holidays (continued)**

| | | |
|---|---|---|
| Holiday Count | 0.0288* | 0.0477 |
| | (0.0166) | (0.0520) |
| Big Gap | -30.03 | -41.21 |
| | (7,298) | (6.677e+06) |
| Constant | -34.20 | -8.037 |
| | (23.50) | (0) |
| var(_cons[notifierx]) | 0.230*** | 3.904*** |
| | (0.0305) | (0.535) |
| Observations | 425,162 | 425,162 |
| Number of groups | 230 | 230 |

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

**Sensitivity Analysis.** The final stage of our analysis was to conduct a sensitivity analysis that aimed to explore whether different holidays had varying effects on different groups of defacers, and whether Middle Eastern defacers might exhibit increased activity during Middle Eastern holidays. The results of this analysis revealed significant and varied effects across different groups, shedding light on nuanced patterns in hacking behavior.

For defacers who were ideologically motivated, the interaction term between Team and Christmas had a substantial positive effect (b = 3.110) on defacement totals. Labor Day also had a positive effect (b = 0.910), although smaller in magnitude compared to the interaction term. Conversely, New Years has a strong negative effect (b =-2.441), while the start of Ramadan had a slightly weaker negative effect (b = -1.108).

Among defacers who were members of a team, Christmas contributed a positively (b = 0.985) to defacement volumes. Meanwhile, Yom Kippur (b = -0.845) and Eid al-Adha (b = -0.976) had negative effects.

Middle Eastern defacers showed a strong positive effect for the interaction term, indicating heightened activity during Christmas if also the member of a team (b = 2.408).

However, akin to ideological defacers, New Year's had a negative effect on hacking volumes for this group (b = -1.546). Perhaps most interestingly, only Yom Kippur, among all Middle Eastern holidays, displayed a statistically significant result, and this effect was negative (b = -1.751). Thus, the results do not support our third hypothesis that Middle Eastern defacers display higher levels of defacements on Middle Eastern holidays.

For the unaffiliated group, Thanksgiving was statistically significant, contributing to a decrease in hacking volumes (b = -0.736). Similarly, Eid al-Fitr also displayed a negative effect (b = -0.719). However, Labor Day positively impacted their defacement levels (b = 0.773).

The results of this analysis also displayed interesting results across the groups of defacers. For instance, the value of the interaction term in the based negative binomial models was significantly smaller than it was for specific groups, perhaps as it was only not significant for unaffiliated defacers. In regard to the variables measuring aspects of defacers' careers, the no hack tally variable, measuring the number of days in a defacer's career was significant for all groups except Middle Easterners. However, like hack average, this was another control variable that helped account for differences in defacer careers and the effect size is relatively small. Another interesting finding is that the relationship between the number of holidays that have passed in a defacer's career and their defacement levels was not significant, nor was the relationship between previous holiday attacks and defacement volumes.

Overall, the results highlighted the importance of considering different holidays and groups of defacers when analyzing hacking behavior. The varying effects observed across different holidays and defacer groups underscored the complexity of cybercrime dynamics and the need for nuanced approaches in studying them. Moreover, the analysis revealed insights into the interplay between holiday events and individual characteristics of defacers, offering valuable

implications for future research in this domain. Overall, the results provided ample support for our second hypothesis that holidays impact the defacement volumes of defacer groups differently from other groups.

**Table 4.7. All Defacements, Sensitivity Analysis**

| VARIABLES | **Ideological** hack | **Team** hack | **Middle East** hack | **Unaffiliated** hack |
|---|---|---|---|---|
| Christmas | -1.359 | 0.985*** | -0.271 | -0.321 |
| | (0.950) | (0.363) | (0.736) | (0.417) |
| Team*Christmas | 3.110** | - | 2.408** | - |
| | (1.291) | | (1.209) | |
| New Years | -2.441*** | 0.372 | -1.546** | 0.360 |
| | (0.832) | (0.366) | (0.618) | (0.390) |
| Independence Day | 0.635 | 0.328 | 0.566 | 0.325 |
| | (0.583) | (0.390) | (0.549) | (0.394) |
| Yom Kippur | -0.426 | -0.976** | -1.751** | 0.0215 |
| | (0.636) | (0.435) | (0.719) | (0.400) |
| Rosh Hashanah | -0.306 | 0.251 | -0.368 | 0.136 |
| | (0.580) | (0.382) | (0.619) | (0.404) |
| Eid al-Fitr | 0.0551 | -0.845** | -0.687 | -0.719* |
| | (0.616) | (0.405) | (0.628) | (0.410) |
| Labor Day | 0.910* | 0.446 | 0.459 | 0.773** |
| | (0.540) | (0.383) | (0.579) | (0.375) |
| Thanksgiving | -0.483 | -0.127 | -0.376 | -0.736* |
| | (0.630) | (0.375) | (0.601) | (0.415) |
| Ramadan start | -1.108* | -0.278 | -0.882 | -0.105 |
| | (0.619) | (0.382) | (0.581) | (0.380) |
| Eid al-Adha | 0.0442 | -0.0437 | 0.304 | -0.435 |
| | (0.614) | (0.413) | (0.573) | (0.397) |
| Ideological | - | 0.153 | 0.227 | - |
| | | (0.175) | (0.170) | |
| Team | -0.188 | - | -0.235 | - |
| | (0.190) | | (0.179) | |
| Middle East | -0.0837 | -0.360* | - | - |
| | (0.194) | (0.194) | | |
| Start Date | 0.00214 | 0.00374 | -0.000992 | 0.00284 |
| | (0.00363) | (0.00231) | (0.00362) | (0.00246) |
| Days Since Hack1 | -0.0113** | -0.00570* | -0.00641 | -0.00714** |
| | (0.00464) | (0.00296) | (0.00490) | (0.00300) |
| Holiday Hack Tally | -0.0595 | -0.0106 | -0.0141 | -0.0418 |
| | (0.0461) | (0.0255) | (0.0455) | (0.0264) |
| Tally | 0.000293 | 0.000244 | -0.000674 | 0.000203 |
| | (0.000424) | (0.000293) | (0.000453) | (0.000298) |
| No Hack Tally | 0.0120*** | 0.00937*** | 0.00531 | 0.00851*** |
| | (0.00321) | (0.00200) | (0.00364) | (0.00174) |

**Table 4.7. All Defacements, Sensitivity Analysis (continued)**

| | | | | |
|---|---|---|---|---|
| Hack Average | 4.149*** | 3.284*** | 3.512*** | 1.969*** |
| | (0.583) | (0.294) | (0.443) | (0.285) |
| Holiday Count | 0.0663 | 0.0124 | 0.0205 | 0.0604** |
| | (0.0474) | (0.0259) | (0.0467) | (0.0277) |
| Big Gap | -26.66 | -27.75 | -26.13 | -30.60 |
| | (3,478) | (4,645) | (2,370) | (12,439) |
| Constant | -40.49 | -62.05 | 17.32 | -43.91 |
| | (66.37) | (38.10) | (60.93) | (37.26) |
| var(_cons[notifierx]) | 0.242*** | 0.265*** | 0.197*** | 0.274*** |
| | (0.0761) | (0.0535) | (0.0626) | (0.0578) |
| Observations | 73,053 | 159,019 | 94,142 | 182,827 |
| Number of groups | 38 | 92 | 45 | 97 |

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

The sensitivity analysis for special defacements revealed notable differences in holiday effects across different groups of defacers and emphasized the importance of distinguishing between target differences when analyzing hacking behavior. Firstly, for ideologically motivated and Middle Eastern defacers, none of the holiday effects were statistically significant, indicating that these groups did not exhibit distinct patterns of activity during holidays compared to regular periods. Showing, no support for our third hypothesis on Middle Eastern holiday defacement levels from Middle Eastern defacers.

Additionally, for unaffiliated defacers, no holidays resulted in a positive effect on defacement volumes. Instead, Ramadan (b = -2.231) and Eid al-Adha (b = -2.618) had strong negative effects. In contrast, for defacers who were members of a team, the opposite holiday effect was observed as Labor Day (b =3.529) and Yom Kippur (b = 2.612) had strong positive effects on the attack volumes of special defacements.

Overall, the analysis underscored the importance of considering target differences when examining holiday effects on hacking behavior. The results provided insights into how different groups of defacers may respond differently to holidays, reflecting the complexity of cybercrime

dynamics and highlighting avenues for future research, and further supporting our second hypothesis on the differences between defacers and the effect of holidays. Additionally, the effects of variables controlling for aspects of a defacer's career remained consistent with the previous regression models, indicating their robustness across different types of defacements.

**Table 4.8. Special Defacements, Sensitivity Analysis**

| VARIABLES | **Ideological** special | **Team** special | **Middle East** special | **Unaffiliated** special |
|---|---|---|---|---|
| Christmas | -39.52 | 0.0986 | 1.421 | -41.62 |
| | (3.370e+08) | (1.656) | (1.669) | (4.853e+08) |
| Team*Christmas | -11.50 | - | -34.15 | - |
| | (0) | | (1.902e+07) | |
| New Years | -39.34 | -25.24 | -32.19 | -0.641 |
| | (2.797e+08) | (159,970) | (8.334e+06) | (1.382) |
| Independence Day | 0.230 | -0.345 | -0.0547 | -2.033 |
| | (1.445) | (1.543) | (1.606) | (1.359) |
| Yom Kippur | -39.86 | 2.612** | -32.69 | -2.291 |
| | (2.864e+08) | (1.065) | (8.505e+06) | (1.634) |
| Rosh Hashanah | -1.001 | 0.898 | -33.08 | -41.63 |
| | (1.762) | (1.209) | (7.759e+06) | (4.619e+08) |
| Eid al-Fitr | 1.123 | -1.223 | 0.651 | -42.15 |
| | (1.239) | (1.574) | (1.495) | (4.017e+08) |
| Labor Day | 1.242 | 3.529*** | 0.695 | -0.486 |
| | (1.118) | (0.960) | (1.289) | (1.086) |
| Thanksgiving | -0.199 | -0.745 | -0.914 | 0.360 |
| | (1.648) | (1.251) | (1.771) | (1.143) |
| Ramadan start | -39.25 | -1.855 | -32.13 | -2.231* |
| | (2.358e+08) | (1.398) | (7.706e+06) | (1.277) |
| Eid al-Adha | -0.318 | -1.017 | 0.405 | -2.618* |
| | (1.663) | (1.301) | (1.673) | (1.475) |
| Ideological | - | 0.0179 | -0.0441 | |
| | | (0.655) | (0.686) | |
| Team | 0.481 | - | -0.0252 | - |
| | (0.677) | | (0.730) | |
| Middle East | -0.856 | -0.762 | - | - |
| | (0.713) | (0.731) | | |
| Start Date | 0.00639 | 0.0175** | 0.00958 | -0.0123** |
| | (0.0102) | (0.00785) | (0.0110) | (0.00622) |
| Days Since Hack1 | -0.0117 | -0.00744 | -0.0109 | -0.0162** |
| | (0.0134) | (0.00984) | (0.0152) | (0.00793) |
| Holiday Hack Tally | -0.275** | -0.00818 | -0.0544 | 0.0187 |
| | (0.139) | (0.0894) | (0.148) | (0.0747) |
| Tally | 0.00283** | 0.00275*** | 0.00294** | 0.000201 |
| | (0.00126) | (0.000987) | (0.00142) | (0.000836) |

**Table 4.8. Special Defacements, Sensitivity Analysis (continued)**

| | | | | |
|---|---|---|---|---|
| No Hack Tally | 0.0120 | 0.0249*** | 0.0191 | 0.00453 |
| | (0.0100) | (0.00668) | (0.0116) | (0.00517) |
| Hack Average | 1.900 | 0.313 | 1.802 | 0.0948 |
| | (2.033) | (1.083) | (1.717) | (0.986) |
| Holiday Count | 0.295** | 0.0196 | 0.0690 | -0.0241 |
| | (0.143) | (0.0904) | (0.153) | (0.0790) |
| Big Gap | -41.83 | -26.36 | -34.43 | -43.02 |
| | (1.898e+07) | (5,224) | (621,258) | (2.183e+07) |
| Constant | -138.4 | -292.5** | -187.2 | 163.0 |
| | (0) | (129.3) | (0) | (0) |
| var(_cons[notifierx]) | 2.929*** | 3.782*** | 3.377*** | 3.766*** |
| | (1.062) | (0.816) | (1.241) | (0.767) |
| Observations | 73,053 | 159,019 | 94,142 | 182,827 |
| Number of groups | 38 | 92 | 45 | 97 |

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

## 4.8. Discussion of Results

The outcomes of the regression models provide valuable insights for cyber-security research and shed light on the hypotheses under examination. Primarily, the results regarding the impact of the aggregated holidays variable on defacements were not statistically significant, challenging the notion of a universal threat posed by holidays as often portrayed in cybersecurity literature and government reports. Instead, our findings suggest that the effect of holidays on defacement volumes varies, with some holidays showing positive impacts, others exhibiting negative effects, while others have no effect.

For instance, Independence Day, Rosh Hashanah, and Eid al-Adha did not achieve statistical significance across all models. Surprisingly, Christmas was only significant for members of hacking teams or when used as an interaction term with team membership, suggesting that team dynamics or aspects of social learning may influence hacking behavior during this holiday. Interestingly, this effect was not significant when examining top-level

domains. Additionally, Labor Day emerged as the only holiday to consistently positively impact defacement levels.

Interestingly, several holidays, including New Years, Yom Kippur, Eid al-Fitr, Thanksgiving, and the start of Ramadan, were associated with decreases in defacement levels. This finding contradicts assumptions in existing literature but could be attributed to defacers taking breaks from cybercrimes to observe religious or social traditions. However, one interesting finding to note was that in one case, Yom Kippur positively influenced defacement levels of top-level domains for members of teams. Two potential explanations of this effect could be hacking teams coordinating attacks as a display of collective action, or from group learning that Yom Kippur lowers staffing levels. However, there are many other potential explanations for this effect, and it is impossible to definitively conclude what drives this relationship. In fact, while we attempt to explain some of the results of our models, it is impossible to definitively conclude the reasons for differing holiday effects, without qualitative assessments directed towards understanding the influence of holidays on defacers', other potential explanations remain feasible conclusions and our discussion of results should be examined under this context.

In addition to varying holiday effects, we discovered a broad spectrum of reactions among hackers concerning the influence of holidays on website defacement levels. While certain holidays exerted a substantial impact on defacement levels for one group of hackers, they could have no discernible effect on others or even produce entirely different directional effects. Moreover, we noted discrepancies in the magnitude of effects for certain holidays that had similar impacts across different hacker groups. One potential rationale for this diversity lies in the varied motivations and attributes of individual hackers. For instance, ideological defacers

might perceive certain holidays as unfavorable for furthering their agendas, as people's focus shifts from regular online activities to holiday festivities, resulting in decreased activity from these defacers during these periods. However, hackers associated with organized teams might view holidays as opportunities for increased defacements or even coordinate their actions to coincide with specific holidays, magnifying the observed effects. Conversely, hackers lacking identifiable affiliations might remain relatively unaffected by holiday dynamics, maintaining consistent activity levels irrespective of external factors. This could elucidate why fewer holidays are statistically significant for this group and why the statistical significance is not as pronounced. This variability in holiday effects warrants a deeper investigation into the underlying factors driving these divergent responses.

Finally, as anticipated, the impact of holidays on attacks targeting top-level domains differed significantly compared to all defacements. Additionally, the observed variation in holiday effects across different groups of defacers further underscores the intricate nature of cybercriminal behavior. Hence, while it's conceivable that these sites are better protected, further research is warranted to ascertain the effect of this protection from various defacers, akin to the study conducted by Howell et al. in 2019.

The results of these models present intriguing findings in light of our hypotheses. Firstly, the observation that some holidays increase defacements while others decrease them suggests that the impact of holidays on hacking behavior is not uniform. Consequently, we only find partial support for our first hypothesis that holidays increase defacement levels as our findings indicate that holidays have mixed effects on hacking activity. However, in support of our second hypothesis, the results of the study display much variation in the impact of holidays on different groups of defacers, underscoring the complexity of cybercriminal behavior. While holidays do

influence defacement volumes differently among various groups of defacers, the direction of these effects varies, with some groups exhibiting increases and others experiencing decreases in attacks depending on the holiday.

Lastly, Middle Eastern defacers did not demonstrate heightened of defacements on Middle Eastern holidays, showing no support for the hypothesis that the volume of defacements from Middle Eastern defacers increases on dates corresponding to Middle Eastern holidays. This finding suggests that cultural or regional factors may not significantly influence hacking activity during these specific periods.

Unrelated to our hypotheses, the many null findings regarding the lack of statistical significance for both the elapsed holidays and previous hacking on holidays variables is particularly intriguing. Initially, we assumed that more opportunities arising from a decrease in capable guardianship during holidays would lead to an increase in defacements. However, our analysis suggests that this assumption does not hold true for defacers.

There are several possible explanations for this unexpected result. Firstly, our analysis revealed that some holidays impact defacement volumes while others do not. Therefore, it is plausible that defacers may not perceive all holidays as opportune times to exploit a decrease in guardianship. Another possibility is that defacers may not be aware of or may not recognize holidays as periods of decreased guardianship.

Overall, these findings have important implications for our understanding of the relationship between holidays and capable guardianship. Further research is warranted to explore the underlying reasons for these results and to gain deeper insights into how defacers perceive guardianship and respond to holiday periods in the context of cybercrime.

### *4.8.1. Conclusions and Implications for Theory and Policy*

This research aimed to investigate the relationship between holidays and the levels of website defacements conducted by individual hackers. The objective was to determine whether the commonly held belief that holidays lead to increased successful hacking, specifically website defacement attacks, holds true. Utilizing an original dataset measuring the daily defacement attacks of website defacers, the findings of this study present preliminary evidence that challenges the conventional wisdom. Contrary to expectations, the results indicate that defacers' attack volumes do not exhibit an uptick during holidays in general. Rather, not only does the holiday matter, but so does the type of defacer and the kind of website. Furthermore, depending on the holiday, this effect can positively or negatively influence defacement levels. These results carry implications for both criminological theory and cybersecurity practices.

The results of this study also raise an intriguing question: "Can hackers be analyzed through the lens of Routine Activities Theory?" While the absence of a clear relationship between holidays and increased defacements suggests a lack of influence from a lack of capable guardianship, an alternative explanation emerges. It is plausible that defacers consistently perceive a deficiency in capable guardianship. To explain, as defacers' activities are conducted online, they may not experience the same deterrent effect of guardianship nor the perceived risk of crime as criminals in the physical world. This is because defacers may not perceive IT personnel as effective guardians due to the minimal risk of detection, and as many defacers do not see IT personnel as able to prevent their attacks. In fact, during the data creation stage, messages mocking IT staff incompetency were often found in the content of defacement. Furthermore, many defacers embrace the challenge of attacking sites with better guardianship to prove their skills. This perspective is echoed in the literature and the content of defaced websites.

Thus, while Routine Activities Theory might be entirely applicable to understanding website defacers, further research is essential to comprehend how cybercriminals fit within this theoretical framework, especially as it relates to the aspect of Capable Guardianship.

Outside of academia, the study's findings have implications for industry practices. As only specific holidays are shown to trigger increased website defacements, commonly suggested cybersecurity strategies like reducing holiday time for IT personnel or hiring temporary staff over holidays in anticipation of more attacks might lack a solid foundation based on this research's outcomes. However, more research is warranted, particularly in investigating other forms of hacking, before definitive conclusions can be drawn. Ideally, these results will stimulate further research and encourage private companies to release data on attempted and successful hacks on their digital infrastructure. Meanwhile, ongoing research involving larger sample sizes and randomized sampling is necessary to validate and extend the conclusions drawn from this study.

### *4.8.2. Limitations*

While this research is likely to advance theory and inform policy, it is not without limitations. Firstly, the study may suffer from limited generalizability as not all defacers report their successful exploits to Zone-H and likely differ in unobserved ways from those who do report. While the majority of defacements are reported to this website, not all defacers report their defacements to Zone-H (Maggi et al., 2021). Thus, because of our use of this the results should be taken with some consideration as it may not reflect all defacers and their defacements. Additionally, our self-imposed parameters, while necessary, likely further limit the generalizability of our results. Those selected for the study may differ from other hackers who report their exploits to Zone-H but were excluded from the study.

Next, like all non-experimental studies, our study likely will suffer from some degree of omitted variable bias. This is especially true as we cannot measure the true level of guardianship. As has been previously discussed, while holidays generally coincide with decreased levels of guardianship, this assumption may not always hold true, especially for more important websites. We adjusted for these potential differences by testing individual holidays and exclusively observing special defacements. Additionally, it is likely that other unidentified factors can influence cyber-criminals' offending behaviors. There are also various issues with the variables we were able to include in the study. Starting with the dependent variable, it is possible the first reported defacement is not an individual's first true defacement. It is, however, the alias's first defacement and the closest achievable proxy. Additionally, it is possible that a hacker reports to Zone-H under a different alias. However, hackers who engage in website defacement tend to use the same username across platforms to bolster their reputations (Maimon et al., 2017). Moreover, the OSINT variables measuring whether the hacker was identified as ideological, on a team, or Middle Eastern could be biased if defacers did not reveal this immediately but later in their career. The potential for a shift in motivations presents a source of omitted variable bias in our fixed variables. Additionally, our study, akin to previous ones, is constrained by its incapacity to capture all pertinent influences on defacement behavior. Variables like daily emotions and levels of self-control, which are likely to impact defacement levels, remain unaccounted for. It's plausible that if we could incorporate these variables, the observed holiday effect could alter. This limitation underscores the intricacy of modeling hacker motivations. Nonetheless, we advocate for future research to enhance our intelligence gathering techniques, incorporating periodic measurement and sentiment analysis, to address these limitations and better encapsulate

evolving motivations. By embracing such advancements, researchers can augment the quality and depth of analyses on the motivations propelling website defacement attacks.

Another limitation is that the study does not utilize a large sample. The creation of the variables we chose requires a significant time commitment for even smaller samples, let alone ones containing thousands of website defacers. While this study could have scraped the Zone-H website for all defacements or purchased their data, and this should be examined in future research, we believe that the decision to include the descriptive variables will provide unique perspectives that are worth exploring over convenient sampling procedures. This is especially true given the lack of confidence in the self-reported motivations in the Zone-H data (Banerjee et al., 2021). An additional limitation is that our initial screening of defacers with over 50 pages on Zone-H biases introduces endogeneity from sample selection bias that could potentially bias the results of our models. The exclusion of prolific offenders could lead to negative biases in our results, as it's conceivable that defacers who attack websites more frequently would also conduct more attacks on holidays. Consequently, we might be underestimating the magnitude of the holiday effect. Despite attempting to mitigate this through the incorporation of variables measuring different career aspects and conducting sensitivity analysis, future research should contemplate purchasing data from Zone-H to capture the entire careers of even prolific offenders and comprehend how these offenders are influenced by holidays.

Lastly, while our research objectives were framed within the context of Routine Activities Theory (RAT), it is important to clarify that our research cannot be considered a direct test of the theory itself. Instead, our focus lies in evaluating the predictive ability of variables derived from RAT principles. This study selected a proxy to measure the potential effect of guardianship akin to other studies on defacement or hacking, such as Howell et al.’s (2019) use

of military presence as a proxy for guardianship. Holidays theoretically provide a useful proxy; although holidays themselves do not provide deterrent effects typical of a guardian, they are likely to disrupt the conditions of capable guardianship. Furthermore, this proxy was selected based on literature suggesting that holidays may alter routines of IT staff, decrease surveillance levels, and reduce security measures. However, while companies' acknowledgment and guidance from cybersecurity professionals support the conclusion that holidays may serve as periods of decreased surveillance and IT security measures, the evidence supporting this assertion often relies on hand-picked case studies, select surveys, or undisclosed sources of evidence. These factors contribute to evidence heterogeneity across studies, raising concerns about the generalizability and reliability of holidays as a proxy for capable guardianship. Variability in security and staffing structures, cultural norms, industry practices, and regional security protocols may influence the effectiveness of holidays in increasing defacement risks. Moreover, reliance on aggregated data or anecdotal evidence may obscure nuances in the relationship between holidays and website security, similar to challenges faced in other studies employing proxy variables.

To mitigate the proxy's potential for heterogeneous effects, we conducted an analysis of various holidays and website types. Despite this limitation, this study contributes significantly to understanding cybersecurity industry assertions about holidays. By examining diverse holidays and website categories, we gained insights into their nuanced impact on website defacement activities. The findings reveal that holidays do not uniformly decrease guardianship, indicating that holidays may not always serve as a reliable proxy for decreased guardianship, with many showing fewer attacks, possibly due to defacers perceiving them as less conducive to hacking or engaging in holiday festivities. This unexpected outcome highlights the need for further

investigation into the underlying mechanisms of holidays, especially their differential effects on different groups of website defacers.

Intriguingly, our study's challenge prevailing assumptions within the cybersecurity community regarding the relationship between holidays and increased defacement activity. This underscores the importance of critically examining claims and assumptions, even those made by industry experts, and conducting empirical research to validate or refute them. In future research endeavors, it will be essential to consider contextual factors such as website size, industry type, and geographic location to gain a more nuanced understanding of how holidays influence defacement rates. By accounting for these variables, researchers can better assess the complex interplay between holidays, capable guardianship, and cyber threats, while addressing the limitations in using holidays as a proxy for guardianship. Additionally, future research endeavors should also delve into both qualitative and quantitative exploration of these discrepancies, possibly through interviews with website defacers. By addressing these nuances, future studies can enrich our understanding of the dynamics shaping cyber threats and security measures, providing valuable insights for developing effective countermeasures.

In summary, the hacking activities of cybercriminals are deeply complex. While headline-grabbing attacks on holidays and admissions of poor security practices during these times have drawn the attention of cybersecurity professionals and government agencies, leading to repeated suggestions that holidays increase the likelihood of attacks, our analysis offers a different, more nuanced perspective. While case studies can offer valuable insights for learning in cybersecurity, it's essential for professionals to exercise caution when using them to draw broad conclusions. We hope that our paper, as the first academic research to explore the impact

of holidays on hacking, will encourage further investigation into the effects of holidays and capable guardianship in cybersecurity.

# Chapter V: Overall Conclusions.

## 5.1. Abstract.

This chapter is the final section of the dissertation and seeks to provide an overall summary of the observations, limitations, and implications of the previous three papers. The section begins with a brief restatement of the problem of website defacement, followed by summaries of the findings from each paper. Theoretical or policy implications are also discussed. Lastly, the section concludes with a proposed direction for future research on website defacement, and a general conclusion on the success of this dissertation.

## 5.2. Discussion of Findings

The proliferation of websites, both for personal and business use, has seen a significant increase in recent years. Despite advancements in digital security and the presence of numerous cybersecurity providers, these websites remain vulnerable to hacking. In a website defacement attack, hackers gain unauthorized access to websites and alter their appearance, often rendering them inoperable. These cyber-attacks, known as website defacements, not only tarnish the reputation of site owners and administrators but also result in costly financial losses. Website defacers, the hackers responsible for such attacks, offer a unique opportunity to study perpetrators of hacking due to the overt nature of their offenses and the abundance of data available on their activities.

In recent years, prior research on website defacers has offered initial insights into their attack preferences and motivations. However, given the relatively new nature of this research field, there are significant opportunities to enhance our understanding beyond simple descriptions of these cybercriminals. Our scoping review aimed to systematically analyze the

existing literature to identify and emphasize the critical research needs in the study of website defacers.

As previously stated, our scoping review aimed to fill potential gaps in our comprehension of website defacers and identify prevalent theoretical trends in the existing literature. Being the inaugural review of its kind on website defacement, it represents a pivotal step forward in advancing our understanding of these hackers and the literature surrounding them. Our analysis focused on two primary aspects of website defacement: the perpetrators and their targets. We observed a notable imbalance in the research, with a predominant emphasis on offender analysis, so we individually discussed subthemes in the research on offenders. This review also discussed papers that utilized methods of research that were non-congruent with the majority of the research. These were discussed in their own section, to avoid potential confusion and to highlight the importance of refraining from these methods until their true generalizability can be shown. This approach facilitated a comprehensive exploration of the multifaceted nature of website defacements, enabling a thorough examination of research outcomes and identifying areas of knowledge gaps.

In this undertaking, the review yielded several significant observations from the studies analyzed. Firstly, as noted earlier, there is a notable skew in research focus towards the hackers engaged in website defacement. This leads to an asymmetry in our comprehension of both offenders and victims. Currently, our insights into the victims of website defacement seem limited to observations of weakened security measures and delayed response times, which are scarcely adequate or compelling. Hence, it is imperative for future research endeavors to prioritize the exploration of the victims' experiences in this type of cybercrime.

Secondly, our scoping review showed that the literature is also skewed in its use of theory. Specifically, we observed that defacers were predominantly examined through the lens of Routine Activities Theory, with more than half of the included studies operationalizing this framework. Consequently, the primary strength of the existing literature lies in its substantial contribution to our comprehension of how various motivations can influence the behavioral patterns of website defacers. However, while the motivated offender aspect of Routine Activities Theory has been extensively explored, the other theoretical components, namely suitable targets and capable guardianship, have received relatively scant attention. Therefore, future research endeavors should aim to enhance our understanding of how website defacers assess targets and perceive and react to capable guardianship.

While the literature predominantly embraces the Routine Activities Theory, alternative perspectives such as Social Learning Theory and Life-Course Criminology have been employed to a lesser extent. This body of research underscores the significance of social connections among defacers in their evolution as cybercriminals, highlighting the considerable variability in the criminal trajectories of these individuals. However, due to limited findings in this area, there remains a pressing need for further exploration.

However, as discussed, the available literature displays methodological issues that need to be addressed. Firstly, the literature is over reliant on self-reported Zone-H data, which has been shown may not accurately measure the motivations of website defacers. Secondly, much of the research is descriptive in nature, lacking in-depth causal analysis to understand how defacers respond to various interventions or treatments. Lastly, a notable proportion of studies rely on non-defacement data obtained from surveys of college students to study active hackers, raising

questions about the applicability of such findings. Therefore, future research should prioritize direct study of defacers themselves rather than relying on proxies for them.

Overall, the scoping review provided a concise overview of the literature examining website defacement. Additionally, it provided a framework for future studies to progress the trend of utilizing more innovative methods and robust analytic strategies, expanding theoretical frameworks, and increase the focus on the victims of website defacement. The two papers following this scoping review sought to address some of these areas of concern.

The second paper aimed to enhance our understanding of the criminal trajectories of website defacers/hackers. As previously mentioned, life course criminology has been underutilized in the context of hackers due to the digital anonymity that conceals traditional offender features such as age, race, education, and family status. Consequently, cybercrime studies have pursued two main approaches. The first approach focused on individuals suspected of cybercrimes, which pose challenges in terms of attribution and validity. The second approach dismissed the applicability of life course criminology to studying hackers, arguing that traditional turning points and transitions cannot be measured in the digital realm. Consequently, there exists limited knowledge about the criminal careers of hackers and the factors influencing divergent criminal trends.

Our research adopted a novel approach to studying the life course criminology of hackers, enhancing our understanding of their criminal trajectories. Instead of focusing on the age of the offender, which is often unknown in cyberspace, we concentrated on the first year of offending. This allowed us to examine hackers' criminal onset and explore patterns of persistence, maintenance, and desistence during this crucial initial period. Since traditional turning points were not observable, we analyzed the characteristics of defacers based on their

attack messages. Through this approach, we gained insights into the motivations driving each defacer in our sample to offend, including ideological motivations, their social networks within the hacker community, their tendency to report attacks on multiple sites, and even their geographical location. Although these characteristics were assessed at the onset, utilizing open-source intelligence to gather data on active hackers remains underutilized in the field.

Employing this methodology, our study revealed that hackers demonstrate trajectories akin to those observed in traditional criminal behavior. We observed four distinct groups: one who seemed to commit crimes as a "one off," a second group showing a gradual decline in criminal activity, another group exhibiting an escalation in persistence in cybercrime, and a fourth group maintaining a consistently high level of cyber-offending. Crucially, our models effectively identified the characteristics of website defacers associated with each group, allowing us to predict group membership at the onset of criminal activity.

Moreover, our research findings are in line with previous studies examining defacer attack patterns, demonstrating that a minority of website defacers are responsible for the majority of attacks. This observation supports the notion among cybercrime researchers that website defacement might serve as a precursor to more serious cybercriminal activities, while a smaller subset of individuals continues to engage in defacement over extended periods. However, this complicates our understanding of desistance, as some individuals may discontinue all cybercriminal activities, while others shift away from defacement to pursue other forms of hacking. This raises intriguing avenues for future research. Yet, tracing the career trajectories of defacers as they transition into or away from new areas of cybercrime poses challenges due to the anonymity typically associated with cyber-offending.

However, there are alternative avenues for future research to broaden our understanding of cybercriminal life courses. For example, delving into significant events in a defacer's career, like joining a hacking team, could elucidate hacker-specific turning points, particularly given the lack of knowledge about traditional turning points in cybercrime trajectories. Gathering such data might entail distributing surveys to active offenders to gain insights into their experiences and motivations. Additionally, future studies should contemplate expanding their sampling criteria to encompass a larger cohort of hackers, enhancing the generalizability of results and enabling the examination of varying trajectories within different subsets of the website defacer population.

In conclusion, while there is abundant potential for advancement in the study of cybercriminal life courses, our research has established essential groundwork that can serve as a cornerstone for future investigations. By delving deeper into hacker-specific events and turning points, and employing innovative data collection methods, we can further enhance our understanding of cybercriminal behavior. This deeper understanding, in turn, can inform the development of more effective strategies for prevention and intervention in cybercrime activities.

The third and final study focused on investigating the correlation between holidays and website defacement activities conducted by individual hackers. Its aim was to scrutinize the common assumption that holidays witness a surge in successful hacking endeavors, particularly website defacement attacks. Through the analysis of an original dataset tracking daily defacement attacks, the findings challenge conventional wisdom. Contrary to expectations, the study reveals that defacement attack volumes do not consistently spike during holidays; instead, the relationship is nuanced and influenced by factors such as the type of defacer and the targeted website. Moreover, the impact of holidays on defacement levels varies, demonstrating both

positive and negative effects depending on the holiday in question. These insights carry significance for both criminological theory and cybersecurity practices.

For example, the study prompts a thought-provoking inquiry into whether hackers can be analyzed through the framework of Rational Choice Theory. On one hand, the absence of a straightforward correlation between holidays and heightened defacement activity suggests a lack of influence from traditional guardianship mechanisms. However, on the other hand, it is plausible that defacers consistently perceive a deficiency in effective guardianship, viewing IT personnel as incapable guardians due to the minimal risk of detection and success in overcoming site security to prove their skills. This perspective, reflected in both literature and defaced website content, underscores the need for further research to elucidate how cybercriminals align with theoretical frameworks such as Routine Activities Theory, particularly concerning the concept of Capable Guardianship.

Moreover, this study underscored the importance of adjusting for and further studying the shape of the criminal careers of website defacers. It shed additional light on the diverse trajectories of defacer careers, revealing significant variability in their patterns and impacts on defacement levels. While overarching trends emerge, with some initiating prolific and high-volume activities from the outset and others gradually escalating over time, there is notable divergence among individual defacers. Additionally, intermittent periods of cessation interspersed with sustained activity further underscore the complexity of criminal careers among website defacers. Understanding these variations is crucial for comprehensively analyzing defacement behaviors and devising effective cybersecurity strategies.

Beyond academic discourse, the study's findings have implications for industry practices. Since only specific holidays trigger increased website defacement, conventional cybersecurity

strategies such as reducing IT personnel's holiday time or hiring temporary staff might lack a solid basis. However, further research is warranted, especially concerning other forms of hacking, before definitive conclusions can be drawn.

### 5.3. Policy Implications

Our research has significant implications for the development of law enforcement and professional policies in several key areas. Firstly, due to the nuanced effects of holidays on website defacement, policymakers and organizations should adopt flexible approaches that can adapt to the changing threat landscape. This entails considering holiday-specific attack patterns and adjusting security measures accordingly. Additionally, given the interconnected nature of cybersecurity threats, collaborative efforts and information sharing among stakeholders are crucial. Policymakers could facilitate collaboration between government agencies, private sector entities, and cybersecurity experts to share cyber-attack incident data. This collaborative approach helps gain a comprehensive understanding of the threat landscape, especially on holidays, and strengthens collective defenses against website defacement and other cyber threats.

Secondly, our research underscores the importance of targeted resource allocation to address high-risk hackers, particularly those within increasing and persistent threat groups. Policymakers and cybersecurity authorities can establish specialized units dedicated to monitoring and engaging with individuals identified as high-risk. This proactive approach helps mitigate potential cyber threats posed by these individuals. Furthermore, policymakers should explore avenues for redirecting the skills of high-risk hackers towards ethical roles within the cybersecurity landscape. Public-private partnerships can play a crucial role in this endeavor by creating mentorship programs, offering ethical hacking courses, and providing employment

opportunities. This strategy aims to steer hackers away from criminal activities, thereby contributing to a safer digital environment.

A community-centric approach to cybersecurity is essential, with policymakers and practitioners actively engaging with online platforms and hacking communities to promote responsible behavior and foster positive norms. Collaboration agreements with online platforms can incentivize users to report vulnerabilities responsibly, while public awareness campaigns and educational initiatives can help deter malicious cyber activities. By building trust and cooperation within these communities, stakeholders can work together to enhance cybersecurity measures and mitigate potential threats effectively.

Lastly, investing in cyber-intelligence capabilities, particularly Open-Source Intelligence (OSINT), is paramount to improve cybersecurity. While our research utilized OSINT to understand the characteristics of defacers, policymakers should allocate resources to establish dedicated OSINT teams. These teams should be equipped with the necessary tools and expertise to monitor online activities, gather intelligence, and assess risks effectively, including identifying holidays that hackers view as opportune times for attacks. This investment enables timely detection of emerging threats and informs proactive and adaptive cybersecurity strategies, thus strengthening overall cyber defense mechanisms.

### 5.4. Limitations

Each of the three studies brings forth insightful findings on the state of the research and into the offending patterns of website defacers. However, as with all research, they are not free of limitations. Firstly, the initial scoping review, while meticulously conducted in adherence to the PRISMA-ScR framework, had a broad focus characteristic of scoping studies, which might have led to oversights despite attempts to mitigate this through rigorous methodology. Limitations

such as the exclusion of non-English language literature and technical coding papers, though necessary for maintaining focus, could have narrowed the scope of insights. Nonetheless, the review sets a solid foundation for future investigations into website defacement.

Our second paper, exploring cyber-offender behavior trajectories, emphasizes the first reported defacement as the initiation point for trajectory analysis, which is practical but may not encapsulate the true beginning of an individual's hacking career. Moreover, the study's sample selection criteria, while vital for addressing specific research questions, may restrict the broader applicability of findings. Lastly, the research, like much of the defacement literature, relies primarily on data sourced from the Zone-H archive. While this archive provides valuable information at a greater scale than other similar websites, its limitations and potential biases need careful consideration. Despite these challenges, the study offers nuanced insights into cyber-offender behavior, laying the groundwork for future research avenues.

The third paper, investigating the effects of holidays and capable guardianship, also relies on data reported to Zone-H, which, as mentioned, may limit the generalizability of the results due to the incomplete reporting by all defacers. Additionally, the study faces the challenge of omitted variable bias since it cannot fully measure guardianship, despite using an intuitive proxy variable. Moreover, the study's smaller sample size, necessitated by the creation of a more detailed dataset, introduces endogeneity and potentially compromises the generalizability of the findings. However, the study's focus on exploring unique perspectives and the endeavor to enhance intelligence gathering techniques signify important directions for future research into website defacement.

In summary, while each study contributes significantly to the understanding of website defacement and cyber-offender behavior, they acknowledge the necessity of addressing

limitations such as reliance on specific datasets, potential biases, and constraints in sample size and scope. Future research endeavors should strive to overcome these limitations to deepen the field's knowledge and to develop more effective policy and intervention strategies. By addressing these challenges, researchers can enhance the robustness and applicability of findings, ultimately advancing our understanding of cybersecurity threats and facilitating more informed responses.

### 5.5. Conclusion

While the three studies exhibit noteworthy limitations, this dissertation provides a comprehensive understanding of website defacement and cyber-offender behavior, contributing to both the advancement of knowledge on website defacers and the identification of remaining gaps.

The first study sheds light on the evolving research methodologies and theoretical frameworks in the field of website defacement, emphasizing the importance of comprehensive reviews such as scoping studies in synthesizing existing knowledge and identifying prevalent theories. Despite significant progress in understanding offender motivations and behaviors, there remains a conspicuous gap in our understanding of the victim's experience, warranting prioritization in future research efforts. The prevalence of Routine Activities Theory underscores the complexity of offender motivations and strategies, yet there is untapped potential in exploring the role of capable guardianship in deterring cybercrime.

The second study delves into the longitudinal trajectories of cyber-offenders, providing insights into the predictors of natural desistence, increased engagement, and persistence in hacking activities over time. This research highlights the developmental nature of cyber-offending behavior, with early-stage hackers often seeking validation and recognition through flashy defacements, while politically motivated hackers tend to have shorter-lived criminal

careers. By integrating cyber-intelligence and life-course perspectives, the study not only advances theoretical understanding but also offers practical implications for policy and intervention strategies. It emphasizes the significance of targeted resource allocation and ethical skill redirection to mitigate potential cyber threats posed by high-risk individuals.

Lastly, the third study challenges conventional wisdom regarding holidays and hacking activities, proposing a nuanced relationship influenced by factors such as the type of defacer and the targeted website. Contrary to widespread beliefs, not all holidays result in increased defacement levels, prompting a reassessment of cybersecurity strategies and industry practices. By examining Rational Choice Theory in the cyber context, the study invites further investigation into the role of capable guardianship and the effectiveness of traditional deterrents in mitigating cybercrime.

Together, these studies underscore the complexity of cyber-offender behavior and the dynamic interplay of individual, contextual, and environmental factors that shape hacking activities. Moving forward, the field stands to benefit from continued interdisciplinary collaboration, innovative research methodologies, and a renewed focus on victim experiences and cyber-intelligence integration. By addressing these avenues, researchers can advance theoretical understanding, inform evidence-based policies, and ultimately foster a more secure digital landscape for all stakeholders.

## Appendix A. Complete Data Extractions

### Table A1. Summary of Included Studies for Scoping Review

| Author/s | Year | Studied Population | Research design | Methodology |
|---|---|---|---|---|
| Aggarwal et al | 2015 | Reinforced learning model of decision and outcome scenario of defacing a website | Reinforced machine learning models. | Quantitative. |
| Aslan et al | 2020 | 96 website defacers | Social network analysis and thematic analysis of content | Quantitative |
| Banerjee et al | 2021 | 2.24 million returned defacements. 40,330 (3,000 images for the handcrafted approach and 37,330 images for the deep learning approach) images for the image-clustering analysis | deep machine learning model, knn (k nearest neighbor clustering) as well as qualitative thematic analysis. | Mixed Methods |
| Bartoli et al | 2009 | More than 62,000 website defacement incidents monitored in near real time for approximately two months | Descriptive analysis examining time (hourly) between defacement and restoration of website. | Quantitative. |
| Adam M. Bossler | 2021 | 657 college student respondents | Logistic regression analysis of survey data. | Quantitative |
| Adam M. Bossler | 2019 | 722 college student respondents | Logistic regression analysis of survey data. | Quantitative |
| Burruss et al | 2021 | 119 defacers, 1292 defacements only 1062 defacements had content analysis | Finite mixture models, negative binomial regression models | Quantitative |
| Han et al | 2016 | 212,093 web-hacking cases | Machine similarity-based learning model | Quantitative |
| Han et al | 2019 | 212,093 web-hacking cases | Machine similarity-based learning model | Quantitative |

**Table A1. Summary of Included Studies for Scoping Review (continued)**

| Author/s | Year | Studied Population | Research design | Methodology |
|---|---|---|---|---|
| Thomas J. Holt | 2009 | 10 Turkish hacker interview respondents. 6 hacker web sites. | Semi-structured Interviews, content analysis. | Qualitative |
| Holt et al | 2020 | over 2.2 million defacements | Descriptive analysis. Binary logistic regression models | Quantitative |
| Holt et al | 2017 | 357 US student respondents. 779 Taiwanese student respondents | Binary logistic regression analysis of survey data. | Quantitative |
| Holt et al | 2020 | 138,361 web defacements performed against websites hosted within the Netherlands IP space | Logistic regression analysis. | Quantitative |
| Holt et al | 2022 | over 2.2 million defacements | binary logistic regression model | Quantitative |
| Howell et al | 2019 | nearly 13,000 defacements against top level domains | Negative binomial regression models | Quantitative |
| Jin R. Lee & Thomas J. Holt | 2023 | over 2.2 million website defacements. 29,035 attackers | Binary logistic regression models | Quantitative |
| Maggi et al | 2018 | 12,992,166 defacements | Scalable clustering machine learning model, BIRCH (balanced iterative reducing and clustering using hierarchies), Sentiment analysis. | Mixed Methods |
| Maimon et al | 2017 | 352 hackers reported 2824 unique web defacements attacks | Negative binomial regression models | Quantitative |
| Maimon et al | 2021 | 117 active defacers with active Facebook accounts | Control and Treatment group mean analysis | Quantitative |
| Moneva et al | 2020 | 9 million website defacements | Descriptive analysis | Quantitative |
| Kok Wei Ooi | 2012 | 3,545,153 observations of 30,627 hacking units | Panel logit regression models | Quantitative |

**Table A1. Summary of Included Studies for Scoping Review (continued)**

| Author/s | Year | Studied Population | Research design | Methodology |
|---|---|---|---|---|
| Perkins et al | 2023 | 86,208 unique defacement incidents reported by 786 hackers across 123 groups | Social network analysis. | Quantitative |
| M. Hassan Shirali-Shahreza & Mohammad Shirali-Shahreza | 2009 | 81 defacements against Iranian IP space. (did not disclose data source) | Descriptive case study analysis | Qualitative |
| van de Weijer et al | 2021 | 2,745,311 attacks performed by 66,553 hackers | Group based trajectory modeling | Quantitative |
| Woo et al | 2004 | 462 defaced Web pages | Content analysis. Descriptive statistics | Mixed Methods |
| Zayid et al | 2023 | 93644 defacements | Machine learning models. Descriptive statistics | Quantitative |
| Balduzzi et al | 2018 | 12,992,166 defacements | Content analysis. Descriptive statistics | Mixed Methods |
| Das et al | 2017 | 99437 defacements | Descriptive statistics | Quantitative |
| Holt et al | 2017 | 10 Turkish hacker interview respondents | Semi-Structured Interviews | Qualitative |

## Appendix B. Full Multilevel Model Output

### Table B1. Aggregated Holiday Effect Logit Regression

| VARIABLES | (1)<br>Did hack? | (2)<br>Did special? |
|---|---|---|
| Holiday | -0.0396 | -0.0667 |
| | (0.0541) | (0.166) |
| Ideological | 0.0879 | -0.0946 |
| | (0.0967) | (0.319) |
| Team | -0.100 | -0.326 |
| | (0.0710) | (0.229) |
| Middle East | -0.153* | -0.440 |
| | (0.0923) | (0.305) |
| Start Date | -0.000767 | 0.00229 |
| | (0.000990) | (0.00304) |
| Days Since Hack1 | -0.00156 | 0.00221 |
| | (0.00122) | (0.00383) |
| Holiday Hack Tally | -0.0351*** | -0.0275 |
| | (0.0110) | (0.0335) |
| Tally | -0.000882*** | -0.000205 |
| | (0.000122) | (0.000403) |
| No Hack Tally | -7.90e-05 | -0.000752 |
| | (0.000794) | (0.00257) |
| Hack Average | 1.613*** | -0.0508 |
| | (0.158) | (0.517) |
| Holiday Count | 0.0391*** | 0.0359 |
| | (0.0113) | (0.0344) |
| Big Gap | -54.70 | -20.44 |
| | (0) | (0) |
| 2.month_of_weekdate | -0.116** | -0.0179 |
| | (0.0537) | (0.171) |
| 3.month_of_weekdate | 0.0598 | -0.0687 |
| | (0.0736) | (0.232) |
| 4.month_of_weekdate | 0.0612 | -0.103 |
| | (0.101) | (0.313) |
| 5.month_of_weekdate | 0.308** | 0.165 |
| | (0.128) | (0.394) |
| 6.month_of_weekdate | 0.276* | 0.00403 |
| | (0.156) | (0.482) |
| 7.month_of_weekdate | 0.149 | -0.333 |
| | (0.185) | (0.569) |
| 8.month_of_weekdate | 0.255 | -0.160 |
| | (0.214) | (0.660) |

**Table B1. Aggregated Holiday Effect Logit Regression (continued)**

| | | |
|---|---|---|
| 9.month_of_weekdate | 0.272 | -0.392 |
| | (0.244) | (0.749) |
| 10.month_of_weekdate | 0.109 | -0.854 |
| | (0.274) | (0.842) |
| 11.month_of_weekdate | 0.221 | -0.439 |
| | (0.303) | (0.931) |
| 12.month_of_weekdate | 0.269 | -0.670 |
| | (0.333) | (1.024) |
| 2002.year_of_weekdate | 12.79 | -3.300 |
| | (0) | (0) |
| 2003.year_of_weekdate | -5.503 | 7.016 |
| | (0) | (0) |
| 2004.year_of_weekdate | 2.428 | -3.759 |
| | (0) | (0) |
| 2005.year_of_weekdate | -17.95 | 10.59 |
| | (16.29) | (49.98) |
| 2006.year_of_weekdate | -17.64 | 9.382 |
| | (16.65) | (51.09) |
| 2007.year_of_weekdate | -18.31 | -6.989 |
| | (17.02) | (0) |
| 2008.year_of_weekdate | -17.90 | 8.359 |
| | (17.38) | (53.29) |
| 2009.year_of_weekdate | -17.18 | 6.896 |
| | (17.74) | (54.41) |
| 2010.year_of_weekdate | -16.18 | 7.879 |
| | (18.10) | (55.51) |
| 2011.year_of_weekdate | -16.85 | -12.74 |
| | (18.46) | (0) |
| 2012.year_of_weekdate | -15.92 | 4.939 |
| | (18.82) | (57.72) |
| 2013.year_of_weekdate | -15.91 | 2.604 |
| | (19.18) | (58.83) |
| 2014.year_of_weekdate | -15.69 | 2.558 |
| | (19.54) | (59.94) |
| 2015.year_of_weekdate | -15.54 | 1.983 |
| | (19.90) | (61.04) |
| 2016.year_of_weekdate | -15.41 | 0.846 |
| | (20.26) | (62.15) |
| 2017.year_of_weekdate | -15.07 | 0.481 |
| | (20.63) | (63.26) |
| 2018.year_of_weekdate | -14.61 | -0.437 |
| | (20.99) | (64.37) |
| 2019.year_of_weekdate | -14.56 | -1.117 |
| | (21.35) | (65.48) |

**Table B1. Aggregated Holiday Effect Logit Regression (continued)**

| | | |
|---|---|---|
| 2020.year_of_weekdate | -14.36 | -2.365 |
| | (21.71) | (66.59) |
| 2021.year_of_weekdate | -14.08 | -3.459 |
| | (22.07) | (67.69) |
| 2022.year_of_weekdate | -14.09 | -3.727 |
| | (22.43) | (68.80) |
| 2023.year_of_weekdate | -13.36 | -3.086 |
| | (22.79) | (69.90) |
| 2024.year_of_weekdate | -12.00 | -21.06 |
| | (23.16) | (0) |
| var(_cons[notifierx]) | 0.224*** | 2.193*** |
| | (0.0260) | (0.309) |
| Constant | 28.62 | -53.48 |
| | (0) | (0) |
| Observations | 425,162 | 425,162 |
| Number of groups | 230 | 230 |

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

**Table B2. Individual Holiday Effects Logistic Regression**

| VARIABLES | (1)<br>Did hack? | (2)<br>Did special? |
|---|---|---|
| Christmas | 0.0232 | -0.918 |
| | (0.220) | (1.013) |
| Team*Christmas | -0.190 | 0.490 |
| | (0.340) | (1.428) |
| New Years | -0.136 | -1.318 |
| | (0.173) | (1.011) |
| Independence Day | -0.00655 | -0.233 |
| | (0.173) | (0.595) |
| Yom Kippur | -0.217 | -0.206 |
| | (0.183) | (0.591) |
| Rosh Hashanah | 0.200 | -0.00509 |
| | (0.156) | (0.517) |
| Eid al-Fitr | -0.445** | -0.921 |
| | (0.194) | (0.717) |
| Labor Day | 0.225 | 1.197*** |
| | (0.152) | (0.310) |
| Thanksgiving | -0.0348 | 0.244 |
| | (0.174) | (0.432) |
| Ramadan start | -0.0806 | -0.921 |
| | (0.165) | (0.717) |
| Eid al-Adha | 0.183 | -0.125 |
| | (0.156) | (0.512) |
| Ideological | 0.0905 | -0.0981 |
| | (0.0923) | (0.319) |
| Team | -0.116* | -0.323 |
| | (0.0677) | (0.229) |
| Middle East | -0.150* | -0.438 |
| | (0.0881) | (0.305) |
| Start Date | -0.000929 | 0.00288 |
| | (0.00100) | (0.00308) |
| Days Since Hack1 | 0.00386*** | 0.00286 |
| | (0.00123) | (0.00387) |
| Holiday Hack Tally | -0.00962 | -0.0330 |
| | (0.0109) | (0.0336) |
| Tally | -0.00165*** | -0.000215 |
| | (0.000122) | (0.000403) |
| No Hack Tally | -0.00496*** | -0.000978 |
| | (0.000788) | (0.00257) |
| Hack Average | 1.670*** | -0.0486 |
| | (0.151) | (0.517) |

**Table B2. Individual Holiday Effects Logistic Regression (continued)**

| | | |
|---|---|---|
| Holiday Count | 0.0128 | 0.0416 |
| | (0.0112) | (0.0345) |
| Big Gap | -70.24 | -22.26 |
| | (0) | (0) |
| 2.month_of_weekdate | -0.143*** | -0.0538 |
| | (0.0538) | (0.171) |
| 3.month_of_weekdate | 0.0136 | -0.117 |
| | (0.0739) | (0.233) |
| 4.month_of_weekdate | -0.00240 | -0.164 |
| | (0.101) | (0.315) |
| 5.month_of_weekdate | 0.246* | 0.0989 |
| | (0.129) | (0.397) |
| 6.month_of_weekdate | 0.220 | -0.0775 |
| | (0.157) | (0.486) |
| 7.month_of_weekdate | 0.105 | -0.440 |
| | (0.187) | (0.576) |
| 8.month_of_weekdate | 0.205 | -0.293 |
| | (0.216) | (0.667) |
| 9.month_of_weekdate | 0.232 | -0.622 |
| | (0.247) | (0.759) |
| 10.month_of_weekdate | 0.105 | -1.033 |
| | (0.276) | (0.852) |
| 11.month_of_weekdate | 0.205 | -0.645 |
| | (0.306) | (0.941) |
| 12.month_of_weekdate | 0.262 | -0.869 |
| | (0.337) | (1.035) |
| 2002.year_of_weekdate | 25.87 | -2.994 |
| | (0) | (0) |
| 2003.year_of_weekdate | -5.547 | 7.743 |
| | (0) | (0) |
| 2004.year_of_weekdate | 27.20 | -4.166 |
| | (0) | (0) |
| 2005.year_of_weekdate | -13.83 | 9.755 |
| | (16.49) | (50.67) |
| 2006.year_of_weekdate | -13.55 | 8.344 |
| | (16.86) | (51.79) |
| 2007.year_of_weekdate | -14.27 | -8.201 |
| | (17.22) | (0) |
| 2008.year_of_weekdate | -13.83 | 6.899 |
| | (17.59) | (54.02) |
| 2009.year_of_weekdate | -12.99 | 5.218 |
| | (17.95) | (55.15) |

**Table B2. Individual Holiday Effects Logistic Regression (continued)**

| | | |
|---|---|---|
| 2010.year_of_weekdate | -11.99 | 5.991 |
| | (18.32) | (56.27) |
| 2011.year_of_weekdate | -12.56 | -14.94 |
| | (18.68) | (0) |
| 2012.year_of_weekdate | -11.53 | 2.621 |
| | (19.05) | (58.52) |
| 2013.year_of_weekdate | -11.49 | 0.0750 |
| | (19.41) | (59.64) |
| 2014.year_of_weekdate | -11.20 | -0.191 |
| | (19.78) | (60.76) |
| 2015.year_of_weekdate | -11.00 | -0.973 |
| | (20.15) | (61.88) |
| 2016.year_of_weekdate | -10.84 | -2.324 |
| | (20.51) | (63.01) |
| 2017.year_of_weekdate | -10.47 | -2.904 |
| | (20.88) | (64.13) |
| 2018.year_of_weekdate | -9.938 | -4.039 |
| | (21.24) | (65.25) |
| 2019.year_of_weekdate | -9.870 | -4.935 |
| | (21.61) | (66.37) |
| 2020.year_of_weekdate | -9.645 | -6.398 |
| | (21.97) | (67.50) |
| 2021.year_of_weekdate | -9.328 | -7.704 |
| | (22.34) | (68.62) |
| 2022.year_of_weekdate | -9.326 | -8.186 |
| | (22.71) | (69.75) |
| 2023.year_of_weekdate | -8.490 | -7.750 |
| | (23.07) | (70.86) |
| 2024.year_of_weekdate | -6.991 | -26.80 |
| | (23.44) | (0) |
| var(_cons[notifierx]) | 0.201*** | 2.189*** |
| | (0.0234) | (0.308) |
| Constant | 27.42 | -62.25 |
| | (0) | (0) |
| Observations | 425,162 | 425,162 |
| Number of groups | 230 | 230 |

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

**Table B3. Aggregated Holiday Effect Negative Binomial Regression**

| VARIABLES | (1)<br>hack | (2)<br>special |
|---|---|---|
| Holiday | -0.00804 | -0.0963 |
| | (0.0815) | (0.249) |
| Ideological | 0.140 | -0.248 |
| | (0.104) | (0.421) |
| Team | -0.140* | -0.279 |
| | (0.0760) | (0.304) |
| Middle East | -0.172* | -0.612 |
| | (0.0991) | (0.403) |
| Start Date | 0.00179 | -0.00143 |
| | (0.00152) | (0.00437) |
| Days Since Hack1 | -0.00687*** | -0.0109** |
| | (0.00186) | (0.00550) |
| Holiday Hack Tally | -0.0202 | -0.0342 |
| | (0.0162) | (0.0507) |
| Tally | 0.000121 | 0.000861 |
| | (0.000181) | (0.000558) |
| No Hack Tally | 0.00815*** | 0.00843** |
| | (0.00116) | (0.00369) |
| Hack Average | 2.710*** | 0.285 |
| | (0.184) | (0.690) |
| Holiday Count | 0.0274* | 0.0442 |
| | (0.0166) | (0.0518) |
| Big Gap | -28.86 | -41.96 |
| | (4,083) | (9.953e+06) |
| 2.month_of_weekdate | -0.448*** | -0.0372 |
| | (0.0803) | (0.242) |
| 3.month_of_weekdate | -0.262** | 0.0330 |
| | (0.111) | (0.324) |
| 4.month_of_weekdate | -0.187 | 0.352 |
| | (0.154) | (0.443) |
| 5.month_of_weekdate | -0.0188 | 1.232** |
| | (0.195) | (0.562) |
| 6.month_of_weekdate | -0.189 | 0.677 |
| | (0.238) | (0.689) |
| 7.month_of_weekdate | -0.539* | 0.612 |
| | (0.282) | (0.814) |
| 8.month_of_weekdate | -0.464 | 0.898 |
| | (0.329) | (0.949) |
| 9.month_of_weekdate | -0.553 | 0.828 |
| | (0.374) | (1.068) |

**Table B3. Aggregated Holiday Effect Negative Binomial Regression (continued)**

| | | |
|---|---|---|
| 10.month_of_weekdate | -0.696* | 0.180 |
| | (0.420) | (1.209) |
| 11.month_of_weekdate | -0.588 | 0.728 |
| | (0.465) | (1.339) |
| 12.month_of_weekdate | -0.601 | 0.745 |
| | (0.513) | (1.471) |
| 2002.year_of_weekdate | 1.534 | -17.56 |
| | (6.445) | (6.566e+08) |
| 2003.year_of_weekdate | -15.76 | 6.522 |
| | (1.187e+08) | (0) |
| 2004.year_of_weekdate | 1.856 | -16.87 |
| | (6.543) | (2.816e+08) |
| 2005.year_of_weekdate | -1.897 | 17.44 |
| | (5.054) | (71.98) |
| 2006.year_of_weekdate | -2.751 | 17.94 |
| | (5.312) | (73.56) |
| 2007.year_of_weekdate | -4.905 | -20.20 |
| | (5.620) | (2.119e+08) |
| 2008.year_of_weekdate | -5.009 | 19.41 |
| | (5.961) | (76.76) |
| 2009.year_of_weekdate | -5.449 | 19.77 |
| | (6.327) | (78.35) |
| 2010.year_of_weekdate | -5.397 | 21.31 |
| | (6.725) | (79.97) |
| 2011.year_of_weekdate | -7.911 | -16.27 |
| | (7.156) | (9.851e+07) |
| 2012.year_of_weekdate | -7.319 | 22.21 |
| | (7.580) | (83.13) |
| 2013.year_of_weekdate | -8.130 | 20.92 |
| | (8.030) | (84.72) |
| 2014.year_of_weekdate | -8.387 | 22.89 |
| | (8.494) | (86.31) |
| 2015.year_of_weekdate | -9.611 | 23.18 |
| | (8.964) | (87.91) |
| 2016.year_of_weekdate | -10.34 | 23.96 |
| | (9.444) | (89.50) |
| 2017.year_of_weekdate | -10.86 | 24.44 |
| | (9.933) | (91.10) |
| 2018.year_of_weekdate | -11.37 | 24.94 |
| | (10.43) | (92.71) |
| 2019.year_of_weekdate | -12.29 | 25.60 |
| | (10.93) | (94.30) |
| 2020.year_of_weekdate | -12.90 | 25.73 |
| | (11.44) | (95.90) |

**Table B3. Aggregated Holiday Effect Negative Binomial Regression (continued)**

| | | |
|---|---|---|
| 2021.year_of_weekdate | -13.69 | 25.68 |
| | (11.95) | (97.50) |
| 2022.year_of_weekdate | -13.96 | 27.56 |
| | (12.46) | (99.09) |
| 2023.year_of_weekdate | -14.40 | 29.35 |
| | (12.98) | (100.7) |
| 2024.year_of_weekdate | -14.06 | -12.24 |
| | (13.54) | (0) |
| lnalpha | 2.971*** | 4.220*** |
| | (0.0104) | (0.0397) |
| var(_cons[notifierx]) | 0.231*** | 3.874*** |
| | (0.0307) | (0.534) |
| Constant | -27.52 | 0.422 |
| | (23.21) | (0) |
| | | |
| Observations | 425,162 | 425,162 |
| Number of groups | 230 | 230 |

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

**Table B4. Individual Holiday Effects Negative Binomial Regression**

| VARIABLES | (1)<br>hack | (2)<br>special |
|---|---|---|
| Christmas | -0.385 | -0.195 |
| | (0.348) | (0.898) |
| Team*Christmas | 1.297*** | 0.189 |
| | (0.498) | (1.771) |
| New Years | 0.215 | -2.091* |
| | (0.247) | (1.247) |
| Independence Day | 0.364 | -0.878 |
| | (0.252) | (0.788) |
| Yom Kippur | -0.493* | 0.942 |
| | (0.261) | (0.779) |
| Rosh Hashanah | 0.0396 | -0.559 |
| | (0.253) | (0.870) |
| Eid al-Fitr | -0.781*** | -1.319 |
| | (0.264) | (0.865) |
| Labor Day | 0.457* | 1.818*** |
| | (0.244) | (0.607) |
| Thanksgiving | -0.428* | -0.0765 |
| | (0.256) | (0.742) |
| Ramadan start | -0.330 | -2.065** |
| | (0.245) | (0.889) |
| Eid al-Adha | -0.184 | -0.795 |
| | (0.254) | (0.795) |
| Ideological | 0.137 | -0.234 |
| | (0.104) | (0.422) |
| Team | -0.146* | -0.289 |
| | (0.0758) | (0.305) |
| Middle East | -0.176* | -0.610 |
| | (0.0989) | (0.405) |
| Start Date | 0.00223 | -0.000815 |
| | (0.00154) | (0.00442) |
| Days Since Hack1 | -0.00630*** | -0.0103* |
| | (0.00188) | (0.00554) |
| Holiday Hack Tally | -0.0219 | -0.0375 |
| | (0.0162) | (0.0509) |
| Tally | 0.000110 | 0.000853 |
| | (0.000181) | (0.000559) |
| No Hack Tally | 0.00799*** | 0.00837** |
| | (0.00116) | (0.00370) |
| Hack Average | 2.716*** | 0.270 |
| | (0.183) | (0.693) |

**Table B4. Individual Holiday Effects Negative Binomial Regression (continued)**

| | | |
|---|---|---|
| Holiday Count | 0.0288* | 0.0477 |
| | (0.0166) | (0.0520) |
| Big Gap | -30.03 | -41.21 |
| | (7,298) | (6.677e+06) |
| 2.month_of_weekdate | -0.454*** | -0.0920 |
| | (0.0806) | (0.244) |
| 3.month_of_weekdate | -0.277** | -0.0213 |
| | (0.112) | (0.326) |
| 4.month_of_weekdate | -0.218 | 0.276 |
| | (0.155) | (0.446) |
| 5.month_of_weekdate | -0.0532 | 1.152** |
| | (0.196) | (0.567) |
| 6.month_of_weekdate | -0.234 | 0.572 |
| | (0.240) | (0.695) |
| 7.month_of_weekdate | -0.616** | 0.517 |
| | (0.285) | (0.823) |
| 8.month_of_weekdate | -0.547* | 0.747 |
| | (0.332) | (0.959) |
| 9.month_of_weekdate | -0.667* | 0.543 |
| | (0.378) | (1.081) |
| 10.month_of_weekdate | -0.802* | -0.0448 |
| | (0.424) | (1.222) |
| 11.month_of_weekdate | -0.704 | 0.504 |
| | (0.469) | (1.352) |
| 12.month_of_weekdate | -0.757 | 0.509 |
| | (0.518) | (1.486) |
| 2002.year_of_weekdate | 1.369 | -17.77 |
| | (6.441) | (4.390e+08) |
| 2003.year_of_weekdate | -17.36 | 5.413 |
| | (4.056e+08) | (0) |
| 2004.year_of_weekdate | 1.401 | -17.52 |
| | (6.544) | (1.883e+08) |
| 2005.year_of_weekdate | -2.528 | 15.80 |
| | (5.064) | (72.82) |
| 2006.year_of_weekdate | -3.536 | 16.10 |
| | (5.328) | (74.42) |
| 2007.year_of_weekdate | -5.863 | -21.48 |
| | (5.643) | (1.434e+08) |
| 2008.year_of_weekdate | -6.128 | 17.11 |
| | (5.992) | (77.66) |
| 2009.year_of_weekdate | -6.742 | 17.24 |
| | (6.365) | (79.27) |
| 2010.year_of_weekdate | -6.843 | 18.57 |
| | (6.771) | (80.90) |

**Table B4. Individual Holiday Effects Negative Binomial Regression (continued)**

| | | |
|---|---|---|
| 2011.year_of_weekdate | -9.528 | -18.45 |
| | (7.209) | (6.710e+07) |
| 2012.year_of_weekdate | -9.075 | 19.01 |
| | (7.642) | (84.10) |
| 2013.year_of_weekdate | -10.05 | 17.49 |
| | (8.099) | (85.72) |
| 2014.year_of_weekdate | -10.47 | 19.20 |
| | (8.572) | (87.32) |
| 2015.year_of_weekdate | -11.86 | 19.31 |
| | (9.050) | (88.94) |
| 2016.year_of_weekdate | -12.74 | 19.88 |
| | (9.538) | (90.55) |
| 2017.year_of_weekdate | -13.45 | 20.11 |
| | (10.04) | (92.17) |
| 2018.year_of_weekdate | -14.11 | 20.40 |
| | (10.54) | (93.79) |
| 2019.year_of_weekdate | -15.20 | 20.85 |
| | (11.05) | (95.40) |
| 2020.year_of_weekdate | -15.97 | 20.75 |
| | (11.56) | (97.02) |
| 2021.year_of_weekdate | -16.92 | 20.51 |
| | (12.08) | (98.64) |
| 2022.year_of_weekdate | -17.34 | 22.16 |
| | (12.60) | (100.3) |
| 2023.year_of_weekdate | -17.95 | 23.77 |
| | (13.12) | (101.9) |
| 2024.year_of_weekdate | -17.77 | -17.38 |
| | (13.69) | (2.228e+09) |
| lnalpha | 2.970*** | 4.214*** |
| | (0.0104) | (0.0396) |
| var(_cons[notifierx]) | 0.230*** | 3.904*** |
| | (0.0305) | (0.535) |
| Constant | -34.20 | -8.037 |
| | (23.50) | (0) |
| Observations | 425,162 | 425,162 |
| Number of groups | 230 | 230 |

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

**Table B5. Sensitivity Analysis for All Defacements**

| VARIABLES | **Ideological** hack | **Team** hack | **Middle East** hack | **Unaffiliated** hack |
|---|---|---|---|---|
| Christmas | -1.359 | 0.985*** | -0.271 | -0.321 |
| | (0.950) | (0.363) | (0.736) | (0.417) |
| Team*Christmas | 3.110** | - | 2.408** | - |
| | (1.291) | | (1.209) | |
| New Years | -2.441*** | 0.372 | -1.546** | 0.360 |
| | (0.832) | (0.366) | (0.618) | (0.390) |
| Independence Day | 0.635 | 0.328 | 0.566 | 0.325 |
| | (0.583) | (0.390) | (0.549) | (0.394) |
| Yom Kippur | -0.426 | -0.976** | -1.751** | 0.0215 |
| | (0.636) | (0.435) | (0.719) | (0.400) |
| Rosh Hashanah | -0.306 | 0.251 | -0.368 | 0.136 |
| | (0.580) | (0.382) | (0.619) | (0.404) |
| Eid al-Fitr | 0.0551 | -0.845** | -0.687 | -0.719* |
| | (0.616) | (0.405) | (0.628) | (0.410) |
| Labor Day | 0.910* | 0.446 | 0.459 | 0.773** |
| | (0.540) | (0.383) | (0.579) | (0.375) |
| Thanksgiving | -0.483 | -0.127 | -0.376 | -0.736* |
| | (0.630) | (0.375) | (0.601) | (0.415) |
| Ramadan start | -1.108* | -0.278 | -0.882 | -0.105 |
| | (0.619) | (0.382) | (0.581) | (0.380) |
| Eid al-Adha | 0.0442 | -0.0437 | 0.304 | -0.435 |
| | (0.614) | (0.413) | (0.573) | (0.397) |
| Ideological | - | 0.153 | 0.227 | - |
| | | (0.175) | (0.170) | |
| Team | -0.188 | - | -0.235 | - |
| | (0.190) | | (0.179) | |
| Middle East | -0.0837 | -0.360* | | |
| | (0.194) | (0.194) | | |
| Start Date | 0.00214 | 0.00374 | -0.000992 | 0.00284 |
| | (0.00363) | (0.00231) | (0.00362) | (0.00246) |
| Days Since Hack1 | -0.0113** | -0.00570* | -0.00641 | -0.00714** |
| | (0.00464) | (0.00296) | (0.00490) | (0.00300) |
| Holiday Hack Tally | -0.0595 | -0.0106 | -0.0141 | -0.0418 |
| | (0.0461) | (0.0255) | (0.0455) | (0.0264) |
| Tally | 0.000293 | 0.000244 | -0.000674 | 0.000203 |
| | (0.000424) | (0.000293) | (0.000453) | (0.000298) |
| No Hack Tally | 0.0120*** | 0.00937*** | 0.00531 | 0.00851*** |
| | (0.00321) | (0.00200) | (0.00364) | (0.00174) |
| Hack Average | 4.149*** | 3.284*** | 3.512*** | 1.969*** |
| | (0.583) | (0.294) | (0.443) | (0.285) |
| Holiday Count | 0.0663 | 0.0124 | 0.0205 | 0.0604** |
| | (0.0474) | (0.0259) | (0.0467) | (0.0277) |
| Big Gap | -26.66 | -27.75 | -26.13 | -30.60 |
| | (3,478) | (4,645) | (2,370) | (12,439) |

**Table B5. Sensitivity Analysis for All Defacements (continued)**

| | | | | |
|---|---|---|---|---|
| 2.month_of_weekdate | -0.662*** | -0.695*** | -0.901*** | 0.0149 |
| | (0.190) | (0.124) | (0.187) | (0.127) |
| 3.month_of_weekdate | -0.349 | -0.315* | -0.360 | -0.134 |
| | (0.262) | (0.171) | (0.264) | (0.177) |
| 4.month_of_weekdate | -0.295 | -0.422* | -0.247 | 0.0435 |
| | (0.362) | (0.232) | (0.366) | (0.250) |
| 5.month_of_weekdate | -0.0727 | -0.187 | 0.0688 | 0.155 |
| | (0.458) | (0.296) | (0.461) | (0.317) |
| 6.month_of_weekdate | -0.0818 | -0.388 | -0.0479 | 0.0137 |
| | (0.567) | (0.363) | (0.566) | (0.385) |
| 7.month_of_weekdate | -0.817 | -0.819* | -0.446 | -0.484 |
| | (0.662) | (0.431) | (0.665) | (0.458) |
| 8.month_of_weekdate | -0.926 | -0.985** | -0.412 | -0.211 |
| | (0.773) | (0.501) | (0.774) | (0.533) |
| 9.month_of_weekdate | -0.842 | -0.960* | -0.207 | -0.681 |
| | (0.882) | (0.569) | (0.886) | (0.608) |
| 10.month_of_weekdate | -1.280 | -1.169* | -0.432 | -0.714 |
| | (1.000) | (0.639) | (0.996) | (0.682) |
| 11.month_of_weekdate | -0.874 | -1.424** | 0.00123 | -0.435 |
| | (1.107) | (0.708) | (1.109) | (0.752) |
| 12.month_of_weekdate | -0.907 | -1.290* | -0.134 | -0.662 |
| | (1.222) | (0.781) | (1.224) | (0.828) |
| 2006.year_of_weekdate | | -1.645* | | -4.786 |
| | | (0.925) | | (6.358) |
| 2007.year_of_weekdate | | -4.615** | -9.177 | -7.042 |
| | | (1.794) | (1.679e+06) | (7.003) |
| 2008.year_of_weekdate | | -7.350*** | 0.893 | -6.984 |
| | | (2.590) | (5.397) | (7.717) |
| 2009.year_of_weekdate | | -7.644** | -1.972 | -7.172 |
| | | (3.406) | (4.093) | (8.451) |
| 2010.year_of_weekdate | | -6.358 | -0.497 | -8.257 |
| | | (6.137) | (5.347) | (9.228) |
| 2011.year_of_weekdate | -3.232 | -9.709* | -1.358 | -11.35 |
| | (257,924) | (5.245) | (6.802) | (10.04) |
| 2012.year_of_weekdate | 0.0370 | -8.640 | 0.417 | -11.11 |
| | (2.781) | (5.922) | (7.989) | (10.83) |
| 2013.year_of_weekdate | -1.490 | -10.68 | 0.653 | -12.79 |
| | (4.071) | (6.767) | (9.285) | (11.67) |
| 2014.year_of_weekdate | -2.460 | -12.86* | 1.981 | -13.34 |
| | (5.385) | (7.608) | (10.61) | (12.50) |
| 2015.year_of_weekdate | -3.956 | -14.33* | 1.305 | -14.80 |
| | (6.693) | (8.446) | (11.93) | (13.34) |
| 2016.year_of_weekdate | -5.290 | -16.19* | 1.235 | -15.46 |
| | (8.016) | (9.288) | (13.24) | (14.19) |
| 2017.year_of_weekdate | -6.176 | -17.44* | 1.704 | -16.43 |
| | (9.339) | (10.14) | (14.56) | (15.04) |
| 2018.year_of_weekdate | -5.951 | -18.52* | 2.680 | -17.51 |
| | (10.66) | (10.98) | (15.88) | (15.90) |

**Table B5. Sensitivity Analysis for All Defacements (continued)**

| | | | | |
|---|---|---|---|---|
| 2019.year_of_weekdate | -6.805 | -20.00* | 2.826 | -18.91 |
| | (11.98) | (11.83) | (17.20) | (16.77) |
| 2020.year_of_weekdate | -7.693 | -21.49* | 3.066 | -19.68 |
| | (13.30) | (12.67) | (18.52) | (17.64) |
| 2021.year_of_weekdate | -8.732 | -23.11* | 3.246 | -20.83 |
| | (14.62) | (13.51) | (19.84) | (18.51) |
| 2022.year_of_weekdate | -8.875 | -23.32 | 2.510 | -21.77 |
| | (15.96) | (14.36) | (21.16) | (19.39) |
| 2023.year_of_weekdate | -8.865 | -25.34* | 4.997 | -22.23 |
| | (17.31) | (15.21) | (22.48) | (20.26) |
| 2024.year_of_weekdate | -10.22 | -23.83 | 5.026 | |
| | (18.84) | (16.13) | (23.86) | |
| teamchris | 3.110** | | 2.408** | |
| | (1.291) | | (1.209) | |
| o.ideological | - | | | - |
| | | | | |
| team | -0.188 | | -0.235 | |
| | (0.190) | | (0.179) | |
| lnalpha | 2.891*** | 2.945*** | 3.024*** | 2.948*** |
| | (0.0254) | (0.0160) | (0.0240) | (0.0163) |
| var(_cons[notifierx]) | 0.242*** | 0.265*** | 0.197*** | 0.274*** |
| | (0.0761) | (0.0535) | (0.0626) | (0.0578) |
| o.middle_east | | | - | - |
| | | | | |
| 2002.year_of_weekdate | | | | 1.433 |
| | | | | (6.411) |
| 2003.year_of_weekdate | | | | -6.560 |
| | | | | (2.035e+06) |
| 2004.year_of_weekdate | | | | 0.917 |
| | | | | (6.798) |
| 2005.year_of_weekdate | | | | -8.739 |
| | | | | (1.732e+06) |
| Constant | -40.49 | -62.05 | 17.32 | -43.91 |
| | (66.37) | (38.10) | (60.93) | (37.26) |
| Observations | 73,053 | 159,019 | 94,142 | 182,827 |
| Number of groups | 38 | 92 | 45 | 97 |

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

**Table B6. Sensitivity Analysis for Special Defacements**

| VARIABLES | **Ideological** special | **Team** special | **Middle East** special | **Unaffiliated** special |
|---|---|---|---|---|
| Christmas | -26.85 | 0.352 | 0.903 | -31.60 |
| | (490,436) | (1.683) | (1.570) | (2.802e+06) |
| Team*Christmas | -3.467 | | -30.01 | |
| | (3.866e+06) | | (3.712e+06) | |
| New Years | -26.52 | -19.82 | -28.37 | -0.603 |
| | (423,727) | (11,617) | (1.166e+06) | (1.414) |
| Independence Day | 0.383 | -0.354 | 0.513 | -2.179 |
| | (1.373) | (1.541) | (1.506) | (1.405) |
| Yom Kippur | -26.29 | 2.049* | -28.54 | -2.803* |
| | (442,440) | (1.046) | (1.098e+06) | (1.692) |
| Rosh Hashanah | 0.119 | 1.021 | -29.00 | -31.81 |
| | (1.569) | (1.100) | (1.122e+06) | (2.782e+06) |
| Eid al-Fitr | 1.066 | -0.923 | 0.419 | -32.08 |
| | (1.180) | (1.434) | (1.523) | (2.719e+06) |
| Labor Day | 0.756 | 2.613*** | 0.866 | -0.561 |
| | (1.225) | (0.906) | (1.282) | (1.073) |
| Thanksgiving | 0.314 | -1.306 | -0.652 | 0.946 |
| | (1.555) | (1.377) | (1.674) | (1.059) |
| Ramadan start | -26.33 | 0.559 | -28.08 | -2.184* |
| | (412,002) | (0.970) | (1.173e+06) | (1.283) |
| Eid al-Adha | 0.410 | -1.611 | 0.706 | -2.931* |
| | (1.509) | (1.444) | (1.493) | (1.546) |
| Ideological | | 0.267 | 0.235 | |
| | | (0.616) | (0.638) | |
| Team | 0.493 | | -0.163 | - |
| | (0.666) | | (0.672) | |
| Middle East | -0.627 | -0.943 | | |
| | (0.711) | (0.683) | | |
| Start Date | 0.00635 | 0.0188** | 0.0191* | -0.00841 |
| | (0.0101) | (0.00770) | (0.0107) | (0.00614) |
| Days Since Hack1 | -0.0114 | -0.00402 | 0.01000 | 0.00591 |
| | (0.0134) | (0.00962) | (0.0152) | (0.00807) |
| Holiday Hack Tally | -0.168 | 0.100 | -0.0254 | -0.115 |
| | (0.136) | (0.0850) | (0.144) | (0.0737) |
| Tally | 0.00355*** | 0.00264*** | 0.00290* | -0.00203** |
| | (0.00130) | (0.000992) | (0.00149) | (0.000892) |
| No Hack Tally | 0.0139 | 0.0245*** | 0.00810 | -0.0172*** |
| | (0.0101) | (0.00636) | (0.0118) | (0.00558) |
| Hack Average | 3.704* | 2.163** | 3.329** | 2.891*** |
| | (2.021) | (1.036) | (1.633) | (0.981) |

**Table B6. Sensitivity Analysis for Special Defacements (continued)**

| | | | | |
|---|---|---|---|---|
| Holiday Count | 0.172 | -0.0864 | 0.0151 | 0.100 |
| | (0.140) | (0.0860) | (0.149) | (0.0780) |
| 2.month_of_weekdate | -1.357** | -1.348*** | -1.028* | 0.183 |
| | (0.582) | (0.421) | (0.579) | (0.348) |
| 3.month_of_weekdate | -1.537** | -2.035*** | -2.052** | 0.957** |
| | (0.770) | (0.581) | (0.813) | (0.442) |
| 4.month_of_weekdate | -0.853 | -1.698** | -2.035* | 1.358** |
| | (1.037) | (0.763) | (1.118) | (0.618) |
| 5.month_of_weekdate | -0.846 | -1.657* | -2.903** | 2.136*** |
| | (1.348) | (0.967) | (1.441) | (0.794) |
| 6.month_of_weekdate | -0.807 | -2.889** | -3.988** | 1.975** |
| | (1.602) | (1.192) | (1.758) | (0.965) |
| 7.month_of_weekdate | -1.630 | -4.503*** | -4.211** | 2.479** |
| | (1.908) | (1.450) | (2.034) | (1.138) |
| 8.month_of_weekdate | -1.260 | -3.973** | -4.126* | 3.122** |
| | (2.213) | (1.654) | (2.342) | (1.326) |
| 9.month_of_weekdate | -1.742 | -4.606** | -4.400* | 2.605* |
| | (2.478) | (1.867) | (2.617) | (1.500) |
| 10.month_of_weekdate | -3.444 | -5.766*** | -6.897** | 2.268 |
| | (2.827) | (2.123) | (3.021) | (1.685) |
| 11.month_of_weekdate | -2.681 | -5.886** | -6.400* | 2.956 |
| | (3.116) | (2.346) | (3.278) | (1.879) |
| 12.month_of_weekdate | -2.043 | -6.190** | -6.987* | 3.055 |
| | (3.405) | (2.593) | (3.607) | (2.059) |
| 2006.year_of_weekdate | | -6.526* | | 6.833 |
| | | (3.338) | | (1.734e+06) |
| 2007.year_of_weekdate | | -32.69 | -13.30 | 9.940 |
| | | (16,779) | (982,532) | (1.686e+06) |
| 2008.year_of_weekdate | | -19.77** | -20.02 | 42.17 |
| | | (8.644) | (949,302) | (107.8) |
| 2009.year_of_weekdate | | -26.24** | -26.57 | 16.11 |
| | | (11.38) | (750,386) | (1.574e+06) |
| 2010.year_of_weekdate | | -52.48 | -33.33 | 49.34 |
| | | (17,022) | (697,809) | (112.2) |
| 2011.year_of_weekdate | -9.998 | -59.17 | -40.10 | 22.39 |
| | (636,360) | (17,808) | (674,615) | (1.584e+06) |
| 2012.year_of_weekdate | 13.73 | -45.25** | -19.16 | 53.67 |
| | (192.3) | (19.68) | (203.6) | (116.7) |
| 2013.year_of_weekdate | 9.171 | -53.07** | -28.12 | 55.68 |
| | (196.0) | (22.49) | (207.5) | (119.0) |
| 2014.year_of_weekdate | 7.071 | -60.68** | -33.72 | 61.11 |
| | (199.7) | (25.28) | (211.4) | (121.2) |
| 2015.year_of_weekdate | 4.033 | -66.00** | -41.38 | 65.61 |
| | (203.4) | (28.09) | (215.3) | (123.4) |

**Table B6. Sensitivity Analysis for Special Defacements (continued)**

| | | | | |
|---|---|---|---|---|
| 2016.year_of_weekdate | -0.0863 | -74.28** | -48.52 | 69.39 |
| | (207.1) | (30.89) | (219.2) | (125.7) |
| 2017.year_of_weekdate | -2.500 | -81.77** | -56.08 | 71.97 |
| | (210.8) | (33.69) | (223.1) | (127.9) |
| 2018.year_of_weekdate | -4.594 | -88.13** | -62.52 | 74.66 |
| | (214.5) | (36.52) | (227.1) | (130.2) |
| 2019.year_of_weekdate | -6.914 | -94.52** | -69.44 | 77.51 |
| | (218.1) | (39.30) | (230.9) | (132.4) |
| 2020.year_of_weekdate | -9.942 | -101.9** | -76.55 | 80.22 |
| | (221.8) | (42.12) | (234.8) | (134.7) |
| 2021.year_of_weekdate | -13.50 | -111.2** | -84.08 | 80.98 |
| | (225.5) | (44.93) | (238.7) | (136.9) |
| 2022.year_of_weekdate | -14.51 | -116.0** | -90.08 | 84.70 |
| | (229.2) | (47.72) | (242.7) | (139.2) |
| 2023.year_of_weekdate | -15.99 | -120.8** | -124.7 | 90.23 |
| | (232.9) | (50.52) | (761,430) | (141.4) |
| 2024.year_of_weekdate | -44.23 | -146.4 | -131.1 | |
| | (2.851e+06) | (83,818) | (5.960e+06) | |
| lnalpha | 4.833*** | 5.150*** | 5.198*** | 4.956*** |
| | (0.117) | (0.0714) | (0.111) | (0.0532) |
| var(_cons[notifierx]) | 2.955*** | 3.400*** | 2.977*** | 3.870*** |
| | (1.072) | (0.742) | (1.050) | (0.774) |
| o.middle_east | | | - | - |
| | | | | |
| 2002.year_of_weekdate | | | | -5.538 |
| | | | | (2.375e+06) |
| 2003.year_of_weekdate | | | | -2.407 |
| | | | | (2.323e+06) |
| 2004.year_of_weekdate | | | | 0.528 |
| | | | | (1.969e+06) |
| 2005.year_of_weekdate | | | | 3.555 |
| | | | | (1.742e+06) |
| Constant | -138.1 | -315.9** | -349.3 | 96.92 |
| | (0) | (126.7) | (0) | (0) |
| Observations | 73,053 | 159,019 | 94,142 | 182,827 |
| Number of groups | 38 | 92 | 45 | 97 |

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

## List of References


Abdulai, M. A. (2020). Examining the Effect of Victimization Experience on Fear of Cybercrime: University Students' Experience of Credit/Debit Card Fraud. *International Journal of Cyber Criminology*, *14*(1), 157–174. https://doi.org/10.5281/zenodo.3749468

Aggarwal, P., Maqbool, Z., Grover, A., Pammi, V. S., Singh, S., & Dutt, V. (2015). Cyber security: A game-theoretic analysis of Defender and attacker strategies in defacing-website games. *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. https://doi.org/10.1109/cybersa.2015.7166127

Akers, Ronald L. (1998). Social Learning and Social Structure: A General Theory of Crime and Deviance. Boston: *Northeastern University Press.*

Akins, J. K., & Winfree, L. T. (2017). Social learning theory and becoming a terrorist. *The Handbook of the Criminology of Terrorism*, 133–149. https://doi.org/10.1002/9781118923986.ch8

Alata, E., Dacier, M., Deswarte, Y., Kaaâniche, M., Kortchinsky, K., Nicomette, V., Pham, V. H., & Pouget, F. (2006). Collection and analysis of attack data based on honeypots deployed on the internet. *Quality of Protection*, 79–91. https://doi.org/10.1007/978-0-387-36584-8_7

Albalawi, M., Aloufi, R., Alamrani, N., Albalawi, N., Aljaedi, A., & Alharbi, A. R. (2022). Website defacement detection and monitoring methods: A Review. *Electronics*, *11*(21), 3573. https://doi.org/10.3390/electronics11213573

Al-Rizzo, H. M. (2008). The undeclared cyberspace war between Hezbollah and Israel*. *Contemporary Arab Affairs*, 1(3), 391–405. https://doi.org/10.1080/17550910802163889

Alsayed, A. O., & Bilgrami, A. L. (2017). E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities . *International Journal of Emerging Technology and Advanced Engineering*, *7*(1).

Arachchilage, N. A., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, *60*, 185–197. https://doi.org/10.1016/j.chb.2016.02.065

Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber Physical Systems Security: Analysis, challenges and solutions. *Computers & Security*, *68*, 81–97. https://doi.org/10.1016/j.cose.2017.04.005

Aslan, C. B., Li, S., Celebi, F. V., & Tian, H. (2020). The world of Defacers: Looking through the lens of their activities on Twitter. *IEEE Access*, *8*, 204132–204143. https://doi.org/10.1109/access.2020.3037015

Bahrami, P. N., Dehghantanha, A., Tooska Dargahi, T., Parizi, R. M., Choo, K.-K. R., & Javadi, H. H. S. (2019, August). Cyber kill chain-based taxonomy of Advanced Persistent Threat Actors ... https://www.researchgate.net/publication/350342843_Cyber_Kill_Chain-Based_Taxonomy_of_Advanced_Persistent_Threat_Actors_Analogy_of_Tactics_Techniques_and_Procedures

Baird, A., While, D., Flynn, S., Ibrahim, S., Kapur, N., Appleby, L., & Shaw, J. (2019). Do homicide rates increase during weekends and national holidays? *The Journal of Forensic Psychiatry & Psychology*, *30*(3), 367–380. https://doi.org/10.1080/14789949.2019.1600711

Balduzzi, M., Flores, R., Gu, L., & Maggi, F. (2018). *A deep dive into defacement: How geopolitical events trigger web attacks*. Trend Micro. https://maggi.cc/publication/balduzzi_defplorexwp_tr_2018/

Banerjee, S., Swearingen, T., Shillair, R., Bauer, J. M., Holt, T., & Ross, A. (2021). Using machine learning to examine cyberattack motivations on web defacement data. *Social Science Computer Review*, *40*(4), 914–932. https://doi.org/10.1177/0894439321994234

Barrett, B. (2021, September 3). *Why ransomware hackers love a holiday weekend*. Wired. https://www.wired.com/story/ransomware-hacks-holidays-weekends/

Bartoli, A., Davanzo, G., & Medvet, E. (2009). The reaction time to web site Defacements. *IEEE Internet Computing*, *13*(4), 52–58. https://doi.org/10.1109/mic.2009.91

Becker, G. S. (1968). Crime and punishment: An economic approach. *The Economic Dimensions of Crime*, 13–68. https://doi.org/10.1007/978-1-349-62853-7_2

Benson, M. L. (2013). *Crime and the life course: An introduction*. Routledge/Taylor & Francis Group.

Bickel, P. J., & Levina, E. (2008). Regularized estimation of large covariance matrices. *The Annals of Statistics*, *36*(1). https://doi.org/10.1214/009053607000000758

Blumstein, A., Cohen, J., Roth, J., & Visher, C. (1986). Criminal careers and "career criminals." *National Academy Press*.

Benson, M. L. (2013). *Crime and the life course: An introduction*. Routledge.

Bock, G., & Goode, J. (1996). Genetics of criminal and antisocial behaviour. *Antisocial Behavior*.

Borg, M. J. (1997). Crime and public policy: Putting theory to work. edited by Hugh D. Barlow. Westview Press, 1995. 301 pp. *Social Forces*, *76*(1), 348–350. https://doi.org/10.1093/sf/76.1.348

Borgolte, K., Kruegel, C., & Vigna, G. (2015). 24th USENIX Security Symposium (USENIX Security 15). In *Meerkat: Detecting website defacements through image-based object recognition.* (pp. 595–610). Washington D.C.; USENIX Association.

Bossler, A. M. (2019). Perceived formal and informal sanctions on the willingness to commit cyber attacks against domestic and foreign targets. *Journal of Crime and Justice, 42*(5), 599–615. https://doi.org/10.1080/0735648x.2019.1692423

Bossler, A. M. (2021). Neutralizing cyber attacks: Techniques of neutralization and willingness to commit cyber attacks. *American Journal of Criminal Justice*, *46*(6), 911–934. https://doi.org/10.1007/s12103-021-09654-5

Bossler, A. M., & Berenblum, T. (2019). Introduction: New directions in cybercrime research. *Journal of Crime and Justice*, *42*(5), 495–499. https://doi.org/10.1080/0735648x.2019.1692426

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*, *3*(1), 400–420.

Bossler, A. M., Holt, T. J., Cross, C., & Burruss, G. W. (2019). Policing fraud in England and Wales: Examining constables' and sergeants' online fraud preparedness. *Security Journal*, *33*(2), 311–328. https://doi.org/10.1057/s41284-019-00187-5

Branic, N. (2015). Routine activities theory. *The Encyclopedia of Crime and Punishment*, 1–3. https://doi.org/10.1002/9781118519639.wbecpx059

Brown, C. F., Demaray, M. K., & Secord, S. M. (2014). Cyber victimization in middle school and relations to social emotional outcomes. *Computers in Human Behavior*, *35*, 12–21. https://doi.org/10.1016/j.chb.2014.02.014

Bryk, A. S., & Raudenbush, S. W. (1988). Toward a more appropriate conceptualization of research on school effects: A three-level hierarchical linear model. *American Journal of Education*, *97*(1), 65–108. https://doi.org/10.1086/443913

Buil-Gil, D., & Saldaña-Taboada, P. (2021). Offending concentration on the internet: An exploratory analysis of Bitcoin-related cybercrime. *Deviant Behavior*, *43*(12), 1453–1470. https://doi.org/10.1080/01639625.2021.1988760

Burruss, G. W., Howell, C. J., Maimon, D., & Wang, F. (2021). Website DEFACER classification: A finite mixture model approach. *Social Science Computer Review*, *40*(3), 775–787. https://doi.org/10.1177/0894439321994232

Bushway, S. D., Piquero, A. R., Broidy, L. M., Cauffman, E., & Mazerolle, P. (2001). An empirical framework for studying desistance as a process. *Criminology*, *39*(2), 491–516. https://doi.org/10.1111/j.1745-9125.2001.tb00931.x

Button, M., Lewis, C., & Tapley, J. (2009). Fraud typologies and the victims of fraud: literature review. *National Fraud Authority*.

Button, M., Lewis, C., & Tapley, J. (2012). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*(1), 36–54. https://doi.org/10.1057/sj.2012.11

Caldwell, T. (2014). The true cost of being hacked. *Computer Fraud & Security*, *2014*(6), 8–13. https://doi.org/10.1016/s1361-3723(14)70500-7

Caneppele, S., & Aebi, M. F. (2017). Crime drop or police recording flop? on the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice*, *13*(1), 66–79. https://doi.org/10.1093/police/pax055

Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., & Sweetnam, J. (2020). *Data Integrity: Identifying and Protecting Assets against Ransomware and Other Destructive Events*. https://doi.org/10.6028/nist.sp.1800-25

Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., Sweetnam, J., & Townsend, A. (2019, December 5). [project description] data confidentiality: Identifying and protecting assets and data against data breaches. CSRC. Retrieved March 21, 2023, from https://csrc.nist.gov/publications/detail/white-paper/2019/12/05/identifying-and-protecting-assets-and-data-against-data-breaches/final

Chiu, A. (2020, January 7). A government website was 'defaced' with pro-iran messaging and an image of a bloodied Trump. hackers claimed responsibility. The Washington Post. Retrieved December 13, 2021, from https://www.washingtonpost.com/nation/2020/01/06/american-government-website-defaced-iran-hackers-bloodied-trump/.

Chiu, J. L., Mansumitrchai, S., & Chiu, C. L. (2016). Privacy, security, infrastructure and cost issues in internet banking in the Philippines: Initial trust formation. *International Journal of Financial Services Management*, *8*(3), 240. https://doi.org/10.1504/ijfsm.2016.10000998

CISA. (2022, February 10). *Ransomware awareness for holidays and weekends: CISA*. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-243a

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*, 100167. https://doi.org/10.1016/j.chbr.2022.100167

Choi, K.-S. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, *2*, 308–333. https://www.researchgate.net/publication/238621672_Computer_Crime_Victimization_and_Integrated_Theory_An_Empirical_Assessment

Christiansen, B., Piekarz, A., & Hai-Jew, S. (2019). The Electronic Hive Mind and Cybersecurity: Mass-Scale Human Cognitive Limits to Explain the "Weakest Link" in Cybersecurity. In *Global Cyber Security Labor Shortage and International Business Risk* (pp. 263–348). essay, IGI Global.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. *National Institute of Standards and Technology*. https://doi.org/10.6028/nist.sp.800-61r2

Cohen, L. E., & Felson, M. (1979). Social Change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588. https://doi.org/10.2307/2094589

Cohn, E. G., & Rotton, J. (2003). Even criminals take a holiday: Instrumental and expressive crimes on major and minor holidays. *Journal of Criminal Justice*, *31*(4), 351–360. https://doi.org/10.1016/s0047-2352(03)00029-1

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and Ways Forward. *Maturitas*, *113*, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

Cross, C. A., Richards, K. M., & Smith, R. (2016). “The reporting experiences and support needs of victims of online fraud.” *Trends and Issues in Crime and Criminal Justice, Canberra: Australian Institute of Criminology*, *518*, 1–14.

Cullen, F. T., Jonson, C. L., & Nagin, D. S. (2011). Prisons do not reduce recidivism. *The Prison Journal*, *91*(3_suppl). https://doi.org/10.1177/0032885511415224

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., & Benedetto, L. (2019). A cyber-kill-chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques*, *15*(4), 277–305. https://doi.org/10.1007/s11416-019-00338-7

Das, A., Thi Nguyen, Q., & Thomas, S. (2017). Entertaining whilst defacing websites: Psychological games for Hackers. *InSITE Conference*. https://doi.org/10.28945/3721

Décary-Hétu, D., Morselli, C., & Leman-Langlois, S. (2012). Welcome to the scene: A study of social organization and recognition among warez hackers. Journal of Research in Crime and Delinquency, 49(3), 359–382. https://doi.org/bv8fnp

Decker, E. (2020). Full count?: crime rate swings, cybercrime misses and why we don’t really know the score. *Journal of National Security Law and Policy*, *10*(3), 583–604.

DeLisi, M. (2005). *Career Criminals in society*. Sage Publications.

DeLisi, M. (2006). Zeroing in on early arrest onset: Results from a population of extreme career criminals. *Journal of Criminal Justice*, *34*(1), 17–26. https://doi.org/10.1016/j.jcrimjus.2005.11.002

DeLisi, M. (2014). 4 age–crime curve and criminal career patterns. *The Development of Criminal and Antisocial Behavior*, 51–63. https://doi.org/10.1007/978-3-319-08720-7_4

DeLisi, M. (2015). Age-crime curve and criminal career patterns. In J. Morizot & L. Kazemian (Eds.), *The development of criminal and antisocial behavior: Theory, research and practical applications* (pp. 51–63). Springer International Publishing AG. https://doi.org/10.1007/978-3-319-08720-7_4

DeLisi, M., & Gatling, J. (2003). Who pays for a life of crime? an empirical assessment of the assorted victimization costs posed by career criminals. *Criminal Justice Studies*, *16*(4), 283–293. https://doi.org/10.1080/0888431032000183489

DeLisi, M., & Piquero, A. R. (2011). New frontiers in criminal careers research, 2000–2011: A state-of-the-art review. *Journal of Criminal Justice*, *39*(4), 289–301. https://doi.org/10.1016/j.jcrimjus.2011.05.001

Denning, D. E. (2011). Cyber conflict as an emergent social phenomenon. *Corporate Hacking and Technology-Driven Crime*, 170–186. https://doi.org/10.4018/978-1-61692-805-6.ch009

Denning, D. E., & Baugh, W. E. (1999). Hiding crimes in cyberspace. *Information, Communication & Society*, *2*(3), 251–276. https://doi.org/10.1080/136911899359583

Dey, D., Lahiri, A., & Zhang, G. (2012). Hacker behavior, network effects, and the security software market. *Journal of Management Information Systems*, *29*(2), 77–108. https://doi.org/10.2753/mis0742-1222290204

Digital Repository at the University of Maryland. (2014). *Abstract title of thesis: The restrictive deterrent effect of warning ...* The Restrictive Deterrent Effect of Warning Messages on the Behavior of Computer System Trespassers. https://drum.lib.umd.edu/bitstream/handle/1903/15544/Jones_umd_0117N_15230.pdf;sequence=1

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643–658. https://doi.org/10.1057/ejis.2011.23

Eaton, K. (2009, August 26). *Hacking, like the weather, is seasonal - fast company*. Fast Company. https://www.fastcompany.com/1339379/hacking-weather-seasonal

Eivazi, K. (2011). Computer Use Monitoring and privacy at work. *Computer Law & Security Review*, *27*(5), 516–523. https://doi.org/10.1016/j.clsr.2011.07.003

Elder, G. H., Jr., Liker, J. K., & Cross, C. E. (1985). "Life course dynamics: Trajectories and transitions," In P. B. Baltes & O. G. Brim, Jr. (Eds.), Life-span development and behavior (Vol. 6, pp. 109-158). New York: Academic Press.

Farrington, D. (1986). Age and crime. In: Tonry M, Morris N (eds) Crime and justice: an annual review of research. *Chicago University Press*.

Farrington, D., Loeber, R., & Van Kammen, W. (1990). Long-term criminal outcomes of hyperactivity-impulsivity-attention deficit and conduct problems in childhood. In *Straight and devious pathways from childhood to adulthood* (pp. 62–81). essay, Cambridge University Press.

Farrington, D., Radke-Yarrow, M., Block, J., & Olweus, D. (1986). Stepping stones to adult criminal careers. In *Development of antisocial and prosocial behavior* (pp. 359–384). essay, Academic Press.

Farrington, D. P., Coid, J. W., & West, D. J. (2009). The development of offending from age 8 to age 50: Recent results from the Cambridge Study in Delinquent Development. *Monatsschrift Für Kriminologie Und Strafrechtsreform*, *92*(2–3), 160–173. https://doi.org/10.1515/mks-2009-922-306

Farrington, D. P., Loeber, R., Elliott, D. S., Hawkins, J. D., Kandel, D. B., Klein, M. W., McCord, J., Rowe, D. C., & Tremblay, R. E. (1990). Advancing knowledge about the onset of delinquency and crime. *Advances in Clinical Child Psychology*, 283–342. https://doi.org/10.1007/978-1-4613-9835-6_8

FBI. (2019, September 12). *Burglary*. https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/topic-pages/burglary

FBI. (2023). *2022 1INTERNET CRIME REPORT - Internet Crime Complaint Center*. Internet Crime Report 2022. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Firdaus, R., Xue, Y., Gang, L., & Sibt e Ali, M. (2022). Artificial intelligence and human psychology in online transaction fraud. *Frontiers in Psychology*, 13, 947234.

Flanagan, W., & McMenamin, B. (1992). The playground bullies are learning to type. *Forbes*, 184–189.

Furnell, S. (2002). *Cybercrime: Vandalizing the information society*. Addison-wesley.

Furnell, S., & Dowling, S. (2019). Cyber crime: A portrait of the landscape. *Journal of Criminological Research, Policy and Practice*, *5*(1), 13–26. https://doi.org/10.1108/jcrpp-07-2018-0021

Gardella, J. H., Fisher, B. W., & Teurbe-Tolon, A. R. (2017). A systematic review and meta-analysis of cyber-victimization and educational outcomes for adolescents. *Review of Educational Research*, *87*(2), 283–308. https://doi.org/10.3102/0034654316689136

Gelman, A. (2007, November 28). *Statistical Modeling, causal inference, and social science: Clustered standard errors vs. multilevel modeling*. Statistical Modeling Causal Inference and Social Science. https://statmodeling.stat.columbia.edu/2007/11/28/clustered_stand/#:~:text=One%20big

%20advantage%20of%20multilevel%20modeling%2C%20beyond%20the,it%20gives%20separate%20estimates%20for%20the%20individual%20states.

Gelman, A., & Hill, J. (2006). *Data analysis using regression and multilevel/hierarchical models*. Cambridge University Press.

Goldstein, H. (2011). *Multilevel statistical models*. John Wiley & Sons.

Gordon, A. (2019). *A Practical Guide to Multilevel Modeling*. *2-Day MLM Workshop*. Toronto; University of Toronto.

Gosler, J. R., & Von Thaer, L. (2013). Resilient Military Systems and the Advanced Cyber Threat. *Washington, DC: Defense Science Board* . https://doi.org/10.21236/ada569975

Gotham, K. F., & Kennedy, D. B. (2019). Chapter 4 - Apartment Security I: Measuring and Analyzing Crime Foreseeability. In *Practicing forensic criminology* (pp. 76–89). essay, Academic Press.

Grabosky, P. (2016). *Cybercrime*. Oxford University Press.

Grabosky, P. (2016). The evolution of cybercrime, 2006–2016. In Holt, T. J. (Ed.). (2016). Cybercrime through an Interdisciplinary Lens. (1st ed., pp. 29–50). London, England: Routledge. https://doi.org/grts

Guerra, C., & Ingram, J. R. (2020). Assessing the relationship between lifestyle routine activities theory and online victimization using panel data. *Deviant Behavior*, *43*(1), 44–60. https://doi.org/10.1080/01639625.2020.1774707

Gupta, B. B., & Gupta, A. (2018). Assessment of honeypots. *International Journal of Cloud Applications and Computing*, *8*(1), 21–54. https://doi.org/10.4018/ijcac.2018010102

Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. *2016 International Conference on Computing, Communication and Automation (ICCCA)*. https://doi.org/10.1109/ccaa.2016.7813778

Han, M. L., Han, H. C., Kang, A. R., Kwak, B. I., Mohaisen, A., & Kim, H. K. (2016). WHAP: Web-hacking profiling using case-based reasoning. *2016 IEEE Conference on Communications and Network Security (CNS)*. https://doi.org/10.1109/cns.2016.7860503

Han, M. L., Kwak, B. I., & Kim, H. K. (2019). CBR-based decision support methodology for Cybercrime Investigation: Focused on the data-driven website defacement analysis. *Security and Communication Networks*, *2019*, 1–21. https://doi.org/10.1155/2019/1901548

Hartley, R. D. (2015). Ethical hacking pedagogy: An analysis and overview of teaching students to hack. *Journal of International Technology and Information Management*, *24*(4). https://doi.org/10.58729/1941-6679.1055

Hirschi, T., & Gottfredson, M. (1983). Age and the explanation of crime. *American Journal of Sociology*, *89*(3), 552–584. https://doi.org/10.1086/227905

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*, *15*(1), 65–79. https://doi.org/10.1057/cpcs.2012.14

Holodinsky, J. K., Austin, P. C., & Williamson, T. S. (2020). An introduction to clustered data and multilevel analyses. *Family Practice*, *37*(5), 719–722. https://doi.org/10.1093/fampra/cmaa017

Holt, T. J. (2007). Subcultural evolution? examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior*, *28*(2), 171–198. https://doi.org/10.1080/01639620601131065

Holt, T. J. (2011). THE ATTACK DYNAMICS OF POLITICAL AND RELIGIOUSLY MOTIVATED HACKERS. In T. Saadawi & L. Jordan (Eds.), *CYBER INFRASTRUCTURE PROTECTION* (pp. 159–180). Strategic Studies Institute, US Army War College. http://www.jstor.org/stable/resrep11979.10

Holt, T. J. (2012). Exploring the intersections of technology, crime, and terror. *Terrorism and Political Violence, 24*(2), 337–354. https://doi.org/10.1080/09546553.2011.648350

Holt, T. J. (2013). Exploring the social organisation and structure of stolen data markets. *Global Crime*, *14*(2–3), 155–174. https://doi.org/10.1080/17440572.2013.787925

Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice, 29*(4), 420–436. https://doi.org/10.1177/1043986213507401

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2010). Social Learning and cyber-deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice*, *33*(2), 31–61. https://doi.org/10.1080/0735648x.2010.9721287

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2016). Assessing the macro-level correlates of malware infections using a routine activities framework. *International Journal of Offender Therapy and Comparative Criminology*, *62*(6), 1720–1741. https://doi.org/10.1177/0306624x16679162

Holt, T. J., Freilich, J. D., & Chermak, S. M. (2017). Exploring the subculture of ideologically motivated Cyber-Attackers. *Journal of Contemporary Criminal Justice*, *33*(3), 212–233. https://doi.org/10.1177/1043986217699100

Holt, T. J., & Kilger, M. (2012). Examining willingness to attack critical infrastructure online and offline. *Crime & Delinquency*, *58*(5), 798–822. https://doi.org/10.1177/0011128712452963

Holt, T. J., Kilger, M., Chiang, L., & Yang, C.-S. (2016). Exploring the correlates of individual willingness to engage in ideologically motivated cyberattacks. *Deviant Behavior*, *38*(3), 356–373. https://doi.org/10.1080/01639625.2016.1197008

Holt, T. J., Lee, J. R., Freilich, J. D., Chermak, S. M., Bauer, J. M., Shillair, R., & Ross, A. (2020). An exploratory analysis of the characteristics of ideologically motivated cyberattacks. *Terrorism and Political Violence*, *34*(7), 1305–1320. https://doi.org/10.1080/09546553.2020.1777987

Holt, T. J., Leukfeldt, R., & van de Weijer, S. (2020). An examination of motivation and routine activity theory to account for cyberattacks against Dutch web sites. *Criminal Justice and Behavior*, *47*(4), 487–505. https://doi.org/10.1177/0093854819900322

Holt, T. J., Stonhouse, M., Freilich, J., & Chermak, S. M. (2019). Examining ideologically motivated cyberattacks performed by far-left groups. *Terrorism and Political Violence*, *33*(3), 527–548. https://doi.org/10.1080/09546553.2018.1551213

Holt, T. J., Strumsky, D. A., Smirnova, O., & Kilger, M. (2012). Examining the Social Networks of Malware Writers and Hackers. *International Journal of Cyber Criminology*, *6*(a).

Holt, T. J., Turner, N. D., Freilich, J. D., & Chermak, S. M. (2021). Examining the characteristics that differentiate jihadi-associated cyberattacks using routine activities theory. *Social Science Computer Review*, *40*(6), 1614–1630. https://doi.org/10.1177/08944393211023324

Holz, T., & Raynal, F. (2005). Detecting honeypots and other suspicious environments. *Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005.* https://doi.org/10.1109/iaw.2005.1495930

Hotten, R. (2020, May 31). Amazon UK website defaced with racist abuse. BBC News. Retrieved December 13, 2021, from https://www.bbc.com/news/business-52867334.

Howell, C. Jordan, Burruss, G. W., Maimon, D., & Sahani, S. (2019). Website defacement and routine activities: Considering the importance of hackers' valuations of potential targets. *Journal of Crime and Justice*, *42*(5), 536–550. https://doi.org/10.1080/0735648x.2019.1691859

Howell, C J, Maimon, D., Cochran, J. K., Jones, H. M., & Powers, R. A. (2017). System trespasser behavior after exposure to warning messages at a Chinese computer network: An examination. *International Journal of Cyber Criminology*, *11*(1), 63–77.

Howell, C. J., Maimon, D., Perkins, R. C., Burruss, G. W., Ouellet, M., & Wu, Y. (2022). Risk avoidance behavior on darknet marketplaces. *Crime & Delinquency*, 00111287221092713.

Howell, C. J., & Burruss, G. W. (2020). Datasets for analysis of cybercrime. *The Palgrave handbook of international cybercrime and cyberdeviance*, 207-219.

Hsiao, D. K., Madnick, S. E., & Kerr, D. S. (2014). *Computer security*. Academic Press, Inc.

Hughes, J., Collier, B., & Hutchings, A. (2019). From playing games to committing crimes: A multi-technique approach to predicting key actors on an online gaming forum. *2019 APWG Symposium on Electronic Crime Research (ECrime)*. https://doi.org/10.1109/ecrime47957.2019.9037586

Hughes, L. A., & DeLone, G. J. (2007). Viruses, worms, and trojan horses: Serious crimes, nuisance, or both? *Social Science Computer Review*, *25*(1), 78–98. https://doi.org/10.1177/0894439306292346

Humphrey, John A., & Cordella, Peter. (2013). Effective Interventions in the Lives of Criminal Offenders. Springer.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Leading Issues in Information Warfare & Security Research*. https://doi.org/ 978-1-908272-08-9

Hétu, D. D.-, Morselli, C., & Leman-Langlois, S. (2011). Welcome to the scene. *Journal of Research in Crime and Delinquency*, *49*(3), 359–382. https://doi.org/10.1177/0022427811420876

Institute for Security and Open Methodologies. (2012). The Hackers Profiling Project: A general overview . https://archive.conference.hitb.org/hitbsecconf2006kl/materials/DAY%202%20-%20Raoul%20Chiesa%20-%20HPP.pdf

Jardine, E. (2020). The case against commercial antivirus software: Risk homeostasis and information problems in cybersecurity. *Risk Analysis*, *40*(8), 1571–1588. https://doi.org/10.1111/risa.13534

Jaswal, P., Sharma, S., Bindra, N., & Krishna, C. R. (2022). Detection and prevention of phishing attacks on banking website. *2022 International Conference on Futuristic Technologies (INCOFT)*. https://doi.org/10.1109/incoft55651.2022.10094345

Jennings. (n.d.). Routine Activities Theory. In The Encyclopedia of Crime and Punishment. John Wiley & Sons, Ltd. https://doi.org/10.1002/9781118519639

Jones, B. L., & Nagin, D. S. (2013). A note on a Stata plugin for estimating group-based trajectory models. *Sociological Methods & Research*, *42*(4), 608–613. https://doi.org/10.1177/0049124113503141

Jones, H. S., Towse, J. N., Race, N., & Harrison, T. (2019). Email fraud: The search for psychological predictors of susceptibility. *PLOS ONE*, *14*(1). https://doi.org/10.1371/journal.pone.0209684

Jordan, T. (2016). A genealogy of hacking. *Convergence: The International Journal of Research into New Media Technologies*, *23*(5), 528–544. https://doi.org/10.1177/1354856516640710

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*(4), 757–780. https://doi.org/10.1111/1467-954x.00139

Kaaniche, M., Deswarte, Y. D., Alata, E., Dacier, M., & Nicomette, V. (2006). Empirical analysis and statistical modeling of attack processes based on honeypots. *IEEE/IFIP International Conference on Dependable Systems and Networks*, 119–124. https://doi.org/https://doi.org/10.48550/arXiv.0704.0861

Kamar, E., Howell, C. J., Maimon, D., & Berenblum, T. (2022). The moderating role of thoughtfully reflective decision-making on the relationship between information security messages and SMISHING victimization: An experiment. *Justice Quarterly*, 1–22. https://doi.org/10.1080/07418825.2022.2127845

Kang, T., & Kruttschnitt, C. (2022). Can persistent offenders help us understand desistance from crime? *Journal of Developmental and Life-Course Criminology*, *8*(3), 365–392. https://doi.org/10.1007/s40865-022-00205-y

Kanti, T., Richariya, V., & Richariya, V. (2011). Implementing a Web browser with Web defacement detection techniques. *World of Computer Science and Information Technology Journal (WCSIT)*.

Kapko, M. (2022, November 18). *Cybercriminals strike understaffed organizations on weekends and holidays*. Cybersecurity Dive. https://www.cybersecuritydive.com/news/cyberattacks-weekends-holidays/636956/

Kaspersky. (2023, April 19). *Types of Malware*. www.kaspersky.com. https://www.kaspersky.com/resource-center/threats/malware-classifications

Kemp, S., Buil-Gil, D., Miró-Llinares, F., & Lord, N. (2021). When do businesses report cybercrime? findings from a UK study. *Criminology & Criminal Justice*, *23*(3), 468–489. https://doi.org/10.1177/17488958211062359

Kemp, S., Miró-Llinares, F., & Moneva, A. (2020). The dark figure and the cyber fraud rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*, *26*(3), 293–312. https://doi.org/10.1007/s10610-020-09439-2

Kerstens, J., & Jansen, J. (2016). The victim–perpetrator overlap in financial cybercrime: Evidence and reflection on the overlap of youth's on-line victimization and perpetration. *Deviant Behavior*, *37*(5), 585–600. https://doi.org/10.1080/01639625.2015.1060796

Khurana, B., Prakash, J., & Loder, R. T. (2022a). Assault related injury visits in US emergency departments: An analysis by weekday, month and weekday-by-month. *Chronobiology International*, *39*(8), 1068–1077. https://doi.org/10.1080/07420528.2022.2065285

Khurana, B., Prakash, J., & Loder, R. T. (2022b). Holiday effect on injuries sustained by assault victims seen in US emergency departments. *Emergency Radiology*, *30*(2), 133–142. https://doi.org/10.1007/s10140-022-02103-8

Kigerl, A. (2011). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review*, *30*(4), 470–486. https://doi.org/10.1177/0894439311422689

Kilger, M. (2011). Social Dynamics and the future of technology-driven crime. *Corporate Hacking and Technology-Driven Crime*, 205–227. https://doi.org/10.4018/978-1-61692-805-6.ch011

Kitteringham, G., & Fennelly, L. J. (2020). Environmental crime control. *Handbook of Loss Prevention and Crime Prevention*, 207–222. https://doi.org/10.1016/b978-0-12-817273-5.00019-3

Korauš, A., Dobrovič, J., Rajnoha, R., & Brezina, I. (2017). The safety risks related to Bank cards and cyber attacks. *Journal of Security and Sustainability Issues*, 563–574. https://doi.org/10.9770/jssi.2017.6.4(3)

Krishnaveni, S., Prabakaran, S., & Sivamohan, S. (2018). A Survey on Honeypot and Honeynet Systems for Intrusion Detection in Cloud Environment. *Journal of Computational and Theoretical Nanoscience*, *15*(9), 2949–2953. https://doi.org/10.1166/jctn.2018.7572

Kudryavtsev, V., & Kuchakov, R. (2021). Do the marginalized kill more during holidays? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3855539

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, *45*, 58–74. https://doi.org/10.1016/j.cose.2014.05.006

Lam, Wyatt. 2020. “Christmas Criminals: A Routine Activity Approach to Crime on U.S. Holidays.” *James Madison Undergraduate Research Journal* 7(1). Retrieved Month Day, Year (http://commons.lib.jmu.edu/jmurj/ vol7/iss1/5).

Landreth, B. (1985). *Out of the inner circle: A hacker's Guide to Computer Security*. Penguin.

Laub, J. H., & Sampson, R. J. (2019). Life-course and developmental criminology: Looking back, moving forward—ASC division of developmental and life-course criminology inaugural David P. Farrington Lecture, 2017. *Journal of Developmental and Life-Course Criminology*, *6*(2), 158–171. https://doi.org/10.1007/s40865-019-00110-x

Laub, J.H. & Sampson R.J. (1993). Turning points in the life course: Why change matters to the study of crime*. *Criminology*, *31*(3), 301–325. https://doi.org/10.1111/j.1745-9125.1993.tb01132.x

Laub, J. H., & Sampson, R. J. (2006). *Shared Beginnings, Divergent Lives: Delinquent Boys to age 70*. Harvard Univ. Press.

Laub, J. H., Rowan, Z. R., & Sampson, R. J. (2018). The age-graded theory of informal social control. *The Oxford Handbook of Developmental and Life-Course Criminology*, 294–322. https://doi.org/10.1093/oxfordhb/9780190201371.013.15

Le Blanc, M. (2020). On the future of the individual longitudinal age-crime curve. Criminal Behaviour & Mental Health, 30(4), 183–195. https://doi.org/10.1002/cbm.2159

Leckie, G. (2010). *Module 5: Introduction to multilevel modelling Stata Practical*. University of Bristol Centre for Multilevel Modelling.

Lee, J. R., & Holt, T. J. (2023). Assessing the correlates of cyberattacks against high-visibility institutions. *Criminal Justice Studies*, *36*(3), 251–268. https://doi.org/10.1080/1478601x.2023.2254098

Leita, C., Pham, V. H., Thonnard, O., Ramirez-Silva, E., Pouget, F., Kirda, E., & Dacier, M. (2008). The Leurre.com project: Collecting internet threats information using a worldwide

distributed Honeynet. *2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing*. https://doi.org/10.1109/wistdcs.2008.8

Lester, D. (1979). Temporal variation in suicide and homicide. *American Journal of Epidemiology*, *109*(5), 517–520. https://doi.org/10.1093/oxfordjournals.aje.a112709

Lester, D. (1987a). Suicide and homicide at easter. *Psychological Reports*, *61*(1), 224–224. https://doi.org/10.2466/pr0.1987.61.1.224

Lester, D. (1987b). Suicide and homicide rates on national holidays. Leukfeldt, E. Rutger. (2014). Phishing for suitable targets in the Netherlands: Routine Activity Theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551–555. https://doi.org/10.1089/cyber.2014.0008

Leukfeldt, E. R. (2017). Research agenda the human factor in cybercrime and cybersecurity. *Eleven International Publishing*.

Leukfeldt, Eric Rutger, & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Levesque, F. L., Nsiempba, J., Fernandez, J. M., Chiasson, S., & Somayaji, A. (2013). A clinical study of risk factors related to malware infections. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS '13*. https://doi.org/10.1145/2508859.2516747

Levi, M. (2016). Assessing the trends, scale and nature of Economic Cybercrimes: Overview and Issues. *Crime, Law and Social Change*, *67*(1), 3–20. https://doi.org/10.1007/s10611-016-9645-3

Lillington, Karlin. “How Real Is the Threat of Cyberterrorism?,” April 14, 2016. https://www.irishtimes.com/business/technology/how-real-is-the-threat-of-cyberterrorism-1.2608935.

Lipton, J. D. (2011). Combatting cyber-victimization. *Berkeley Technology Law Journal*, *26*(2), 1103–1156.

Liu, J., Francis, B., & Soothill, K. (2011). A longitudinal study of escalation in crime seriousness. *Journal of Quantitative Criminology*, *27*(2), 175–196. https://doi.org/10.1007/s10940-010-9102-x

Longobardi, C., Settanni, M., Fabris, M. A., & Marengo, D. (2020). Follow or be followed: Exploring the links between Instagram popularity, social media addiction, cyber victimization, and subjective happiness in Italian adolescents. *Children and Youth Services Review*, *113*, 104955. https://doi.org/10.1016/j.childyouth.2020.104955

Lorenzini, G., Shaw, D. M., & Elger, B. S. (2022). It takes a pirate to know one: Ethical hackers for healthcare cybersecurity. *BMC Medical Ethics*, *23*(1). https://doi.org/10.1186/s12910-022-00872-y

Lozano-Blasco, R., Quilez-Robres, A., & Latorre-Cosculluela, C. (2023). Sex, age and cyber-victimization: A meta-analysis. *Computers in Human Behavior*, *139*, 107491. https://doi.org/10.1016/j.chb.2022.107491

Luo, W., Li, H., Baek, E., Chen, S., Lam, K. H., & Semma, B. (2021). Reporting practice in Multilevel Modeling: A revisit after 10 years. *Review of Educational Research*, *91*(3), 311–355. https://doi.org/10.3102/0034654321991229

Lu, Y., Luo, X., Polgar, M., & Cao, Y. (2010). Social network analysis of a criminal hacker community. *Journal of Computer Information Systems*, *51*(2), 31–41.

Lyngaas, S. (2021, November 22). *US government issues Thanksgiving ransomware warning | CNN politics*. CNN. https://www.cnn.com/2021/11/22/politics/thanksgiving-ransomware-warning/index.html

Lévesque, F. L., Fernandez, J. M., Young, G., & Batchelder , D. (2016). Are They Real? Real-Life Comparative Tests of Anti-Virus Products. *Virus Bulletin Conference*, 1–11.

MacCord, J. (2001). *Juvenile crime, juvenile justice: Panel on juvenile crime: Prevention, treatment, and Control*. National Academy Press.

Maggi, F., Balduzzi, M., Flores, R., Gu, L., & Ciancaglini, V. (2018). Investigating web defacement campaigns at large. *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. https://doi.org/10.1145/3196494.3196542

Maimon, David, Fukuda, A., Hinton, S., Babko-Malaya, O., & Cathey, R. (2017). On the relevance of social media platforms in predicting the volume and patterns of web defacement attacks. *2017 IEEE International Conference on Big Data (Big Data)*. https://doi.org/10.1109/bigdata.2017.8258513

Maimon, David, & Howell, C. J. (2020, May 26). *The Coronavirus Pandemic Moved Life Online – a Surge in Website Defacing Followed.* Government Technology State & Local Articles - e.Republic,. . https://www.govtech.com/security/The-Coronavirus-Pandemic-Moved-Life-Online--a-Surge-in-Website-Defacing-Followed.html.

Maimon, D., Howell, C. J., & Burruss, G. W. (2021). Restrictive deterrence and the scope of hackers' reoffending: Findings from two Randomized Field Trials. *Computers in Human Behavior*, *125*, 106943. https://doi.org/10.1016/j.chb.2021.106943

Maimon, D., Kamerdze, A., Cukier, M., & Sobesto, B. (2013). Daily trends and origin of computer-focused crimes against a large university computer network: An application of

the routine-activities and lifestyle perspective. *British Journal of Criminology*, *53*(2), 319–343. https://doi.org/10.1093/bjc/azs067

Maimon, David, & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology*, *2*(1), 191–216. https://doi.org/10.1146/annurev-criminol-032317-092057

Maimon, David, Testa, A., Sobesto, B., Cukier, M., & Ren, W. (2019). Predictably deterrable? the case of system trespassers. *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, 317–330. https://doi.org/10.1007/978-3-030-24900-7_26

Maimon, David, Wilson, T., Ren, W., & Berenblum, T. (2015). On the relevance of spatial and temporal dimensions in assessing computer susceptibility to system trespassing incidents. *British Journal of Criminology*, *55*(3), 615–634. https://doi.org/10.1093/bjc/azu104

Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in high school: Cybercrime perpetration by Juveniles. *Deviant Behavior*, *35*(7), 581–591. https://doi.org/10.1080/01639625.2013.867721

Martinez Santander, C. J., Moreno, H., & Hernandez Alvarez, M. B. (2020). The evolution from traditional to intelligent web security: Systematic Literature Review. *2020 International Symposium on Networks, Computers and Communications (ISNCC)*. https://doi.org/10.1109/isncc49221.2020.9297240

Mattern, T., Felker, J., Borum, R., & Bamford, G. (2014). Operational Levels of Cyber Intelligence. *International Journal of Intelligence and CounterIntelligence*, *27*(4), 702–719. https://doi.org/10.1080/08850607.2014.924811

McGee, T. R., & Farrington, D. P. (2019). Developmental and life-course theories of crime. *Oxford Research Encyclopedia of Criminology and Criminal Justice*. https://doi.org/10.1093/acrefore/9780190264079.013.250

Middleton, L. (2022, November 13). *Why hackers love the holidays*. Tekscape. https://www.tekscape.com/blog/why-hackers-love-the-holidays/

Mirkovic, J., & Reiher, P. (2004). A taxonomy of ddos attack and ddos defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39–53. https://doi.org/10.1145/997150.997156

Miró, F. (2014). Routine activity theory. *The Encyclopedia of Theoretical Criminology*, 1–7. https://doi.org/10.1002/9781118517390.wbetc198

Mitropoulos, S., Patsos, D., & Douligeris, C. (2006). On incident handling and response: A state-of-the-art approach. *Computers & Security*, *25*(5), 351–370. https://doi.org/10.1016/j.cose.2005.09.006

Moffitt, T. E. (1993). Adolescence-limited and life-course-persistent antisocial behavior: A developmental taxonomy. *Psychological Review*, *100*(4), 674–701. https://doi.org/10.1037//0033-295x.100.4.674

Moffitt, T. E. (1993). A developmental taxonomy. Psychological Review, 100(4), 674–701.

Moneva, A., Leukfeldt, E. R., Van De Weijer, S. G. A., & Miró-Llinares, F. (2022). Repeat victimization by website defacement: An empirical test of premises from an environmental criminology perspective. *Computers in Human Behavior*, *126*, 106984. https://doi.org/10.1016/j.chb.2021.106984

Morris, R. G., & Blackburn, A. G. (2009). Cracking the code: An empirical exploration of social learning theory and computer crime. *Journal of Crime and Justice, 32*(1), 1–34. https://doi.org/10.1080/0735648x.2009.9721260

Mujezinovic, D. (2022, November 21). *Cyberattacks surge during the holiday season: Here's why*. MUO. https://www.makeuseof.com/why-cyberattacks-surge-during-holiday-season/

Mulvey, E. P., Steinberg, L., Fagan, J., Cauffman, E., Piquero, A. R., Chassin, L., ... & Losoya, S. H. (2004). Theory and research on desistance from antisocial activity among serious adolescent offenders. *Youth violence and Juvenile Justice*, 2(3), 213-236.

Nagin, D. S. (1999). Analyzing developmental trajectories: A semiparametric, group-based approach. *Psychological Methods*, 4(2), 139–157. https://doi.org/10.1037/1082-989X.4.2.139

Nagin, D. S. (2005). Group-based modeling of development. Cambridge, MA: *Harvard University Press*.

Nagin, D. S. (2014). Group-based trajectory modeling: An overview. *Annals of Nutrition and Metabolism*, *65*(2-3), 205–210. https://doi.org/10.1159/000360229

Najaf, K., Mostafiz, M. I., & Najaf, R. (2021). Fintech firms and Banks Sustainability: Why cybersecurity risk matters? *International Journal of Financial Engineering*, 2150019. https://doi.org/10.1142/s2424786321500195

Nawrocki, M., Wählisch, M., Schmidt, T. C., Keil, C., & Schönfelder, J. (2016, August 22). *A survey on honeypot software and data analysis*. arXiv.org. https://arxiv.org/abs/1608.06249

Neubert, T., & Vielhauer, C. (2020). Kill chain attack modelling for hidden channel attack scenarios in Industrial Control Systems. *IFAC-PapersOnLine, 53*(2), 11074–11080. https://doi.org/10.1016/j.ifacol.2020.12.246

Nezlek, J. (2020). Diary Studies in social and personality psychology: An introduction with some recommendations and suggestions. *Social Psychological Bulletin, 15*(2). https://doi.org/10.32872/spb.2679

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*.

NIAC 2017.Securing Cyber Assets: Addressing urgent cyber threats to critical infrastructure. Departement of Homeland Security.Avilable at: https://www.dhs.gov/sites/default/files/publications/niac-cyber-studydraft-report-08-15-17-508.pdf

Ooi, K. W., Kim, S.-H., Qui, H.-W., & Hui, K. L. (2012). Do hackers seek variety? An empirical analysis of website defacements. *ICIS 2012: Proceedings of the 33rd International Conference on Information Systems*.

PandaLabs. (2022, November 28). *The antivirus market continues to grow*. Panda Security Mediacenter. https://www.pandasecurity.com/en/mediacenter/security/antivirus-market/

Pearman, S., Kumar, A., Munson, N., Sharma, C., Slyper, L., Thomas, J., Bauer, L., Christin, N., & Egelman, S. (2016). *Risk compensation in home-user computer security behavior: A mixed* ... USENIX. https://www.usenix.org/sites/default/files/soups16poster23-pearman.pdf

Perkins, R. C., & Howell, C. J. (2021). Honeypots for Cybercrime Research. *Researching Cybercrimes*, 233–261. https://doi.org/10.1007/978-3-030-74837-1_12

Perkins, R. C., Howell, C. J., Dodge, C. E., Burruss, G. W., & Maimon, D. (2022). Malicious spam distribution: A routine activities approach. *Deviant Behavior*, *43*(2), 196-212.

Perkins, R. C., Ouellet, M., Howell, C. J., & Maimon, D. (2022). The illicit ecosystem of hacking: A longitudinal network analysis of website defacement groups. *Social Science Computer Review*, 089443932210978. https://doi.org/10.1177/08944393221097881

Peterson, A. (2021, December 6). Hackers accidentally defaced NASA sites. here's how to tell NASA and the NSA apart. The Washington Post. Retrieved December 13, 2021, from https://www.washingtonpost.com/news/the-switch/wp/2013/09/18/hackers-accidentally-defaced-nasa-sites-heres-how-to-tell-nasa-and-the-nsa-apart/.

Piquero, A. R. (2008). Taking stock of developmental trajectories of criminal activity over the life course. *The Long View of Crime: A Synthesis of Longitudinal Research*, 23–78. https://doi.org/10.1007/978-0-387-71165-2_2

Piquero, A., Farrington, D., & Blumstein, A. (2003). The criminal career paradigm: Background and recent developments. *University of Chicago Press*, *13*, 359–506.

Pompon, R., Walkowski, D., Boddy, S., & Levin, M. (2018, November 8). *2018 phishing and fraud report: Attacks peak during the holidays*. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/2018-phishing-and-fraud-report--attacks-peak-during-the-holidays

Pouget, F., & Dacier, M. (2004). Honeypot-based forensics. *N AusCERT Asia Pacific Information Technology Security Conference*.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267–296. https://doi.org/10.1177/0022427810365903

Preacher, K. J. (2021). *Introduction to Multilevel Models*. *A PDHP workshop*. Nashville; Vanderbilt University.

Purpura, P. P. (2013). Foundations of security and loss prevention. *Security and Loss Prevention*, 55–88. https://doi.org/10.1016/b978-0-12-387846-5.00003-6

Pérez-Sánchez, A., & Palacios, R. (2022). Evaluation of Local Security Event Management System VS. standard antivirus software. *Applied Sciences*, *12*(3), 1076. https://doi.org/10.3390/app12031076

Rabe-Hesketh, S. & Skrondal, A. (2008) *Multilevel and longitudinal modeling using Stata* (Second Edition). College Station, TX: Stata Press.

Rasbash, J. (2023, August 17). *What are multilevel models and why should I use them?*. What are multilevel models and why should I use them? | Centre for Multilevel Modelling | University of Bristol. https://www.bristol.ac.uk/cmm/learning/multilevel-models/what-why.html

Rantala, R. (2008). *Cybercrime against businesses, 2005*. . Bur. Justice Stat. Spec. Rep. NCJ 221943, US Dep. Justice, Washington, DC.

Raudenbush, S. W., & Bryk, A. S. (2002). *Hierarchical linear models: Applications and Data Analysis Methods*. Sage Publications.

Raudenbush, S. W., Johnson, C., & Sampson, R. J. (2003). 6. A multivariate, multilevel Rasch model with application to self-reported criminal behavior. *Sociological Methodology*, *33*(1), 169–211. https://doi.org/10.1111/j.0081-1750.2003.t01-1-00130.x

Reese, M. J., Ruby, K. G., & Pape, R. A. (2017). Days of action or restraint? how the islamic calendar impacts violence. *American Political Science Review*, *111*(3), 439–459. https://doi.org/10.1017/s0003055417000193

Reinhart, R. (2017, November 6). *Cybercrime tops Americans' crime worries*. Gallup.com. https://news.gallup.com/poll/221270/cybercrime-tops-americans-crime-worries.aspx

Reyns, B. W. (2015). A routine activity perspective on online victimisation. *Journal of Financial Crime*, *22*(4), 396–411. https://doi.org/10.1108/jfc-06-2014-0030

Reyns, B. W., Fisher, B. S., Bossler, A. M., & Holt, T. J. (2018). Opportunity and self-control: Do they predict multiple forms of online victimization? *American Journal of Criminal Justice, 44*(1), 63–82. https://doi.org/10.1007/s12103-018-9447-5

Riera, T. S., Higuera, J.-R. B., Higuera, J. B., Herraiz, J.-J. M., & Montalvo, J.-A. S. (2022). A new multi-label dataset for web attacks Capec classification using Machine Learning Techniques. *Computers & Security*, *120*, 102788. https://doi.org/10.1016/j.cose.2022.102788

Rodriguez, A., & Okamura, K. (2019). Generating real time cyber situational awareness information through social media data mining. *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*. https://doi.org/10.1109/compsac.2019.10256

Romagna, M., & van den Hout, N. J. (2017). Hacktivism and Website Defacement: Motivations, Capabilities and Potential Threats. In *27th Virus Bulletin International Conference*. Madrid, Spain.

Rostami, A., Vigren, M., Raza, S., & Brown, B. (2022). *Being hacked: Understanding victims' experiences of {IOT} hacking*. USENIX. https://www.usenix.org/conference/soups2022/presentation/rostami

Rotton, J., & Frey, J. (1985). Air Pollution, weather, and violent crimes: Concomitant time-series analysis of archival data. *Journal of Personality and Social Psychology, 49*(5), 1207–1220. https://doi.org/10.1037//0022-3514.49.5.1207

Sakellariadis, J. (2022, November 21). *Cyber experts buckle up for the holidays*. POLITICO. https://www.politico.com/newsletters/weekly-cybersecurity/2022/11/21/cyber-experts-buckle-up-for-the-holidays-00069654

Sampson, R. J., & Laub, J. H. (1990). Crime and deviance over the life course: The salience of adult social bonds. *American Sociological Review*, *55*(5), 609. https://doi.org/10.2307/2095859

Sampson, R. J., & Laub, J. H. (2018). A life-course theory of cumulative disadvantage and the stability of delinquency. *Developmental Theories of Crime and Delinquency*, 133–162. https://doi.org/10.4324/9780203793350-4

Sampson, R., & Laub, J. (1993). Crime in the making: Pathways and turning points through life. *Harvard University Press*, *31*(03). https://doi.org/10.5860/choice.31-1824

Sasse, M. A., Brostoff, S., & Weirich, D. (2002). Transforming the "weakest link" - a human-computer interaction approach to usable and effective security. *Internet and Wireless Security*, 243–262. https://doi.org/10.1049/pbbt004e_ch15

Sasse, S. (2005). "motivation" and routine activities theory. *Deviant Behavior*, *26*(6), 547–570. https://doi.org/10.1080/01639620500218260

Schell, B. H., & Dodge, J. L. (2002). *The hacking of america: Who's doing it, why, and how*. Greenwood Publ.

Schwartz, M. (2005, April 5). *Web site attacks continue to rise sharply*. Enterprise Systems. https://esj.com/articles/2005/05/04/web-site-attacks-continue-to-rise-sharply.aspx

Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation*, *14*, 36–45. https://doi.org/10.1016/j.diin.2015.07.002

Sganga, N. (2021a, September 2). *Feds warn organizations not to take a cyber vacation after high-profile hacking on holidays*. CBS News. https://www.cbsnews.com/news/fbi-cisa-cyber-vacation-warning/

Sganga, N. (2021b, November 17). *Businesses worried about cyberattacks during the holidays, report finds*. CBS News. https://www.cbsnews.com/news/cyber-security-cybersecurity-ransomware-hacking-businesses-worry-holidays/

Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to cyber-warfare a multidisciplinary approach*. Morgan Kaufmann Publishers, an imprint of Elsevier.

Shirali-Shahreza, M. H., & Shirali-Shahreza, M. (2009). International Conference on Knowledge Discovery and Data Mining. In *Analysis of Iranian Defaced Websites*.

Sikra, J., Renaud, K. V., & Thomas, D. R. (2023). UK Cybercrime, Victims and Reporting: A Systematic Review. *Commonwealth Cybercrime Journal*, *1*(1), 28–59.

Singer, J. D., & Willett, J. B. (2003). *Applied Longitudinal Data Analysis: Modeling Change and event occurrence*. Oxford University Press.

Snijders, T. A. B., & Bosker, R. J. (2012). *Multilevel Analysis: An introduction to basic and Advanced Multilevel Modeling*. Sage Publications.

SolarWinds. (2012). *The US hosts 43% of the world's top 1 million websites*. pingdom.com. https://www.pingdom.com/blog/united-states-hosts-43-percent-worlds-top-1-million-websites/#:~:text=It%20should%20come%20as%20no%20surprise%20that%20the,million%20websites%20are%20hosted%20in%20the%20United%20States.

Spitzner, L. (2003). *Honeypots: Tracking hackers*. Addison-Wesley.

Squires, S., & Shade, M. (2015). People, the weak link in cyber-security: Can ethnography bridge the gap? *Ethnographic Praxis in Industry Conference Proceedings*, *2015*(1), 47–57. https://doi.org/10.1111/1559-8918.2015.01039

Standler, Dr. R. B. (2002). *Computer Crime*. Computer crime. http://www.rbs2.com/ccrime.htm

Steinmetz, K. F. (2015). Craft(Y)Ness. *British Journal of Criminology*, *55*(1), 125–145. https://doi.org/10.1093/bjc/azu061

Sukhai, N. B. (2004). Hacking and Cybercrime. *Proceedings of the 1st Annual Conference on Information Security Curriculum Development*. https://doi.org/10.1145/1059524.1059553

Sureda Riera, T., Bermejo Higuera, J.-R., Bermejo Higuera, J., Martínez Herraiz, J.-J., & Sicilia Montalvo, J.-A. (2020). Prevention and fighting against web attacks through anomaly detection technology. A systematic review. *Sustainability*, *12*(12), 4945. https://doi.org/10.3390/su12124945

Taylor, P. (1999). Hackers: Crime in the Digital Sublime. London: Routledge.

Taylor, R. W., Caeti, T. J., Loper, D. K., Fritsch, E. J., & Liederbach, J. (2006). *Digital crime and digital terrorism: and time criminal justice, special edition*. Pearson Prentice Hall.

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2015). The dark figure of online property crime: Is cyberspace hiding a crime wave? *Justice Quarterly*, *33*(5), 890–911. https://doi.org/10.1080/07418825.2014.994658

Testa, A., Maimon, D., Sobesto, B., & Cukier, M. (2017). Illegal roaming and file manipulation on target computers. *Criminology & Public Policy*, *16*(3), 689–726. https://doi.org/10.1111/1745-9133.12312

Tremblay, R., & Nagin, D. (2005). he developmental origins of physical aggression in humans. In: Tremblay RE, Hartup WH, Archer J (eds) Developmental origins of aggression. *Guilford Press*.

Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., Moher, D., Peters, M. D. J., Horsley, T., Weeks, L., Hempel, S., Akl, E. A., Chang, C., McGowan, J., Stewart, L., Hartling, L., Aldcroft, A., Wilson, M. G., Garritty, C., … Straus, S. E. (2018). Prisma extension for scoping reviews (PRISMA-SCR): Checklist and explanation. *Annals of Internal Medicine, 169*(7), 467–473. https://doi.org/10.7326/m18-0850

Tripwire. (2022, December 15). *How to deal with cyberattacks this holiday season*. https://www.tripwire.com/state-of-security/how-deal-cyberattacks-holiday-season

Trivedi, A. J., Judge, P., & Krasser, S. (2007). Analyzing network and content characteristics of spim using honeypots. *SRUTI*.

Tsiakis, T., & Stephanides, G. (2005). The economic approach of information security. *Computers & Security*, 24(2), 105-108.

Tung, L. (2021). *Ransomware warning: Hackers see holidays and weekends as a great time to attack*. ZDNET. https://www.zdnet.com/article/security-warning-ransomware-attackers-are-working-on-the-holidays-even-if-you-arent/

Van der Stouwe, T., Asscher, J. J., Stams, G. J. J., Deković, M., & van der Laan, P. H. (2014). The effectiveness of multisystemic therapy (MST): A meta-analysis. *Clinical Psychology Review*, 34(6), 468-481.

van de Weijer, S. G. A., Holt, T. J., & Leukfeldt, E. R. (2021). Heterogeneity in trajectories of Cybercriminals: A longitudinal analyses of web defacements. *Computers in Human Behavior Reports, 4*, 100113. https://doi.org/10.1016/j.chbr.2021.100113

van de Weijer, S. G. A., Leukfeldt, R., & Bernasco, W. (2018). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*, *16*(4), 486–508. https://doi.org/10.1177/1477370818773610

van de Weijer, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: Determinants, motives, and previous experiences. *Policing: An International Journal*, *43*(1), 17–34. https://doi.org/10.1108/pijpsm-07-2019-0122

Waldrop, M. M. (2016). How to hack the hackers: The human side of cybercrime. *Nature*, *533*(7602), 164–167. https://doi.org/10.1038/533164a

Wall, D. S. (2012). Enemies within: Redefining The insider threat in organizational security policy. *Security Journal*, *26*(2), 107–124. https://doi.org/10.1057/sj.2012.1

Wetzig, C. (2022, November 2). *Cyber attacks during holidays: Why the spike?*. ThriveDX. https://thrivedx.com/resources/article/cyber-attacks-during-holidays

Weulen Kranenbarg, M., Ruiter, S., van Gelder, J.-L., & Bernasco, W. (2018). Cyber-offending and traditional offending over the life-course: An empirical comparison. *Journal of Developmental and Life-Course Criminology*, *4*(3), 343–364. https://doi.org/10.1007/s40865-018-0087-8

Weulen Kranenbarg, M., Holt, T. J., & van Gelder, J.-L. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior*, *40*(1), 40–55. https://doi.org/10.1080/01639625.2017.1411030

Whitten, T., McGee, T. R., Homel, R., Farrington, D. P., & Ttofi, M. (2019). Comparing the criminal careers and childhood risk factors of persistent, chronic, and persistent–chronic

offenders. *Australian & New Zealand Journal of Criminology*, *52*(2), 151–173. https://doi.org/10.1177/0004865818781203

Williamson, G. D. (2006). Enhanced Authentication In Online Banking . *Journal of Economic Crime Management*, *4*(2).

Wilsem, J. van. (2013). Hacking and harassment—do they have something in common? comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 437–453. https://doi.org/10.1177/1043986213507402

Wilson, T., Maimon, D., Sobesto, B., & Cukier, M. (2015). The effect of a surveillance banner in an attacked Computer System. *Journal of Research in Crime and Delinquency*, *52*(6), 829–855. https://doi.org/10.1177/0022427815587761

Wolfe, S. E., Higgins, G. E., & Marcum, C. D. (2008). Deterrence and digital piracy. *Social Science Computer Review*, *26*(3), 317–333. https://doi.org/10.1177/0894439307309465

Wolfgang, M. E., Figlio, R. M., & Sellin, T. (1987). *Delinquency in a birth cohort*. University of Chicago Press.

Woo, H., Kim, Y., & Dominick, J. (2004). Hackers: Militants or Merry Pranksters? A content analysis of defaced web pages. *Media Psychology*, *6*(1), 63–82. https://doi.org/10.1207/s1532785xmep0601_3

W3Techs. (2024). *Distribution of websites per server location*. https://w3techs.com/technologies/overview/server_location

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior*, *84*, 375–382. https://doi.org/10.1016/j.chb.2018.02.019

Yar, M. (2005). The novelty of 'cybercrime.' *European Journal of Criminology*, *2*(4), 407–427. https://doi.org/10.1177/147737080556056

Yegneswaran, Y., V. ,. Barford, P. ,. &. Paxson, V., Barford, P., & Paxson, V. (2005). Using honeynets for internet situational awareness. *Proceedings of the Fourth Workshop on Hot Topics in Networks (HotNets IV)* , 17–22.

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the minds of hackers. *Information Systems Management*, *24*(4), 281–287. https://doi.org/10.1080/10580530701585823

Yu, S. (2014). Fear of cyber crime among college students in the United States: an exploratory study. *International Journal of Cyber Criminology*, *8*, 36–46.

Yucedal, B. (2010). . Victimization in cyberspace: an application of Routine Activity and Lifestyle Exposure theories. . . *PhD Diss., Kent State Univ., Kent, OH*.

Zayid, E. I., Isah, I., Adam, Y. A., Farah, N. A., & Alshehri, O. A. (2023). *Examine Website Defacement Dataset by Exploiting Some Classifiers' Capabilities*. https://doi.org/10.20944/preprints202310.1743.v1

Zhang, X., Tsang, A., Yue, W. T., & Chau, M. (2015). The classification of hackers by Knowledge Exchange Behaviors. *Information Systems Frontiers*, *17*(6), 1239–1251. https://doi.org/10.1007/s10796-015-9567-0

## Vita

Cameron Hoffman is from rural western Pennsylvania. He graduated Summa Cum Laude from the University of Pittsburgh in 2019, majoring in Political Science, History, and Arabic. Cameron has interned with NGOs like Rise to Peace where he published analytical articles on terrorist threats and events. He has also traveled to over a dozen countries and even spent entire summers living in the Middle East.

While originally studying Middle Eastern affairs, focusing on terrorism and energy politics, noticing an increase in the role of cybertechnologies in Middle Eastern and Global politics he began to diversify his research interests. In 2021, he earned his master's degree in Public and International Affairs at the University of Pittsburgh majoring in Security and Intelligence Studies and minoring in Cybersecurity Policy and Law. Additionally, during graduate school he became a guest researcher at the Evidence-Based Cybersecurity Research Group, which would lead to becoming a PhD Student in the Department of Criminal Justice and Criminology at Georgia State University, where he would focus on cybercrimes.

Cameron has worked for companies like the National Bank of Canada, the Federal Reserve System, and Dell Technologies in darknet threat intelligence and currently works on the GSU collaboration with Navy Federal Credit Union to research cyber fraud. He has also published academic work in the top Computer Science journal, Computers and Security. After graduation, Cameron is assuming a full-time role with Dell Technologies in a fraud intelligence and investigation role.

For future inquiries you can reach Cameron at CJH100@pitt.edu or HoffmanCameron@outlook.com