2019

# Website Defacement and Routine Activities: Considering the Importance of Hackers' Valuations of Potential Targets

C. Jordan Howell
*Georgia State University*

George W. Burruss
*University of South Florida*

David Maimon
*Georgia State University*

Shradha Sahani
*Georgia State University*



## Recommended Citation

Howell, Jordan C., George W. Burruss, David Maimon & Shradha Sahani. Website Defacement and Routine Activities: Considering the Importance of Hackers' Valuations of Potential Targets. Journal of Crime and Justice 42:536-550.

## Introduction

In 2015, a group of hackers known as "Impact Team" targeted Ashley Madison, an online dating service that openly facilitated extra-marital affairs. The hackers took issue with the website and demanded its immediate termination. When Ashley Madison refused to discontinue operations, "Impact Team" defaced their website, breached their database, and publicly released the names of their subscribers (Hackathorn et al. 2017). As exemplified by this attack, website defacement, or the replacement of a website's original content with one's own content, is a relatively simple form of hacking with potentially severe consequences (Holt 2009, 2012). Although hackers have found numerous ways to deface websites, with varying degrees of complexity, the most common method is via SQL injection (Trend Micro 2019).[1] Although over one million websites are defaced each year (Zone-H 2018), only a few criminological studies exist that have studied website defacement as a form of cybercrime (i.e. Holt et al. 2017; Holt et al. 2019; Maimon et al. 2017).

We suspect that criminological research into the causes and correlates of website defacement is currently limited for two main reasons. First, most criminologists are unfamiliar with computer technology or the cyber-environment (Maimon and Louderback 2019). Therefore, the discipline avoids studying cybercrime generally. Second, those who do study cybercrime struggle to find valid and reliable data sources. This is in part because most hackers hide their identity and erase evidence of their intrusion (Howell et al. 2017); thus, official data sources like the FBI's Internet Crime Complaint Center probably underreport incidents of cybercrime.

[1] SQL (Structured Query Language) injection is a hacking technique involving malicious code entered into a web page through the site's input fields.

Some scholars, however, have started using original data collection techniques to overcome these issues, and garner insight into the correlates of website defacement. For example, Holt et al. (2017) examined the attitudinal and behavioral correlates of engaging in website defacement and found that political attitudes towards marginalized groups are associated with an increased willingness to engage in website defacement. Similarly, Holt and colleagues (2019), using a qualitative methodological approach, found that far-left extremist groups deface websites for the same political reasons they engage in physical crimes. Lastly, Maimon and colleagues (2017), using data they gathered from various social media platforms, found that hackers' social media use increases their attack frequency. Although these studies certainly provide valuable insight, the correlates of website defacement victimization are still unknown. If website hosts are unaware of the risk factors associated with victimization, they cannot effectively mitigate attack frequency.

The current study seeks to address this gap in the literature. By taking advantage of a unique online dataset compiled by Zone-H, which includes website defacers' reports of their malicious activities against websites hosted by servers all over the world, we focus on understanding how countries' structural factors correlate with the volume of website defacements. To date, we know of no study examining the relationship between a country's Internet infrastructure and socioeconomic characteristics on the incidence of website defacements in that country.

To frame our study, we draw on the routine activities framework because it has been used to explain macro-level variations in victimization patterns in the physical world and in cyberspace (Holt et al. 2018). Stated simply, routine activity theory (RAT)

proposes that victimization results from the convergence of motivated offenders, suitable targets, and the absence of capable guardianship in time and space.

Combining the Zone-H data with other macro-level data allowed for an examination of the predictive efficacy of theoretically derived variables on country-level victimization frequency. In addition, we were able to examine these relationships across hackers' valuations of potential targets. We used this distinction as an approximation for target suitability (namely value) and examined whether political defacements have different predictive factors than recreational defacements across nations. We hypothesized that capable guardianship will decrease website defacement frequency across nations, and that target suitability will increase website defacement frequency across nations. Drawing from Clarke (1999), we suspect that hackers do not view all targets as equally suitable. Target criteria for political defacements likely differs from the target criteria for recreational defacements. Therefore, we seek to answer the following research question: Do the country-level correlates of website defacement vary based on hackers' valuations of target suitability?

## Theoretical Background

### *Website Defacement*

Website defacement originated as a way for hackers to mock system administrators for poor security protocol, and as a way to generate their reputations as skilled hackers (Kilger 2011; Woo et al. 2004). Today, website defacement is commonly used to protest social and political injustice around the globe, where hacktivists often rely on website defacement to spread their ideological messages to a wider audience (Maimon et al. 2017; Fitri 2011). Although over one million websites were defaced in 2017 alone,

the existing literature virtually ignores the correlates of victimization, focusing almost exclusively on the content of the defacements (Holt et al. 2017; Zone-H 2018).

For example, analyzing the content of 462 defaced websites, Woo and colleagues (2004) concluded that 70% were classified as pranks, while the rest were politically motivated. Furthermore, they found that politically motivated hackers post more aggressive content than those who primarily attack for fun. Additionally, politically motivated hackers are more likely to deface websites following real-world political events (Al-Rizzo 2008; Denning 2011; Kilger 2011), and during times of war (Geers 2008), suggesting that structural factors may influence patterns of website defacement victimization. Relatedly, Maimon and colleagues (2017) observed that hackers tend to use social media platforms such as Facebook and Twitter to spread their ideology and build their reputation. Also, web-defacers who use social media platforms generate higher frequency of website defacement attacks than hackers who do not.

Holt and colleagues (2017) examined the attitudinal and behavioral correlates of the willingness to deface websites using a college student sample. They found that definitions favorable to cybercrime and attitudes in support of marginalized groups predicted individuals' willingness to deface websites, while technological skill and involvement in cybercrime did not. Although providing insight into the correlates of website defacement, the study's findings were limited because the authors used a scenario design to gauge motivation. Scenario designs have been successfully used in criminology but have notable shortcomings. Because Holt et al. (2017) asked subjects to pretend they had "necessary skills" to orchestrate the attack, it is likely that hackers who engage in website defacement differ from these college students in their knowledge about

website defacement. Consequently, the process of learning how to hack may affect the motivation to conduct defacement. Therefore, to gain a more complete understanding of how and why offenders choose their victims, researchers should employ samples of active offenders.

In addition to using appropriate samples, researchers should employ theory to explain website defacement. Not only can criminological theory be used to explain cybercrime, cybercrime can be used to further develop criminological theory (Maimon and Lounderback 2019). For example, Ooi and colleagues (2012) found that website defacers are "variety seeking," meaning they attack domains around the world. Moreover, website defacers choose their victims based on the underlying reason for the attack rather than choosing those close in proximity. Although the authors attribute variety-seeking behavior to boredom, a rival hypothesis could be offered: victimization results from the structural characteristics of the country where the domain is hosted. Given that website defacement is used to protest social and political injustice (Holt et al. 2017), it is plausible a country's political and economic structure influences website defacement victimization. Hackers may therefore value targets based on country-level characteristics (Ooi et al. 2012). To ground Ooi et al.'s empirical finding in a theoretical frame, Cohen and Felson's (1979) RAT offers a way to explore these assertions. Accordingly, we used this theory to frame our examination of the global variation in website defacements.

*Routine Activity Theory*

RAT was originally formulated by Lawrence E. Cohen and Marcus Felson (1979) to explain increased burglary rates in post-World War II society. Routine activity theory, unlike most mainstream criminological theories, is a theory of victimization that focuses

on ecological conditions. Additionally, RAT is not concerned with individual characteristics, but rather the situational and structural dimensions conducive to victimization. Stated simply, the base premise of RAT is that societal changes in post-war daily routines connected motivated offenders with suitable targets while simultaneously limiting the availability of capable guardianship. This convergence of the three elements in time and place then causes crime.

Even when motivated offenders come across targets, however, the offenders must view the potential target as suitable, which depends on their motivational reasoning about its worth. In other words, not all targets are equally suitable to all offenders. Clarke (1999), argued stolen products are typically concealable, removable, available, valuable, enjoyable, and disposable, which makes up the acronym CRAVED. For these reasons, burglars often elect to steal small electronic devices rather than refrigerators, or other bulky items. For offline theft, value is typically related to the pecuniary worth of an object making it universally appealing as a suitable target.

CRAVED does not apply perfectly to cyberspace, but it makes evident that target suitability varies based on the criminals' valuations of a product or target. In the case of website defacement, the value of the target might depend on the motivated offenders' judgement of the website's symbolic importance. For political defacements, a website's sponsor, or the organization associated with the site, may be valuable. Far-left extremists, for example, deface websites belonging to businesses they deem unethical (e.g. furriers, animal laboratories, construction companies) (Holt et al. 2019). Recreational hackers, instead, might find website content less valuable as they prize the accumulation of

defacements to demonstrate their influence (Holt 2007). This notion of differential target valuation in cyberspace, however, is underdeveloped.

Despite this underdevelopment, RAT is often regarded a general theory of crime (Ngo and Paternoster 2011), and it has been used to explain a host of victimization patterns in both the physical world (Cohen and Felson 1979) and in cyberspace (Maimon and Lounderback 2019), at both the macro- (Kigerl 2012) and individual-levels (Holt and Bossler 2013). However, the relevance of RAT to various forms of cybercrime has sparked a criminological debate. Based on the premise that cyberspace is "anti-spatial" (Mitchell 1995, 8) and lacks temporal ordering, Yar (2005) argued that the "spatio-temporal ontologies" of virtual and non-virtual environments are distinctly different (p.414). Yar asserted motivated offenders, suitable targets, and the absence of a capable guardian could not converge in cyberspace in the same manner that was hypothesized by Cohen and Felson (1979). Reyns and colleagues (2011), however, convincingly argued convergence is made possible via networked systems. In other words, victims and offenders still converge regardless of their physical locations.

Most tests of RAT in cyberspace have found moderate support (Maimon and Louderback 2019). For example, capable guardianship decreases the likelihood of data loss (Bossler and Holt 2009), malware infection (Holt and Bossler 2013), and hacking victimization (Wilsem 2013); whereas, time spent online increases one's likelihood of experiencing various forms of cyber victimization (Leukfeldt and Yar 2016; Reynes 2015; Yucedal 2010). At the macro-level, Maimon and colleagues (2013) found that cyber-attacks against university networks are more likely to occur during business hours. The authors attributed this finding to the increased visibility and accessibility of potential

suitable targets. Similarly, Kigerl (2012) found that wealthier nations (as a result of target suitability) experience higher amounts of phishing and spam. Lastly, Holt and colleagues (2018) found that countries with greater technological infrastructure, more political freedom, and less organized crime are more likely to report malware infections. Taken together, these studies show RAT to be useful in explaining cybercrime victimization patterns.

Although these studies find support for the three main concepts of RAT (motivated offenders, suitability of targets, and capability of guardianship), they do not measure specifically what makes a target suitable or what makes a guardian capable. Cohen and Felson (1979, 595) did break down target suitability into four components (value, inertia, visibility, and accessibility), but most tests lack the data to empirically parse out the components of the concept. This is a common issue with tests of the theory for both traditional crimes and cybercrimes (Holt et al. 2018).

With regard to cybercrime specifically, Yar (2005) discussed the various components of RAT. With respect to the value of suitable targets in cyberspace, Yar (2005, 419) noted:

> *Broadly speaking, we can conclude that the targets of cybercrime, like those of terrestrial crime, vary widely and attract different valuations, and that such valuations are likely to impact on the suitability of the target when viewed from the standpoint of a potential offender…*

In the case of website defacement, hackers might select websites based on their own valuation of the potential targets. For example, script kiddies attempting entry into elite hacker circles might value any accessible website as they build their CVs with volume of increasingly difficult hacks (Holt 2007). Hacktivists, on the other hand, might only value websites with political, religious, or economic significance (Romagna and van

den Hout 2017). Finally, ethical hackers might value poorly guarded systems as a means to identify and call out careless cybersecurity practices. The variation in target selection should therefore affect the way other RAT constructs predict victimization. Few tests of RAT, especially in cyberspace, have measured target suitability, assuming all digital information is equally valuable to hackers. In particular to website defacement, the value of the target depends on the offenders' perceived worth in building reputation and status, or as a symbol of thwarting oppression.

In addition, prior research suggests that other country-level structural variables may affect various forms of cybercrime victimization, including website defacement. Computer vulnerabilities embody Cohen and Felson's (1979) original operational definition of target suitability, namely accessibility. A vulnerability is a weakness or flaw that can be exploited to allow a hacker illegitimate access to a computer system. Hackers can exploit vulnerable systems with ease to deface websites and spread their ideological message. Therefore, countries with more vulnerabilities should experience more website defacements.

In addition to computer vulnerabilities, other characteristics have been shown to increase cybercrime victimization at different units of analysis. For example, Holt and colleagues (2018) argue that Asian nations likely report more malware due to the "prominence of hacker communities" (1727) and the substantial pool of potential victims with high-speed Internet access. In this vein, Asian nations should experience higher rates of various forms of cybercrime, including website defacement, due to increased visibility and accessibility in cyberspace.

Moreover, a country's gross domestic product (GDP), commitment to educational attainment, and level of freedom are positively associated with the amount of time spent online and the sophistication of the Internet infrastructure within the nation (Holt et al. 2018). Multiple studies have reported that time spent engaging in online leisure activities is associated with an increased risk of victimization (Maimon and Louderback 2019). This is likely because increased Internet traffic increases the visibility and accessibility of potential targets, thus making them more suitable (Wang et al. 2015). At the macro-level, Maimon and colleagues (2013) demonstrated that attack frequency is greater when more people are online. Wealthy, educated, and free countries are at an increased risk of being attacked because more of their citizens have Internet browsing capabilities and because the country is more equipped to host websites. Since cybercrime tends to be geographically clustered (Maimon et al. 2015), and since website defacement can only be launched against countries that host websites, it is likely that GDP, commitment to educational attainment, and level of freedom will increase website defacement frequency by increasing visibility and accessibility.

The presence of certain characteristics, however, likely have an adverse effect of cybercrime victimization. Muslim majority countries and countries that prioritize societal well-being, for example, are perhaps less likely to be targets of various forms of cybercrime such as website defacements. If target suitability increases crime rates, unsuitable targets should have the opposite effect. As discussed above, website defacement is often used as a form of social and political protest. Many of these protestors are pro-Islamic (Choo 2008); therefore, it is likely these protestors find less value in defacing Muslim majority countries. Although there is a likelihood that tensions

across countries influence mutual targeting, given that many defacers are pro-Islamic we expect that Muslim majority nations will less frequently be targeted by website defacement.

Similarly, countries that prioritize societal well-being should be viewed as less suitable. One way to assess the prioritization of societal well-being is through the existence of social programs, such as healthcare (Messner and Rosenfeld 1997). If a country prioritizes societal well-being, protestors will likely find less value in defacing their websites.

Capable guardianship is the other essential part of the RAT equation (Cohen and Felson 1978). Computer emergency response teams (CERT) operate around the world and serve as first responders to various forms of cyber-victimization (i.e. hacking, viruses, malware). In addition, they disseminate information that can be used to prevent victimization (Holt 2003; Wall 2007). Therefore, as suggested by Holt et al. (2018), the presence of a CERT should decrease the frequency of various forms of cybercrime victimization, such as website defacement, at the country-level. Another measure of guardianship is cyber defense through a country's military. Lynn (2010, 63) noted cyber defense is "…just as critical to military operations as land, sea, air, and space". It is believed that a strong military presence will be seen as a capable guardian by hackers, especially with regard to critical infrastructure (Kugler 2009). Therefore, a strong military presence should be associated with a decrease in website defacement frequency.

**Current Study**

The current study can be viewed as an assessment of the predictive ability of theoretical constructs drawn from RAT on website defacement frequency across nations,

and an investigation into how the influence of structural characteristics of website defacement victimization vary based on hackers' valuations of potential targets. To conduct this investigation, we first test the predicative ability of RAT derived variables on total website defacement frequency across nations. We then examine the effects of the country-level structural variables on two substantively different forms of website defacement: political and recreational. We focus exclusively on these two types of defacements because they are the most prevalent and distinctly different (Woo et al. 2004). In essence, we seek to test the predictive ability of RAT proxies on total website defacement frequency, and determine if, and how, the structural characteristics conducive to website defacement victimization vary based on offenders' valuations of potential targets.

We first hypothesize that *the presence of capable guardianship will decrease website defacement frequency across nations*. Specifically, a strong military presence and the presence of a CERT should be associated with a decrease in website defacement frequency across nations. Computer emergency response teams serve as first responders to various cyber-attacks and can be used to prevent victimization (Holt 2003; Wall 2007). Military presence, through cyber defense tactics, has shown to have a deterrent effect on attacks against critical infrastructure (Lynn 2010). Both CERT and military presence should deter attacks against websites across nations due to the increased risk of punishment and increased difficultly of infiltration (target hardening).

At the same time, we hypothesize that the presence of suitable targets will increase website defacement frequency across nations. Specifically, computer vulnerabilities, GDP, commitment to educational attainment, political freedom, and being

an Asian nation should be associated with an increase in attack frequency across nations, while Muslim majority nations, and nations that prioritize societal well-being should experience less defacements. Vulnerabilities are easily exploited by hackers; therefore, countries with more vulnerabilities are more accessible to those wishing to deface a website. Prior research has found that Asian nations report more cybercrime due to the sheer number of potential victims that reside within close proximity to hacker communities (Holt et al. 2018). In this vein, Asian nations should experience higher frequencies of website defacement due to increased visibility and accessibility of the websites hosted in Asia. Moreover, a country's GDP, commitment to educational attainment, and level of freedom are positively associated with the amount of time spent online and a nation's Internet infrastructure (Holt et al. 2018), which increases the visibility and accessibility of potential targets. In other words, nations with more websites, and more citizens accessing those websites, likely receive more website defacements as a result.

Muslim majority countries and countries that prioritize societal well-being are likely deemed as less suitable, and therefore should experience fewer website defacements. Although there may be retaliation targeted toward Muslim majority countries, we expect that these attacks will be less frequent decreasing the presence of defacements in Muslim majority countries. Similarly, if a country prioritizes societal well-being, protestors will likely find less value in defacing websites hosted in that country.

As stated above, not all targets are equally suitable to all offenders. Political hackers likely valuate potential targets differently than recreational hackers. In other

words, attacks launched recreationally are likely influenced by a country's characteristics; whereas political defacements are likely target specific (Romagna and van den Hout 2017). For these reasons, we ask the following research question. *Do the country-level correlates of website defacement vary based on hackers' valuations of target suitability?* Specifically, we seek to determine if, and how, the structural correlates of political defacement differ from the structural correlates of recreational defacement.

**Methods**

To test our hypotheses and answer our research question, we collected data from a variety of different sources including Zone-H (zone-h.org), the United States' Central Intelligence Agency (cia.gov/library/publications/the-world-factbook), Freedom House (freedomhouse.org), Forum of Incident Response and Security Teams or FIRST (first.org), and Kaspersky Lab (kaspersky.com). Our final sample consisted of 114 nations in 2017. We focus our analysis on website defacement victimization at the country-level.

*Dependent Variable: Website Defacement*

Zone-H was created in 2002 to archive defaced websites. Hackers report their successful defacements to Zone-H, and after the defacement is verified, it is permanently housed in their archive. Over 13 million defacements have been reported to Zone-H thus far. In addition to archiving defaced websites, Zone-H provides attack specific information. Relevant to the current study, Zone-H reports the target location, self-reported offense motivation, and attack date. They also classify some website defacements as "special," which they vaguely define as attacks on "important websites" (Zone-H 2018). Although the special defacements are loosely defined, this distinction

allows us to focus our attention on attacks against higher value targets. It is important to note that the large majority of these special defacements are attacks against government websites. An analysis of the non-special, common defacements might therefore show different findings.

Using the Zone-H archive, we gathered the total number of special defacements that occurred in 2017. We then calculated the total number of special defacements launched against each country in 2017. Additionally, we calculated the total number of these special defacements that were classified as political or recreational[2], then calculated the total number of political or recreational defacements that occurred at the country-level. We therefore have three distinct dependent variables to examine variation in country-level website defacement incidents: total website defacements, recreational defacements, and political defacements.

As made clear in the above paragraph, the current study employs population data of all special defacements that were reported to Zone-h in 2017. In total, nearly 13,000 special defacements were reported to Zone-h in 2017. We focus on attacks that occurred in 2017 because it was, at the time of writing, the most recent year of data available on Zone-h. We believe restricting our analysis to a recent year is beneficial. It is likely the correlates of website defacement in contemporary times are different than they were in earlier years.

*Capable Guardianship*

Capable guardianship at the country-level is operationalized as the presence of a CERT (i.e. Holt et al. 2018) and a strong military presence (i.e. Lynn 2010). Using data

[2] Recreational defacements, for the purpose of the current study, are defacements Zone-h lists as "just for fun".

gathered from FIRST (an organization that gathers data on CERTs around the world), we created a dummy variable for CERT presence. We measured military presence using percent GDP spent on military expenditures, which was collected from the *CIA World Fact Book* (an almanac-style resource that provides information on countries around the world).

*Target Suitability*

Drawing from prior research, we employed multiple measures of target suitability. To measure country-level vulnerability, we gathered the total number of vulnerabilities per day, per country, as reported by Kaspersky Lab (a multi-national cybersecurity company) for a period of six months in 2018. We then took the mean number of vulnerabilities for each country to ensure that our final measure minimizes the influence of random fluctuation.

We used *The CIA World Fact Book* to gather data for the following variables: GDP, commitment to educational attainment, prioritization of societal well-being, and Muslim majority. GDP is measured using a country's total gross domestic product. Commitment to educational attainment is measured by percent GDP spent toward education. We created a dummy variable for Muslim majority countries (i.e. countries with over 50% of their total population being Muslim). Societal well-being was measured as percent GDP spent on healthcare.

To measure a country's level of political freedom, we employed a freedom scale that was calculated by Freedom House (an independent nongovernmental agency), which ranks countries based on their citizens' political freedoms and civil liberties. Higher

scores indicate higher levels of freedom. Lastly, drawing from prior research (Holt et al. 2018), we created a dummy variable for Asian nations.

**Analytic Strategy**

We employ negative binomial models because our dependent variables were skewed count measures. In addition, the defacement variables' variances were greater than the means indicating overdispersion, which renders the commonly used Poisson regression problematic. Negative binominal regression, however, allows for the assessment of overdispersed count data.

Furthermore, because our dependent variables are measured as a count, rather than a rate, we considered country-level exposure to victimization. Countries with more Internet users likely received a greater number of website defacements simply because more opportunity existed. Count models account for the difference in opportunity by adding an exposure variable into the model and constraining the coefficient to one. We used the number of Internet users (collected from the *CIA World Fact Book*) as our exposure variable. Stated simply, the count (of website defacements) is adjusted based on opportunity (number of Internet users), which allows for a non-biased assessment of the data.

**Results**

Table 1 presents descriptive statistics of our sample. As shown in the table, there was an average of about 70 (SD=304.67) special defacements in each country in 2017, and a substantial variation in total attack frequency. Recreational defacements (M=67.42, SD=171.68) occur more frequently than political defacements (M=3.38, SD=13.79)[3].

[3] Of the 184 countries we gathered data for in 2017, 71% reported at least one special defacement.

This variation shows that some countries are frequently targeted, whereas others receive fewer attacks.[4] Additionally, the fact that recreational defacements occur more frequently than political defacements, could be viewed as preliminary evidence that political hackers are more selective of their target.

[Insert Table 1 about here]

To examine the effects of a country's Internet infrastructure and socioeconomic characteristics on website defacement frequency, we employed a negative binominal model. Results attained from this analysis, reported in Table 2, provide partial support for RAT. In regard to capable guardianship in cyberspace, both CERT and Military operate in the anticipated direction, but only Military attained statistical significance (b = -211, $p$=0.006).

Target suitability was measured using multiple proxies. Specifically, we hypothesized that the number of known vulnerabilities, Asian countries, GDP, commitment to educational attainment, and level of freedom would be associated with an increased number of website defacements, whereas Muslim majority countries and countries that prioritize societal well-being would experience less defacements. All of our measures operate in the hypothesized direction, but only Vulnerability (b=0.001, $p$=0.009), Asian (b=1.755, $p$=0.000), Muslim (b=-1.030, $p$=0.015), and Health (b=-0.258, $p$=0.003) attained statistical significance.

Incident rate ratios (IRR) provide an intuitive way to assess effect magnitude. Although statistically significant, the effect size of Vulnerability (IRR=1.000) is practically equivalent to the null value. Asian nations (IRR=5.782), however, are nearly

[4] A check of the variance inflation factor indicated no problem with multicollinearity.

six times more likely to experience an increase in the count of website defacements than non-Asian nations. Muslim majority countries are nearly three times less likely to experience defacements than non-Muslim majority nations (IRR=0.357). The effect size of Health (IRR=0.772) and Military (IRR=0.810) are moderate to low.

[Insert Table 2 about here]

To understand how structural characteristics vary across hackers' valuations of potential targets, we examine the frequency of political and recreational defacements. As reported in Table 3, structural characteristics still have an effect on website defacement frequency when looking at defacements conducted recreationally. In regard to capable guardianship, Military still has a deterrent effect (b=-0.644, $p$=0.000). In addition, Vulnerability (0.001, $p$=0.030) and Asian (b=2.159, $p$=0.000) remained statistically significant. The effect size of Vulnerability is still about zero (IRR=1.000), but Asian nations (IRR=8.664) are now over eight times more likely to have an increase in counts than their non-Asian counterparts.

[Insert Table 3 about here]

Next, we examined political defacement frequency. None of our predictor variables attained statistical significance. Military no longer has a deterrent effect, Asian nations are not more likely to be attacked, and the effect of vulnerability disappeared. Results reported in Table 4 show that political defacements, in the context of the current study, are not influenced by measures of a country's Internet infrastructure and socioeconomic characteristics.

In the interest of testing the significance of the difference between the statistically significant coefficients presented in Table 3 and their non-significant counterparts in

Table 4 we examined the equality of regression coefficients using the formula suggested by Paternoster et al. (1998). The effect of military presence is signficantly different across groups (z=-3.00), whereas the effects of vulnerability and Asian are invariant.

[Insert Table 4 about here]

**Discussion**

Routine activity theory posits that crime occurs when a motivated offender, suitable target, and the absence of a capable guardian converge in time and space (Cohen and Felson 1979). Historically, many tests of RAT have not specifically measured the sub domains of target suitability (VIVA). We argue, however, that value can be measured through the choice in targets. By analogy, burglars and arsonists likely evaluate the value of a target differently. The burglar, as stated by Cohen and Felson (1979), may elect to steal an electronic device rather than a refrigerator because it is more portable and easily converted to cash. An arsonist, however, cannot be influenced by the same factors as the burglar because their evaluation criteria for target suitability are different. Thus the target value for the arsonist can be judged in the kind of buildings he burns. In the same vein, political hackers likely evaluate the worth of a target differently than recreational hackers. Political hackers likely have a narrow view of target suitability; whereas recreational hackers have a wider selection of targets to choose from. For the purpose of the current study, we viewed recreational defacements and political defacements as separate types of offenses. Although the modus operandi can be similar, if not the same, past research has shown the attacks are substantively different (Woo et al., 2004).

The current study sought to assess the predictive ability of RAT derived variables on website defacement frequency, and attempted to determine if, and how, structural

characteristics conducive to website defacement vary based on hackers' valuations of potential targets. Specifically, using country-level victimization data, we examined the macro-level correlates of total website defacement frequency, recreational defacement frequency, and political defacement frequency. We found that a country's structural characteristics influence the number of total defacements and defacements conducted for recreational reasons but found no evidence that political defacement frequency is influenced by other macro-level variables.

More specifically, total website defacement frequency is deterred by capable guardianship (a strong military) and influenced by a few measures of target suitability (Vulnerability, Asian, Muslim, and Health). Hackers likely attack countries with known vulnerabilities because vulnerabilities make it easier to infiltrate and deface websites. Asian countries are likely targeted due to the prominent hacker communities that reside in Asia and the sheer number of potential targets. Therefore, it is our belief that victimization is more prevalent in Asian nations due to increased visibility and accessibility. Majority Muslim countries and countries that prioritize societal well-being receive fewer website defacements. Website defacement is used to protest events around the globe (Holt et al. 2017). A large number of these protestors are pro-Islamic (Choo 2008). Perhaps countries that prioritize societal well-being and Muslim majority countries are deemed as less suitable by those who engage in website defacement for altruistic reasons.

Regarding recreational defacements, structural characteristics still had an effect. A strong military still had a deterrent effect and known vulnerabilities still increased attack frequency across nations. Asian countries suffered from a greater likelihood of

victimization when the attack was recreational. This is likely a result of hacker rivalries that exist in Asia that are country specific (Pinkston 2016). Muslim majority nations and the prioritization of societal well-being, however, no longer had a statistically significant effect. Recreational hackers may not care about a country's prioritization of societal well-being or their citizens' faith; they might attack for sheer enjoyment and to build a reputation as a skilled hacker (Kilger 2011).

Political defacement frequency was not influenced by a country's socioeconomic characteristics or Internet infrastructure. As stated above, political motivation can be used as an approximation for target suitability. Political attacks are not opportunistic, but rather target specific. In other words, those hacking for political reasons may be driven by their evaluation of a target's value, and unfazed by the presence of a capable guardian or the other elements of target suitability (i.e. inertia, visibility, accessibility). Politically motivated attacks are common in India and Pakistan (Rasool 2015). It is possible these hackers are solely driven by the ongoing conflict over Kashmir making these countries more vulnerable to politically motivated website defacement.

These politically motivated hackers may operate like politically motivated terrorists in the physical world (Holt et al. 2019). Terrorism research has demonstrated that typical deterrence strategies have less utility than other forms of deterrence (i.e. reintegrative punishment strategy) (Ginges 2007). Therefore, a more multidimensional approach may be warranted if policy makers wish to deter this type of attack.

The findings presented in the current study provide partial support for RAT. Total website defacement frequency was deterred by capable guardianship (a strong military) and influenced by multiple measures of target suitability (Vulnerability, Asian, Muslim,

and Health). Interestingly, we found that the structural characteristics conducive to website defacement vary across hackers' self-reported valuations of the attacked website.

This study, like most, suffers from notable limitations. Data for our dependent variables were gathered from Zone-H. Zone-H only includes reported website defacements. It is likely, and even probable, that those who report their defacements to Zone-H differ from those who choose not to report. In addition, due to data availability, we were only able to include 114 countries in our regression models due to missing data across datasets.[5] Although this is on par with previous research (e.g. Messner and Rosenfeld 1997), future studies should attempt to include all countries in their analysis. We only included special defacements that occurred in 2017. Although nearly 13,000 special defacements occurred in 2017, this choice limits the generalizability of our findings. However, it did allow us to focus our analysis on recent attacks on higher value targets. In the future, researchers may want to include non-special defacements and defacements that occurred in other years.

Additionally, we relied on hackers' self-reported motivations through the Zone-H website, which offers a variety of motivations to choose from when hackers log their attack. This measure is neither exhaustive nor mutually exclusive. A content analysis examining hackers' self-reported motivations and defacement content should be used to validate the measure. Lastly, we operationalize hackers' self-reported motivations as an approximation for target suitability, namely value. We believe this decision is justified in that motivation to attack a specific target is an evaluation of that target's value; however, we were unable to assess individual hacker rationale. Future studies should consider a

[5] Most of the countries missing data were small island nations, but there were a few large developing countries that were also excluded (e.g., North Korea).

mixed methodological approach to gain a more nuanced understanding of the phenomenon.

Although we draw from RAT, the current study cannot be considered a true test of the theory. Instead, we test the predictive efficacy of theoretically derived variables. Although the presence of a CERT and a strong military establish face validity, it is unclear whether these measures are truly indicative of capable guardianship at the country-level. Any private or public organization can have a CERT; therefore, it may be a better measure of capable guardianship at a smaller scale. If CERTs are only capable guardians at the organizational level, this would explain why neither Holt et al. (2018), nor the current study, found the presence of a CERT to have a deterrent effect. Although military presence is statistically significant, and in the anticipated direction, it is likely that other governmental measures would be more effective. For example, the existence of policy created to curtail attacks against a country would likely have a stronger effect than military presence. Additionally, although our measures of target suitability do not indicate signs of multicollinearity, they may be theoretically correlated. We include GDP, freedom, and education as independent variables in our model, but they may work together, or with other variables not included in our model, to form a latent variable that serves as a better measure of target suitability. Future studies should work to better understand how the components of RAT operate at different levels of measurement and attempt to identify theoretically sound constructs that serve as better proxies for target suitability and capable guardianship in cyberspace.

Despite these limitations, our findings have both real world and theoretical implications. Both capable guardianship and target suitability impact defacement

frequency. If country-level policies aimed to increase guardianship or decrease any of the components of target suitability (value, inertia, visibility, accessibility) are implemented, perhaps defacement frequency will decline; however, these policies may prove ineffective for deterring political hackers. A multi-dimensional approach, similar to those used for politically motivated terrorists in the physical world, may prove more effective (Ginges 2007). Additionally, although this test was conducted at the country-level, micro-level policies can be inferred. Specifically, those who host websites might have the ability to protect their site from potential defacers by ensuring their website does not suffer from exploitable vulnerabilities.

Regarding theory, the current study expands the scope of RAT to website defacement, a form of cybercrime largely ignored by criminologists. In addition, this is the first known study to examine variation in macro-level crime correlates across hackers' self-reported valuations of a specific target. By using hackers' motivations as an approximation for target suitability, we were able to examine how country-level correlates vary based on hackers' valuations. Results from the current study provide partial support for RAT. Specifically, we found that website defacements are less likely to occur in the presence of capable guardianship (strong military presence) and more likely to occur when certain measures of target suitability are present. These patterns of victimization lend additional support to the premise that hackers are rational actors (Maimon et al. 2014). In addition, our findings suggest that although a country's socioeconomic characteristics and Internet infrastructure are related to website defacement frequency, the correlates of victimization vary based on hackers' perceived valuations of potential targets. Recreational defacements are deterred by capable

guardianship (strong military presence) and are influenced by certain measures of target suitability while political defacements are not.

## References

Al-Rizzo, Hasan M. 2008. "The Undeclared Cyberspace War Between Hezbollah and Israel." *Contemporary Arab Affairs* 1 (3): 391-405.

Bossler, Adam M., and Thomas J. Holt. 2009. "On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory." *International Journal of Cyber Criminology* 3 (1).

Choo, Kim-Kwang Raymond. 2008. "Organised Crime Groups in Cyberspace: A Typology." *Trends in Organized Crime* 11 (3): 270-295.

Clarke, Ronald V. 1999. *Hot products: Understanding, Anticipating and Reducing Demand for Stolen Goods* (Paper 112, B. Webb Ed.). London: Home Office, Research Development and Statistics Directorate.

Cohen, Lawrence E., and Marcus Felson. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review*: 588-608.

Denning, Dorothy E. 2011. "Cyber Conflict as an Emergent Social Phenomenon." in *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, 170-186. IGI Global.

Fitri, Nofia. 2011. "Democracy Discourses Through the Internet Communication: Understanding the Hacktivism for the Global Changing." *Online Journal of Communication and Media Technologies* 1 (2): 1-20.

Geers, Kenneth. 2008. "Cyberspace and the Changing Nature of Warfare." *SC Magazine* 27.

Ginges, Jeremy, Scott Atran, Douglas Medin, and Khalil Shikaki. 2007. "Sacred Bounds on Rational Resolution of Violent Political Conflict." *Proceedings of the National Academy of Sciences* 104, (18): 7357-7360.

Hackathorn, Jana, Jordan Daniels, Brien K. Ashdown, and Sean Rife. 2017. "From Rear and Guilt: Negative Perceptions of Ashley Madison Users." *Psychology & Sexuality* 8: 41-54.

Holt, Thomas J. 2003. "Examining a Transnational Problem: An Analysis of Computer Crime Victimization in Eight Countries from 1999 to 2001." *International Journal of Comparative and Applied Criminal Justice* 27 (2): 199-220.

Holt, Thomas J. 2007. "Subcultural Evolution? Examining the Influence of On-and Off-line Experiences on Deviant Subcultures." *Deviant Behavior* 28 (2): 171-198.

Holt, Thomas J. 2009. "The Attack Dynamics of Political and Religiously Motivated Hackers." *Cyber Infrastructure Protection*: 161-182.

Holt, Thomas J. 2012. "Exploring the Intersections of Technology, Crime, and Terror." *Terrorism and Political Violence* 24 (2): 337-354.

Holt, Thomas J., and Adam M. Bossler. 2013. "Examining the Relationship Between Routine Activities and Malware Infection Indicators." *Journal of Contemporary Criminal Justice* 29 (4): 420-436.

Holt, Thomas J., George W. Burruss, and Adam M. Bossler. 2018. "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.

Holt, Thomas J., Max Kilger, Lichun Chiang, and Chu-Sing Yang. 2017. "Exploring the Correlates of Individual Willingness to Engage in Ideologically Motivated Cyberattacks." *Deviant Behavior* 38 (3): 356-373.

Holt, Thomas J., Mattisen Stonhouse, Joshua Freilich, and Steven M. Chermak. 2019 "Examining Ideologically Motivated Cyberattacks Performed by Far-Left Groups." *Terrorism and Political Violence* 1-22.

Howell, Christian J., John K. Cochran, Ráchael A. Powers, David Maimon, and Hattie M. Jones. 2017. "System Trespasser Behavior after Exposure to Warning Messages at a Chinese Computer Network: An Examination." *International Journal of Cyber Criminology* 11 (1).

Kigerl, Alex. 2012. "Routine Activity Theory and the Determinants of High Cybercrime Countries." *Social Science Computer Review* 30 (4): 470-486.

Kilger, Max. 2011. "Social Dynamics and the Future of Technology-Driven Crime." in *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications,* 205-227. IGI Global.

Kugler, Richard L. 2009. "Deterrence of Cyber Attacks." *Cyberpower and National Security* 320.

Leukfeldt, Eric Rutger, and Majid Yar. 2016. "Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis." *Deviant Behavior* 37 (3): 263-280.

Lynn III, William F. 2010. "Defending a New Domain-the Pentagon's Cyberstrategy." *Foreign Affairs.* 89: 97.

Maimon, David, Mariel Alper, Bertrand Sobesto, and Michel Cukier. 2014. "Restrictive Deterrent Effects of a Warning Banner in an Attacked Computer System." *Criminology* 52 (1): 33-59.

Maimon, David, Andrew Fukuda, Steve Hinton, Olga Babko-Malaya, and Rebecca Cathey. 2017. "On the Relevance of Social Media Platforms in Predicting the Volume and Patterns of Web Defacement Attacks." in *2017 IEEE International Conference on Big Data (Big Data)*, 4668-4673. IEEE.

Maimon, David, Amy Kamerdze, Michel Cukier, and Bertrand Sobesto. 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.

Maimon, David, and Eric R. Louderback. 2019. "Cyber-Dependent Crimes: An Interdisciplinary Review." *Annual Review of Criminology* 2: 191-216.

Maimon, David, Theodore Wilson, Wuling Ren, and Tamar Berenblum. 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.

Messner, Steven F., and Richard Rosenfeld. 1997. "Political Restraint of the Market and Levels of Criminal Homicide: A Cross-National Application of Institutional-Anomie Theory." *Social Forces* 75 (4): 1393-1416.

William, Mitchell. 1995. *City of Bits: Space, Place, and the Infobahn.* Massachusetts Institute of Technology.

Ngo, Fawn T., and Raymond Paternoster. 2011. "Cybercrime Victimization: An Examination of Individual and Situational Level Factors." *International Journal of Cyber Criminology* 5 (1).

Ooi, Kok Wei, Seung-Hyun Kim, Qiu-Hong Wang, and Kai Lung Hui. 2012. "Do Hackers Seek Variety? An Empirical Analysis of Website Defacements." *AIS*.

Paternoster, Raymond, Robert Brame, Paul Mazerolle, and Alex Piquero. 1998. "Using the Correct Statistical Test for the Equality of Regression Coefficients." *Criminology* 36 (4): 859-866.

Pinkston, Daniel A. 2016. "Inter-Korean Rivalry in the Cyber Domain: The North Korean Cyber Threat in the" Sŏn'gun" Era." *Georgetown Journal of International Affairs*: 60-76.

Rasool, Sadia. 2015. "Cyber Security Threat in Pakistan: Causes, Challenges and Way Forward." *International Scientific Online Journal* 12: 21-32.

Reyns, Bradford W. 2015. "A Routine Activity Perspective on Online Cictimisation: Results from the Canadian General Social Survey." *Journal of Financial Crime* 22 (4): 396-411.

Reyns, Bradford W., Billy Henson, and Bonnie S. Fisher. 2011. "Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization." *Criminal Justice and Behavior* 38 (11): 1149-1169.

Romagna, Marco, and Niek Jan van den Hout. 2017 "Hacktivism and Website Defacement: Motivations, Capabilities and Potential Threats." in *27th Virus Bulletin International Conference*.

Trend Micro. 2019. *Website Defacement.* Retrieved from https://www.trendmicro.com/vinfo/us/security/definition/website-defacement.

Wall, David. 2007. *Cybercrime: The Transformation of Crime in the Information Age*. Vol. 4. Malden: Polity,

Wang, Jingguo, Manish Gupta, and H. Raghav Rao. 2015. "Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications." *MIS Quarterly* 39 (1).

Wilsem, Johan 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.

Woo, Hyung-jin, Yeora Kim, and Joseph Dominick. 2004. "Hackers: Militants or Merry Pranksters? A Content Analysis of Defaced Web Pages." *Media Psychology* 6 (1): 63-82.

Yar, Majid. 2005. "The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory." *European Journal of Criminology* 2 (4): 407-427.

Yucedal, Behzat. 2010. "Victimization in Cyberspace: An Application of Routine Activity and Lifestyle Exposure Theories." *PhD Diss., Kent State University.*

Zone-H. 2018. *Unrestricted information.* Retrieved from http://www.zone-h.org

**Table 1.** Descriptive Statistics for Country Data.

| **Variable** | **Observations** | **Mean** | **Standard Deviation** | **Minimum** | **Maximum** |
|---|---|---|---|---|---|
| Total Defacement | 184 | 69.47 | 304.67 | 0 | 2783 |
| Recreational Defacement | 184 | 67.42 | 171.68 | 0 | 1748 |

| | | | | | |
|---|---|---|---|---|---|
| Political Defacement | 184 | 3.38 | 13.79 | 0 | 111 |
| CERT | 184 | 0.49 | 0.50 | 0 | 1 |
| Military | 148 | 2.02 | 1.90 | 0.10 | 13.73 |
| Vulnerability | 143 | 1620.09 | 5083.59 | 4.50 | 36737 |
| Asian | 184 | 0.26 | 0.44 | 0 | 1 |
| GDP | 178 | 21473.60 | 22648.61 | 700 | 124900 |
| Education | 149 | 4.81 | 2.01 | 0.60 | 13 |
| Freedom | 176 | 56.85 | 29.95 | -1 | 100 |
| Muslim | 184 | 0.27 | 0.44 | 0 | 1 |
| Health | 168 | 6.67 | 2.53 | 1.50 | 17.10 |

**Table 2.** Assessing the Macro-Level Correlates of Website Defacement Using a Negative Binomial Regression (n=114).

| **Total Defacement** | **b** | **IRR** | **s.e.** | ***p*** |
|---|---|---|---|---|
| **Capable Guardianship** | | | | |
| CERT | -0.099 | 0.906 | 0.323 | 0.759 |

| | | | | |
|---|---|---|---|---|
| Military | -0.211 | 0.810 | 0.077 | 0.006 |
| **Target Suitability** | | | | |
| Vulnerability | 0.001 | 1.000 | 0.000 | 0.009 |
| Asian | 1.755 | 5.782 | 0.436 | 0.000 |
| GDP | 2.560 | 1.000 | 8.810 | 0.771 |
| Education | 0.012 | 1.013 | 0.100 | 0.900 |
| Freedom | 0.012 | 1.012 | 0.008 | 0.131 |
| Muslim | -1.030 | 0.357 | 0.423 | 0.015 |
| Health | -0.258 | 0.772 | 0.087 | 0.003 |
| Internet Users | 1 | | (exposure) | |

Log Likelihood=-426.285; Pseudo $R^2$=0.053

**Table 3.** Assessing the Macro-Level Correlates of Recreational Website Defacement Using a Negative Binomial Regression (N=114).

| **Recreational Defacement** | **b** | **IRR** | **s.e.** | ***p*** |
|---|---|---|---|---|
| **Capable Guardianship** | | | | |
| CERT | 0.562 | 1.754 | 0.390 | 0.150 |

| | | | | |
|---|---|---|---|---|
| Military | -0.644 | 0.524 | 0.156 | 0.000 |
| **Target Suitability** | | | | |
| Vulnerability | 0.001 | 1.000 | 0.001 | 0.030 |
| Asian | 2.159 | 8.664 | 0.469 | 0.000 |
| GDP | 9.450 | 1.000 | 9.160 | 0.302 |
| Education | -0.033 | 0.967 | 0.124 | 0.788 |
| Freedom | 0.012 | 1.011 | 0.009 | 0.199 |
| Muslim | -0.899 | 0.407 | 0.498 | 0.071 |
| Health | -0.177 | 0.838 | 0.115 | 0.124 |
| Internet Users | 1 | | (exposure) | |

Log Likelihood=-322.243; Pseudo $R^2$=0.083

**Table 4.** Assessing the Macro-Level Correlates of "Political" Website Defacement Using a Negative Binomial Regression (N=114).

| **Political Defacement** | **b** | **IRR** | **s.e.** | ***P*** |
|---|---|---|---|---|
| **Capable Guardianship** | | | | |
| CERT | 0.340 | 1.405 | 0.604 | 0.573 |

| | | | | |
|---|---|---|---|---|
| Military | -0.038 | 0.962 | 0.128 | 0.763 |
| **Target Suitability** | | | | |
| Vulnerability | 0.001 | 1.000 | 0.000 | 0.283 |
| Asian | 1.028 | 2.800 | 0.673 | 0.127 |
| GDP | 5.100 | 1.000 | 0.001 | 0.971 |
| Education | 0.148 | 1.160 | 0.171 | 0.386 |
| Freedom | -0.001 | 0.999 | 0.014 | 0.930 |
| Muslim | -0.610 | 0.543 | 0.717 | 0.394 |
| Health | -0.236 | 0.790 | 0.181 | 0.192 |
| Internet Users | 1 | | (exposure) | |

Log Likelihood=-158.159; Pseudo $R^2$=0.030