Computers in Human Behavior Reports 4 (2021) 100113

Contents lists available at ScienceDirect

Computers in Human Behavior Reports

journal homepage: www.journals.elsevier.com/computers-in-human-behavior-reports

Heterogeneity in trajectories of cybercriminals: A longitudinal analyses of web defacements

Steve G.A. van de Weijer [a,*], Thomas J. Holt [b], E. Rutger Leukfeldt [a,c]

[a] Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), Amsterdam, the Netherlands
[b] School of Criminal Justice, Michigan State University, USA
[c] Centre of Expertise Cybersecurity, The Hague University of Applied Sciences, the Netherlands

ARTICLE INFO

Keywords:
Cybercrime
Web defacements
Hacking
Trajectories
Zone-H

ABSTRACT

Longitudinal criminological studies greatly improved our understanding of the longitudinal patterns of criminality. These studies, however, focused almost exclusively on traditional types of offending and it is therefore unclear whether results are generalizable to online types of offending. This study attempted to identify the developmental trajectories of active hackers who perform web defacements. The data for this study consisted of 2,745,311 attacks performed by 66,553 hackers and reported to Zone-H between January 2010 and March 2017. Semi-parametric group-based trajectory models were used to distinguish six different groups of hackers based on the timing and frequency of their defacements. The results demonstrated some common relationships to traditional types of crime, as a small population of defacers accounted for the majority of defacements against websites. Additionally, the methods and targeting practices of defacers differed based on the frequency with which they performed defacements generally.

1. Introduction

Criminological inquiry regarding the nature of offender behavior over time has increased dramatically since the 1970s, and our understanding of the longitudinal patterns of criminality has been improved greatly (Piquero, Farrington, & Blumstein, 2003, 2007;DeLisi & Piquero, 2011;Sampson & Laub, 2003). Longitudinal studies demonstrate that there is variability in the pathways and trajectories of offenders (Piquero, 2008; Piquero et al., 2007, 2003; Van Koppen, Blokland, Van Der Geest, Bijleveld, & van de Weijer, 2014). Evidence from various studies also demonstrates that offenders differ in their frequency of offending, with a small proportion of actors performing the majority of crimes in an area (Farrington, 2003:; Piquero, Farrington, & Blumstein, 2003). In fact, chronic offenders are more likely to commit crimes for long periods of time with a higher frequency of offending generally.

The foundational literature related to heterogeneity in the timing and frequency of offending has largely focused on crime in general (DeLisi & Piquero, 2011; Farrington, 2003; Piquero, 2008; Piquero et al., 2007; Van Koppen et al., 2014), though more recent research has begun to examine the characteristics of specific offense types, such as sex offending (Lussier, Van Den Berg, Bijleveld, & Hendriks, 2012) and white collar crime (Van Onna, Van Der Geest, Huisman, & Denkers, 2014). Examinations of specific types of offenses furthers our understanding of the commonalities of crime, and enables the identification of intervention strategies that may minimize the likelihood of accelerations in offending over the life course (DeLisi & Piquero, 2011; Piquero et al., 2007; Van Koppen et al., 2014).

Such insights are essential, particularly with emergent offenses such as cybercrime, or the use of the Internet and technology in order to offend (Holt & Bossler, 2015; Leukfeldt, 2017). Some speculate that since the target of cybercrimes and the mediums in which they occur differ from traditional physical crimes, the nature of the offender must differ as well (Bossler & Burruss, 2010; Holt & Bossler, 2015). This is particularly true for computer hacking behaviors, as offenders must typically cultivate a degree of technical competency in order to successfully hack (Holt, 2007; Jordan & Taylor, 1998; Steinmetz, 2016). In addition, since hackers primarily target computer systems and data, they have near constant access to a global set of potential victims through the on-demand nature of the Internet (Holt, Leukfeldt, & Van De Weijer, 2020; Leukfeldt & Yar, 2016; Maimon, Wilson, Ren, & Berenblum, 2015; Yar, 2005).

At the same time, a growing body of evidence suggests individuals who hack are relatively similar to those who engage in deviance and crime in off-line spaces (Holt & Bossler, 2015; Maimon & Louderback, 2019). Specifically, hacking is a learned behavior informed by social

* Corresponding author.
E-mail address: svandeweijer@nscr.nl (S.G.A. van de Weijer).

https://doi.org/10.1016/j.chbr.2021.100113
Received 16 April 2021; Received in revised form 8 June 2021; Accepted 17 June 2021
Available online 20 June 2021

relationships to other offenders who provide insights on methods of and ways to justify hacking generally (Bossler & Burruss, 2010; Holt, 2007; Steinmetz, 2016). Additionally, qualitative studies suggest individuals who hack typically report an early interest in technology and involvement in simple hacking techniques during early adolescence, with some acceleration in offense frequency and severity through adolescence (Holt, 2007; Jordan & Taylor, 1998; Steinmetz, 2016). They also appear to be willing to engage in attacks against targets of convenience with weak guardianship, similar to physical crimes (Holt, Freilich, & Chermak, 2017; Maimon, Alper, Sobesto, & Cukier, 2014; 2015).

These conflicting issues call to question whether hackers' trajectories of offending differ from those of traditional delinquents and criminals. To date, there is no large-scale quantitative data source available to assess the longitudinal trajectories of hackers using traditional self-report survey data of youth (Holt & Bossler, 2015; Maimon & Louderback, 2019). As a consequence, researchers have begun to draw upon alternative data sources as a means to examine hacker behavior using actual attack data (Holt, Burruss, & Bossler, 2018; Kigerl, 2013; Maimon et al., 2014).

Researchers have become particularly in analyses of web defacements in recent years, where hacking techniques are used to change the content of an active website to a set of images, text, and sound files selected by the attacker (Banerjee, Swearingen, Shillair, Bauer, & Ross, 2021; Burruss, Howell, Maimon, & Wang, 2021; Holt et al., 2020; Howell, Burruss, Maimon, & Sahani, 2019). For instance, Banerjee et al. (2021) used machine learning techniques to assess the content of web defacements relative to the self-reported reason the individual performed the defacement. Burruss et al. (2021) also used defacement data to identify different groups of website defacers based on their attack volume. Using data from 1,062 defacements performed by 119 hackers reported between June 1 and August 1, 2017, they distinguished a smaller group of high-volume defacers (31% of the sample) from a larger group of low-volume defacers (69%).

Thus, the current study builds upon these studies by using a much larger dataset of defacements over a seven-year window, and by classifying different groups of hackers on both the timing and frequency of their defacements. Additionally, the current study examined whether these groups of hackers differ in their self-reported motivations, in the targets they select, and in the modus operandi of their defacements. Addressing these questions will improve our inherent understanding of the qualities and practices of defacers and the extent to which they resemble offending patterns of offline criminals generally.

The data for this study consisted of web defacements performed by 66,553 hackers who targeted at least one website between January 2010 and March 2017. Semi-parametric group-based trajectory models were developed through the use of zero-inflated Poisson-based models to assess heterogeneity within this group of hackers, with regard to the timing and frequency of performed defacements. The results demonstrated some common relationships to off-line crime, as a small population of defacers accounted for the majority of defacements against websites. Additionally, the methods and targeting practices of defacers differed based on the frequency with which they performed defacements generally. The implications of this study for our understanding of computer hacking, and criminal career research generally were examined in detail.

1.1. Computer hacking and web defacements

The broader literature exploring street criminality demonstrates consistent longitudinal patterns of behavior across offenders (Farrington, 2003; Piquero, 2008; Piquero et al., 2003, 2007). Minimal research to date has considered the extent to which these dynamics may be observed in cybercriminals. This is due largely to the lack of consistent empirical evidence of hacks performed against various targets by the same set of actors over time (Holt & Bossler, 2015; Leukfeldt, 2017; Maimon & Louderback, 2019). Additionally, longitudinal panel data assessing participation in even simple forms of cybercrime is virtually non-existent, making it difficult to identify consistent patterns and trajectories of hacking (Holt, Navarro, & Clevenger, 2020; Leukfeldt, 2017). As a consequence, there may be value in identifying a form of hacking that can performed for various personal motivations using multiple techniques to produce the same outcome in order to identify variations in attacker trajectories (Holt et al., 2020; Howell et al., 2019; Woo, Kim, & Dominick, 2004).

One of the few forms of hacking that would allow for such a measure are web defacements, as they allow attackers to replace the existing content of a website with images and text of their own design, including greetings to peers and taunts to system administrators and security professionals (Denning, 2011; Holt et al., 2020; Woo et al., 2004). Defacements also cause economic harm to the target, as the website owner can incur costs associated with repairing the site, lost revenue from any website downtime, and potential reputational costs due to public nature of a defacement (Andress & Winterfeld, 2013; Denning, 2011).

Web defacements also occur with great frequency as noted by Zone-H, which maintains a self-reported database of defacements made by hackers. Their statistics indicate that 1 million website defacements had occurred during the 2017 calendar year alone (Zone-H, 2018). Recent evidence suggests that website defacements comprise about 19.7% of all types of online attacks (Passeri, 2014). This is likely due to the range of techniques that can be used to engage in a defacement, including low-skill methods such as guessing a system administrator's username and password to more sophisticated techniques including the use of vulnerabilities and malicious code (Andress & Winterfeld, 2013; Woo et al., 2004).

Web defacements can be performed for a range of reasons, most of which would be considered expressive due to their direct emotional rather than economic benefit to the attacker (Holt, Freilich, & Chermak, 2017; Woo et al., 2004). For instance, defacers who hack to demonstrate their skills and see if they can actually affect a target may feel a sense of gratification and entertainment from their attack (Holt, 2007; Jordan & Taylor, 2004:; Woo et al., 2004). Successfully completing an attack, particularly against high profile or public targets that can be verified, can also lead individuals to gain social status and respect within the hacker community (Howell et al., 2019; Taylor, 1999; Woo et al., 2004). A small proportion of attackers may also hack out of a desire for revenge against someone who they feel may have wronged them (Holt et al., 2020; Jordan & Taylor, 2004). There is also growing evidence that individuals engage in hacks in support of nationalist, political, or ideological causes (Andress & Winterfeld, 2013; Holt, Freilich, & Chermak, 2017; Jordan & Taylor, 2004). State-sponsored hackers frequently target high priority government and industry systems and networks for compromise in order to gain access to intellectual property or sensitive information (Andress & Winterfeld, 2013; Denning, 2011).

1.2. Identifying potential attacker trajectories through analyses of Web defacements

The diversity of motivations apparent among defacers, coupled with the scope of defacements regularly occurring against the broad range of targets available suggests examining defacers' behaviors longitudinally may illustrate potential offender trajectories (Holt et al., 2020; Howell et al., 2019). Prior literature on offline crime provides potential direction for hypotheses related to the behaviors of defacers generally. First, we may expect to observe a similar pattern of persistent heterogeneity of offending in defacement patterns as observed in offline offending (DeLisi & Piquero, 2011; Piquero, 2008; Piquero et al., 2003). Specifically, it is plausible a small proportion of defacers would account for the majority of all defacements performed. In fact, evidence from a recent study of defacer behaviors found 3,463 defacers accounted for 138,361 defacements against IP addresses hosted in The Netherlands (Holt et al., 2020). Burruss et al. (2021) also identified a relatively small group of high-volume defacers who were responsible for the majority of website defacements in their sample.

In addition, it is expected that a small proportion of defacers may be able to offend repeatedly over long periods of time due to the investigative challenges and low risk of prosecution observed with most cybercrimes (Brenner, 2009; Hutchings & Holt, 2017; Smith, Grabosky, & Urbas, 2004). Some individuals may also be inclined to engage in web defacements for long periods of time due to their persistent skill development and desire to demonstrate their expertise and mastery of techniques (Holt, Freilich, & Chermak, 2017; Steinmetz, 2016). A larger proportion of defacers may only engage in defacements for a small period of time, either abandoning the activity in favour of other interests, or because they pivot from defacements to more serious hacks (Denning, 2011; Holt, Freilich, & Chermak, 2017; Hutchings & Holt, 2015).

There should also be distinct differences observed in the behavior of defacers on the basis of both their frequency of offending and length of time engaged in defacements similar to street offenders (DeLisi & Piquero, 2011; Farrington, 2003; Piquero et al, 2003, 2007; Van Koppen et al., 2014). First, the motivations of offenders may differ depending on the length of their involvement in defacements, with persistent defacers reporting fewer attacks for overtly expressive reasons over time. For instance, individuals may initially engage in defacements for the sake of gaining a reputation among other hackers (Holt et al., 2017, 2020). Those who deface for longer periods of time may transition from doing so for notoriety or entertainment, to attacking sites for a cause, or utilitarian reasons such as becoming more proficient in a certain attack method (Holt, 2007; Holt, Freilich, & Chermak, 2017; Jordan & Taylor, 2004; Steinmetz, 2016).

The characteristics of the defacement may also vary based on the point an individual may be on their trajectory as a defacer. Specifically, defacers may target a single website at a time, or attempt to engage in a so-called mass defacement where all pages hosted on a server have been compromised and changed by the attacker (Howell et al., 2019; Jordan & Taylor, 2004; Woo et al., 2004). From a value perspective, engaging in a mass defacement would garner an attacker more credit within the cybercrime community due to the skill or knowledge required to successfully hack the site (Holt, 2010; Holt et al., 2020; Steinmetz, 2016). Higher profile attacks, especially large scale mass defacements, may also draw the risk of detection by law enforcement and increase the likelihood of arrest (Holt & Bossler, 2015; Smith et al., 2004). Thus, individuals who are less persistent defacers may be more likely to affect any target, and be more willing to use mass defacement techniques to affect as many sites located online as is possible. Chronic, persistent defacers may be more likely to selectively attack single sites at a time so as to reduce their risk of detection.

A defacer may also attack the same websites over time, and that degree of persistence may be a reflection of the defacer's overall offending trajectory. System administrators or cybersecurity personnel who manage a website that is defaced would ideally change its security configuration after the incident in order to reduce the likelihood of future attacks (Andress & Winterfeld, 2013; Holt & Bossler, 2015; Woo et al., 2004). This change may make the defaced site a more attractive target for some defacers due to the increased difficulty with which it may be compromised. Some hackers describe hacking as a logic puzzle or game that must be completed, and the degree of difficulty involved in successful hacks can also help individuals gain some status in the community (Holt, 2007; Jordan & Taylor, 1998; Steinmetz, 2016).

To that end, individuals who are motivated by a desire to demonstrate their skills or as a challenge to their abilities were more likely to repeatedly deface websites (Holt et al., 2020). In this respect, hackers who engage in redefacements may deface with more frequency. In line with this hypothesis, Burruss et al. (2021) indeed found a positive relationship between engaging in redefacements and the number of defacements among both low-volume and high-volume defacers.

Additionally, web defacements may affect the homepage of a site, or a secondary page within the overall domain (Holt et al., 2020; Howell et al., 2019). It is feasible to argue that a defacement targeting a homepage may be more severe as it is more likely to be observed by the public and identified by the victim (Denning, 2011; Holt et al., 2020; Jordan & Taylor, 2004). Affecting a secondary page may be less likely to be detected by the target or the public, though the defacement can still be proven by the attacker. As a result, more frequent defacers may be less discriminatory in the target of their attack, making them more likely to affect any page within a website rather than striking at the main page of the site only. Burruss et al. (2021) did not find that the attack volume of defacers was related to the attacking of homepages or secondary pages. This may, however, be explained by the fact that they focused on 'special defacements' which are attacks against critical infrastructure, such as attacks against government websites. For such websites, the difference in severity and likelihood of detection between defacements of the homepage and of secondary pages might be smaller than for other websites.

It is unclear whether the frequency with which a defacer engages in attacks depends on the methods they utilize. Individuals can implement a variety of techniques to produce defacements, which depends in part on the capabilities of the defacer and the characteristics of their target (Holt et al., 2020; Woo et al., 2004). In fact, the various server operating systems and targets available online mean that attackers are not limited to one method of attack in order to complete a defacement (Andress & Winterfeld, 2013; Maimon et al., 2015). In some cases, simple password guessing can be used to access system administrator privileges, or various attack scripts targeting the server's operating system (Holt, 2007; Steinmetz, 2016). Additional common attack techniques employed by defacers involves SQL injection or file inclusion attacks, where weaknesses in database software are used to gain control access to the site (Holt et al. 2017, 2020).

Since various methods can produce a defacement, it may be that the frequency with which an individual engages in defacements is associated with the range of attacks they employ. For instance, frequent defacers may be more apt to use a smaller range of attacks that are most likely to affect the widest number of web sites. Less frequent defacers may be more willing to use a broader number of attacks to ensure success, though they may be more interested in affecting a smaller group of targets. In fact, qualitative research on religiously-motivated defacers noted that they are willing to use whatever attack techniques are necessary to complete their task against ideologically appropriate targets (see also Holt, Freilich, & Chermak, 2017). Few researchers have addressed this question, thus it is unclear whether these relationships would be supported through statistical analyses.

1.3. The present study

Taken as a whole, there may be unique factors that shape the trajectories of individuals who engage in web defacements. It is not clear how these longitudinal patterns of defacers mirror what is known about traditional street criminals generally. Thus, this study is the first to explore heterogeneity in the length and frequency of defacers' offending trajectories, using a massive data set of over 2 million defacements performed by 66,553 defacers over a seven-year period. The self-reported motivations, selected targets and methods of defacement were also explored to identify any additional variations in the defacers' trajectories over time. Two research questions guided this analysis:1) can different groups of defacers be identified, based on the timing and frequency of their defacements, and 2) to what extent do these group differ in their motivations, selected targets and defacement methods?

2. Data and methods

In order to examine heterogeneity in the longitudinal trajectories of defacers, this study makes use of the archive of web defacements maintained at the website 'Zone-H' (www.zone-h.com). For over two decades, Zone-H has been active in various forms, providing an outlet for hackers who engage in web defacements to publicly report websites that they have defaced (Woo et al., 2004). Hundreds of thousands of websites are archived here annually and given the paucity of data available on this

subject, it is regarded as a relatively comprehensive data store for those hackers advertising their defacement activity (Holt et al., 2020; Howell et al., 2019; Maggi, Balduzzi, Flores, Gu, & Ciancaglini, 2018).

When a malicious actor engages in a defacement, it can be reported to the Zone-H website through an on-line form. Reporters are asked to provide a hacker handle (e.g., an adopted online identity of the individual or group) that is labeled as the "notifier" for the attack. Moreover, they are asked to report specific characteristics of the defacement, such as the date and time of the attack, the affected web domain, the modus operandi of the attack, and the motivation of the actor. When this information is validated by the Zone-H administrators, the defacement is then archived and mirrored in perpetuity on their site.

These conditions essentially make Zone-H a self-report repository for web defacements, similar to traditional data sources for criminological inquiry (e.g. Holt et al., 2020; Howell et al., 2019). This study focused on all 2,745,311 attacks that were reported to Zone-H between January 2010 and March 2017, which was the point at which the researchers requested access to the data. Based on the hacker handles present in the data, it was possible to identify 66,553 unique hackers or hacker groups who defaced one or more websites during the research period.

2.1. Variables

The longitudinal trajectories of defacers were developed based on the number of attacks attributed to each unique defacer handle reported during the research period. A distinction was made between two types of defacements: mass defacements and single defacements. In a mass defacement, as many pages hosted on a server as possible are targeted in a single attack. In the data from Zone-H, however, all pages that were defaced during a mass defacement were listed separately. We decided to count all defaced websites that were attacked in a mass defacement, by the same hacker, on the same day, with the same modus operandi, and with the same motivation, as one attack in order to avoid an overestimation of the number of attacks in the case of a mass defacement. Single defacements are targeted on a single page or url and are therefore all counted as separate attacks. This resulted in a total number of 2,745,311 attacks, which equals an average number of 41.25 attacks per hacker (range: 1 and 39,422).[1] Based on the dates on which attacks were reported, they were divided over the 29 quarters of a year between January 2010 and March 2017.

Other variables in the analyses were used to describe differences between groups of defacers with different developmental trajectories. First of all, the reporting attackers indicated their *motivations* for performing the defacement by choosing from six options: 1) just for fun, 2) as a challenge, 3) to be the best defacer, 4) patriotism, 5) political reasons, and 6) revenge against that website. A seventh category, not reported, was added for those who did not want to report their reasons.

A second variable indicates whether a defacer targeted the *homepage* or a secondary page of a website. Defacements of the homepage may generate greater attention as they are immediately visible to anyone visiting that URL, while secondary pages may be more easily accessible as they are generally less secured. Third, a binary variable was constructed to indicate whether an attack was a *mass defacement* or a single defacement. A fourth measure assessed whether the site was *redefaced*, measuring whether it was attacked once or multiple times by different attackers.

Fifth, the *operating system of the server* was included in the analyses as it is thought that open source programs may be more secure than closed source programs due to the public reporting and patching processes used by open platforms such as Linux. Since the large majority of servers in this sample utilized some variation of the Linux operating system, a binary variable was constructed indicating whether Linux or non-Linux systems (e.g., Macintosh, Microsoft, or Unix-based programs) were used.

Finally, the attackers reported to Zone-H about the *attack methods* that they used. These methods were recoded into a categorical variable with the following six categories: 1) SQL injections, 2) Known vulnerabilities, 3) File inclusion, 4) Server intrusion, 5) Other methods, and 6) Not reported. These categories reflect the most common forms of attack, and demonstrate the diversity of skills defacers may employ. SQL injection and file intrusions are commonly employed by defacers and involve some technical competency on the part of the attacker to effectively use against a target (Andress & Winterfeld, 2013; Holt et al., 2020). The use of known vulnerabilities requires additional skill in order to be effective as the defacer must understand how the vulnerability works and what existing attack scripts may be employed against the target to enable the defacement (Andress & Winterfeld, 2013; Holt et al., 2020). The other category includes a range of attack techniques that may require less skill on the part of the defacer to cause harm, such as password guessing through dictionary attack scripts (Maimon et al., 2015), as well as social engineering or system misconfigurations by the website administrator. Thus, this measure enabled an assessment of the relationship between defacer trajectories and the sophistication of the attack.

2.2. Analytic approach

Semi-parametric group-based trajectory models were applied in order to identify distinct groups of defacers with different developmental trajectories of hacking activity over time. In these models, the unknown underlying continuous distribution of defacements by a discrete number of unobserved groups is estimated (Nagin, 1999, 2005). A zero-inflated Poisson-based model was used as the number of defacements in a period takes the form of a count event and because most attackers did not carry out any attack during most periods. Moreover, a few attackers were highly active during specific periods, which led to extreme high values. In order to control for such outliers, the maximum number of attacks was set to 10 attacks per quarter in the trajectory analyses. A maximum of 10 attacks was chosen as, in each quarter, only 1 to 1.5 percent of the hackers defaced more than 10 websites.[2]

Usually, the trajectories in such analyses are estimated over the lifespan of respondents or the reporting period within the data set. Such a strategy could not be employed in the current study since the Zone-H data does not contain any information on the age of defacers. Instead, a hacker's first defacement within the research period (January 2010–March 2017) was taken as the starting point in their trajectory and used to examine how the number of defacements developed over the subsequent quarters. As a substantial number of the defacers started defacing at later moments within the research period, the trajectories were not estimated based on all 29 quarters between January 2010 and March 2017, but based only on the 16 quarters (i.e., 4 years) following the first defacement.

For our trajectory model it was assumed that:

$\text{Log}\,(\lambda^{j}_{it}) = \beta^{j}_{0} + \beta^{j}_{1}\,(\text{Period}/10)_{it} + \beta^{j}_{2}\,(\text{Period}/10)^{2}_{it}$ Where λ^{j}_{it} is the expected number of attacks by defacer *i* in quarter *t*, given membership in group *j*. Period reflected the sequence of the quarters and period and squared period were divided by ten as for computational reasons, see Nagin (2005, p.44) for further explanation. The coefficients in the model (i.e., β^{j}_{0}, β^{j}_{1}, and β^{j}_{2}) determined the shape of the trajectory of group *j*. In order to allow the trajectories of these groups to have different shapes, these parameters were specified to vary freely across groups. After the model was estimated, the posterior probability of each defacer *i* to be

[1] Since mass defacements are counted as a single attack, the total number of defaced websites in this dataset was much higher than the number of attacks: 8.740.171 defaced websites were reported to Zone-H between January 2010 and March 2017.

[2] Additional analyses were carried out in which a maximum of 25 and 50 attacks per quarter was used, in order to examine whether and how the results of the trajectory analyses were altered by the choice of this maximum number of defacements.

assigned to each group *j* was estimated. Each defacer was then assigned to the group with the highest posterior probability of assignment.

The Bayesian Information Criterion (BIC) was used to determine the optimal number of groups. A higher BIC (i.e., less negative) indicates that the model fits the data better, and therefore the model with the highest BIC value is usually selected (Nagin, 2005). Next, the average posterior probability of assignment (AvePP), and the odds of correct classification (OCC) were used to assess model adequacy. The AvePP is the average posterior probability of assignment of all defacers assigned to a particular group. The OCC is based on the AvePP but corrects for the estimated probability of group membership $\widehat{\pi}_j$. This $\widehat{\pi}_j$ is the probability that a random defacer from the sample was allocated to group *j*. The values of the AvePP and OCC should, respectively, be at least .7 and 5 for all groups to indicate good assignment accuracy (Nagin, 2005).

The variables related to each attack were then aggregated to the defacer level, such that each variable indicated in what percent of the attacks a defacer reported a specific motivation, target, or hacking method. For example, a score of 0.75 on the variable *homepage* indicated that this defacer defaced homepages in 75 percent of the attacks. These variables were then included in a multinomial logistic regression analyses in which group-membership was predicted. The pair-wise comparisons show to what extent high scores on each motivation, selected targets, and hacking methods were related to an increased probability to follow a certain longitudinal trajectory.

3. Results

Trajectory models distinguishing up to 10 different groups were estimated. The BIC-values kept increasing with every additional group that was added to the model, a pattern that is not uncommon in studies using large datasets (see for example, Blokland, Nagin, & Nieuwbeerta, 2005; Van Koppen et al., 2014). Nagin (2005) recommended that in such cases "more subjective criteria based on domain knowledge and the objectives of the analysis must be used to select the number of groups to include in the model" (p. 74). In this case, the six-group model was selected, as the addition of more groups to the model did not lead to substantively different trajectories than those estimated in the six-group model. Moreover, the AvePP's and OCC's in the six-group model (see Table 1) were all larger than 0.7 and 5, respectively, indicating that the defacers were assigned to groups with high accuracy.

Fig. 1 illustrates the development of the trajectories from the six-group model. The first two groups in Fig. 1 were groups that only offended sporadically, during one or a couple of quarters. The largest group were the low sporadic defacers, who comprised 69.1 percent of all defacers. The majority of the defacers in this group only performed one or a few attacks in a single quarter. Only 971 low sporadic defacers (2.1%) also defaced one website in the second quarter. In fact, defacers in this group were responsible for an average of 1.6 attacks overall.

The high sporadic group was much smaller, encompassing only 8.2 percent of the defacers in the sample. The defacers in this group were very active during the first quarter when they appeared and all defaced at least four websites in this period. After this first quarter, their defacement activity rapidly declined, and only 4.2 percent of them continued to deface websites during the third quarter. On average, the high sporadic defacers performed 17.83 attacks.

Next, the low declining defacers (7.2% of all defacers) and high declining defacers (7.5%) were active in the first couple of quarters of the research period, then the majority stopped defacing websites after one to two years. The low declining defacers were responsible for an average of 4.74 attacks, while the high declining group was much more active with 55.09 attacks per defacer.

Finally, two groups of defacers were identified in the trajectory analyses, who defaced websites persistently. The low chronic group included 5.1 percent of all defacers who performed an average number of 116.58 attacks. The high chronic group was the smallest group with only 2.9 percent of the defacers. These high chronic defacers were by far the most active, performing 963.43 attacks on average. These findings demonstrated that defacements strongly concentrate within a small group of hackers: 68.5 percent of all attacks were carried out by only the 2.9 percent of defacers in the high chronic group.[3]

Next, Table 2 shows the average scores of defacers in the six groups on their reported motivations, selected targets, and used hacking methods. No substantial differences were observed in reported motivations across groups. The most frequently reported motivation among all defacers was doing it 'just for fun' (46.1%). Moreover, the high chronic defacers indicated that they defaced websites 'to be the best defacer' with some frequency (12.3%), while the low sporadic (8.9%) and low declining defacers (8.3%) were least likely to report this motivation. In addition, both the low (10.4%) and high chronic defacers (10.7%) defaced websites for political reasons with some frequency.

The results in Table 2 show that the defacers used a mass defacement in less than a third of their attacks (31.5%) on average, and that redefacements were relatively infrequent (15.1%). The high chronic defacers and the two groups with the lowest number of attacks, the low sporadic and low declining defacers, redefaced websites with some frequency, while they were less likely to use mass defacements compared to the other three groups. Homepages were defaced in about two thirds of the attacks on average (65.5%), although the high chronic defacers were considerably less likely to do so. Furthermore, defacers from all groups targeted Linux operating systems in the majority of their attacks (81.3% overall), which may be a function of the common use of this software for web servers (Holt et al., 2020).

Finally, there was some variety in the hacking methods employed within each group (see Table 2). In fact, the most frequently reported attack method within each trajectory group was the other methods category. In addition, the low sporadic and low declining defacers relatively often used SQL injections. The high sporadic, high declining, and high chronic defacers were the groups that most often exploited known vulnerabilities to deface websites. Both file and server inclusion methods were most often used by the low and high chronic groups.

In order to test whether these differences between groups were significant, multinomial logistic regression analyses were performed in which group membership was predicted. Table 3 shows all pair-wise comparisons with the low sporadic group as the reference category, though all comparisons between the other groups can be found in the Appendix. Although many pair-wise comparisons in the multinomial logistic regression analyses showed significant differences between groups, the Nagelkerke R^2 of the model indicated that it explained only 2

Table 1
Model specifications of trajectory groups.

Group	N (%)	Avepp	OCC	Average number of attacks
Low Sporadic	45,975 (69.1%)	0.96	12.04	1.60
High Sporadic	5,470 (8.2%)	0.87	73.94	17.83
Low Declining	4,763 (7.2%)	0.91	106.11	4.74
High Declining	5,015 (7.5%)	0.89	98.37	55.09
Low Chronic	3,377 (5.1%)	0.93	228.27	116.58
High Chronic	1,953 (2.9%)	0.93	401.89	963.43
Total	66,553 (100%)			41.25

Note: The average number of attacks are based on all defacements between January 2010 and March 2017, and not only on the first 16 months after the first attack.

[3] Additional trajectory models were estimated, in which maximum numbers of 25 and 50 defacements per quarter were used. These analyses resulted in similar trajectories as those shown in Fig. 1, although the estimated number of defacements per quarter was higher, particularly for the high chronic and high declining defacers.

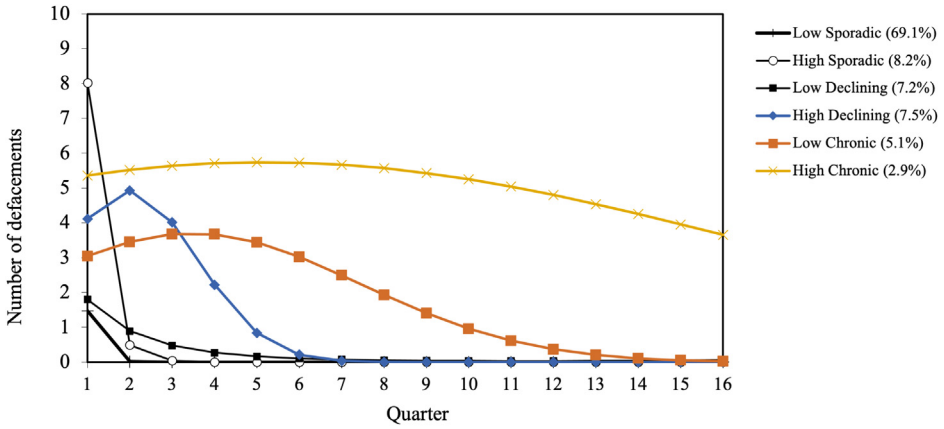

Fig. 1. Developmental trajectories of the six-group model.

Table 2
Average scores of trajectory groups on motivations, targets and hacking methods.

		Low Sporadic	High Sporadic	Low declining	High declining	Low chronic	High chronic	Total
Motivation								
Challenge		7.7%	7.5%	7.3%	7.7%	7.7%	7.1%	7.6%
Fun		46.2%	46.5%	46.7%	45.4%	44.9%	46.3%	46.1%
To be the best		8.9%	10.4%	8.3%	10.3%	10.3%	12.3%	9.3%
Patriotism		5.5%	5.7%	5.4%	5.3%	5.0%	4.8%	5.5%
Political		9.1%	9.3%	9.6%	9.6%	10.4%	10.7%	9.3%
Revenge		7.8%	7.6%	7.8%	8.2%	8.8%	8.1%	7.9%
Not reported		14.8%	13.0%	14.9%	13.6%	13.0%	10.7%	14.4%
Targets								
Mass defacements	29.9%		35.5%	30.8%	38.8%	37.5%	32.7%	31.5%
Redefacements	15.5%		12.8%	16.8%	12.8%	14.5%	15.5%	15.1%
Homepage	66.7%		63.9%	63.6%	63.6%	62.7%	55.6%	65.5%
Linux	81.0%		81.0%	80.7%	84.2%	82.0%	82.3%	81.3%
Hacking method								
SQL injections	22.4%		18.2%	21.7%	19.0%	18.2%	18.0%	21.4%
Known vulnerabilities	12.5%		15.2%	11.9%	13.3%	11.3%	16.1%	12.8%
File inclusion	6.0%		7.4%	6.7%	7.2%	8.6%	8.0%	6.5%
Server inclusion	15.5%		16.6%	15.8%	16.5%	17.7%	17.3%	15.8%
Other methods	31.6%		31.8%	31.4%	31.7%	32.0%	30.4%	31.6%
Not reported	12.0%		10.8%	12.5%	12.3%	12.2%	10.1%	11.9%

percent of the variance between groups. Thus, the model does not predict group membership very well. Despite these concerns, the analyses provide some direction for future research.

The results regarding the defacer motivations illustrated that the two groups with the lowest frequency of defacements (i.e., the low sporadic and low declining group) were significantly less likely to deface websites because they want to be the best, compared to the other four groups. The high chronic defacers were significantly more likely to report that they wanted to be the best defacers relative to all other groups. Thus, a higher frequency of defacements may be related to a desire to be recognized for one's hacks. Moreover, the low sporadic defacers were significantly less likely to deface for political reasons than the high declining, low chronic, and high chronic groups. The high chronic defacers were also significantly more likely to deface for political reasons compared to the high sporadic and low declining defacers. Only the high sporadic defacers were significantly more likely to deface because of revenge relative to low chronic defacers. No significant differences were observed between groups for defacements reported for challenge and patriotic reasons.

The results of the multinomial logistic regression analyses further showed that the high declining and low chronic groups were significantly more likely to use mass defacements than all other groups. The low sporadic and low declining groups were significantly less likely to use mass defacements compared to all other groups. Moreover, the low declining defacers were significantly more likely to redeface websites, while the high sporadic and high declining groups were significantly less likely to redeface websites. Low sporadic defacers were significantly more likely to target homepages than all other groups, though the high chronic defacers were significantly more likely to hack secondary pages. Linux operating systems were also significantly more likely to be targeted among the high chronic and high declining defacers.

Finally, analyses of the hacking methods showed that all methods were significantly less likely to be used by the low sporadic group compared to all other groups (see Table 3), indicating that SQL injections (i.e., the reference category) were more likely to be used by low sporadic defacers. Moreover, the hacking methods used by the lowest frequency groups were very similar. The other four groups reported similar uses of hacking methods, although the high sporadic and high chronic groups were significantly more likely to exploit known vulnerabilities than the high declining and low chronic groups.

4. Discussion

Longitudinal research on traditional types of criminal behavior has grown substantially since the 1990s, improving our understanding of the characteristics of offenders and variations in their trajectories of offending (DeLisi & Piquero, 2011; Piquero et al., 2003, 2007). These studies are instrumental in improving our understanding of criminality, though research is needed to increase our knowledge of specialized offenses like computer hacking, where offenders utilize their knowledge of computer hardware and software to affect the way a system functions

Table 3
Multinominal logistic regression analyses.

	High Sporadic	Low declining	High declining	Low chronic	High chronic
Reference group: Low Sporadic					
	OR (95% CI)	OR (95% CI)	OR (95% CI)	OR (95% CI)	OR (95% CI)
Motivation:					
Fun	(ref.)	(ref.)	(ref.)	(ref.)	(ref.)
Challenge	0.987 (0.868–1.122)	0.920 (0.803–1.055)	1.011 (0.886–1.154)	0.989 (0.844–1.160)	0.947 (0.765–1.171)
To be the best	1.249*** (1.119–1.394)	0.894 (0.787–1.016)	1.248*** (1.113–1.399)	1.213** (1.058–1.392)	1.584*** (1.344–1.867)
Patriotism	1.087 (0.943–1.252)	0.954 (0.818–1.113)	0.998 (0.856–1.163)	0.913 (0.756–1.102)	0.946 (0.738–1.211)
Political	1.087 (0.967–1.223)	1.072 (0.949–1.211)	1.140* (1.010–1.287)	1.224** (1.064–1.408)	1.397*** (1.169–1.669)
Revenge	0.942 (0.825–1.076)	0.978 (0.853–1.123)	1.057 (0.925–1.208)	1.160 (0.995–1.354)	1.106 (0.899–1.360)
Not reported	0.939 (0.847–1.042)	0.974 (0.877–1.081)	0.928 (0.834–1.033)	0.871* (0.764–0.992)	0.762** (0.636–0.913)
Target					
Mass defacements	1.487*** (1.381–1.602)	1.092* (1.006–1.186)	1.814*** (1.681–1.956)	1.689*** (1.542–1.850)	1.263*** (1.117–1.428)
Redefacements	0.712*** (0.640–0.792)	1.124* (1.018–1.240)	0.728*** (0.651–0.813)	0.891 (0.787–1.010)	0.925 (0.791–1.082)
Homepage	0.804 *** (0.750–0.863)	0.832*** (0.772–0.895)	0.745*** (0.693–0.801)	0.730*** (0.669–0.796)	0.507*** (0.455–0.565)
Linux	1.006 (0.924–1.095)	1.014 (0.928–1.109)	1.335*** (1.214–1.468)	1.090 (0.979–1.214)	1.277*** (1.109–1.471)
Hacking method:					
SQL injections	(ref.)	(ref.)	(ref.)	(ref.)	(ref.)
Known vulnerabilities	1.613*** (1.447–1.798)	0.973 (0.864–1.096)	1.336*** (1.189–1.500)	1.151 (0.993–1.334)	1.795*** (1.509–2.135)
File inclusion	1.708*** (1.481–1.969)	1.184* (1.014–1.381)	1.547*** (1.332–1.796)	2.049*** (1.732–2.423)	1.895*** (1.517–2.367)
Server inclusion	1.364*** (1.223–1.521)	1.093 (0.977–1.224)	1.256*** (1.122–1.406)	1.465*** (1.282–1.675)	1.511*** (1.269–1.799)
Other methods	1.273*** (1.160–1.396)	1.049 (0.956–1.152)	1.187*** (1.079–1.306)	1.275*** (1.135–1.431)	1.255** (1.078–1.461)
Not reported	1.175* (1.038–1.330)	1.109 (0.982–1.254)	1.298*** (1.147–1.469)	1.416*** (1.219–1.645)	1.291* (1.052–1.584)
Overall N	**66,553**				
Nagelkerke R^2	**0.020**				

Note: *p < .05; **p < .01; p < .001.

(Holt & Bossler, 2015; Leukfeldt, 2017; Maimon & Louderback, 2019). Computer hacking and hackers are thought by some to be different from traditional offender groups due to the specialized knowledge required to be effective (Holt, 2007; Steinmetz, 2016) and differences in the availability of potential targets for offending available at all times online (Maimon et al., 2015; Maimon & Louderback, 2019; Yar, 2005).

This study sought to address this gap in research by exploring the heterogeneity in the trajectories of computer hackers who engage in web defacements, where they change the content of a website to feature images, music, and text of the attacker's choosing (Banerjee et al., 2021; Holt et al., 2020; Howell et al., 2019; Woo et al., 2004). A sample of over 2 million web defacements performed by 66,553 unique attacker names were analyzed to assess the characteristics of defacers' attacks over time. Six groups of defacers were distinguished based on the frequency and timing of their attacks over the seven-year period of our data: low and high sporadic defacers, low and high declining defacers, and low and high chronic defacers.

The analyses found that a small group of defacers performed a large number of web defacement throughout the research period, mirroring prior research on street offenders generally (DeLisi & Piquero, 2011; Piquero, 2008; Piquero et al., 2007). This group of 2.9 percent high chronic defacers was responsible for 68.5 percent of all attacks reported during the seven-year period of study. The strong concentration of offending within the high chronic group was larger than what has been observed in broader samples of street criminals generally (Blokland et al., 2005; D'unger et al., 1998; Piquero, 2008).

A possible explanation for this finding could be that cybercriminals have a lower risk of prosecution which enables a longer overall offending trajectory relative to traditional street criminals (Holt & Bossler, 2015; Hutchings & Holt, 2017; Smith et al., 2004). In addition, defacers do not have to converge in physical space and time with their targets (Newman & Clarke, 2003; Yar, 2005), enabling them to asymmetrically affect hundreds of pages at a time within a website through the use of mass defacements (Holt et al., 2017, 2020; Howell et al., 2019).

An alternative explanation for the high concentration of attacks within the high chronic defacer group might be that the hacker handles reporting the attacks to Zone-H reference hacker groups rather than individuals. Groups of defacers have been observed in various parts of the globe, and consist of multiple hackers who often seek to attack a large number of websites quickly (Denning, 2011; Holt, Freilich, & Chermak, 2017). To partially control for the possibility that the number of high chronic defacers was overestimated due to the presence of hacker groups, the trajectory model limited the maximum number of defacements to 10 per quarter. Since an individual could easily reach 10 defacements in a quarter, it seems likely that the high chronic defacers included both individuals and groups. Since we were not able to separate individuals and groups in our data, future research is needed to assess the ways that hacker group affiliation affects one's overall offending practices (see Dupont, Côté, Boutin, & Fernandez, 2017; Leukfeldt, Kleemans, & Stol, 2017).

The analyses also demonstrated that chronic, high-frequency defacers were different from other defacer group trajectories based on the characteristics of their attacks. This category of defacers were more often motivated by a desire to be the best compared to attackers in other trajectories. High chronic defacers were also more likely to exploit known vulnerabilities when attacking, and used various methods overall. They were also less likely to redeface websites and to target homepages.

The other defacer trajectories identified in this analysis were much less active, and again mirrors prior research on street offending generally (DeLisi & Piquero, 2011; Piquero, 2008; Piquero et al., 2007). The majority of defacers (69.1%) were classified as low sporadic defacers who only defaced one or a few websites within a short time period. It is unclear if these individuals grew bored with hacking and moved on to other activities, or transitioned into more serious criminal hacks (Holt & Bossler, 2015; Hutchings, 2015). In fact, low sporadic defacers were the least likely to report that they wanted to be the best defacer. They were, however, more likely to deface the homepages of websites which could indicate that they wanted their messages to be observed by as much people as possible. It is unclear whether such visibility increased their perceived risk of arrest and thereby impacted the length of their overall career, or if they simply found other ways to express themselves through hacking or other means (see Holt, Freilich, & Chermak, 2017; Steinmetz, 2016). Further study is needed to assess the factors that directly and indirectly affect desistence from hacking, particularly web defacements, to better understand when, why, and how actors leave the activity (Brewer et al., 2019; Holt & Bossler, 2015).

Taken as a whole, these findings illustrate that cybercrime offending trajectories share some common characteristics with offline crime.

Though there are differences in the composition and features of cybercrime, the similarities in the general nature of offender behaviors provides a beneficial basis for future research. At the same time, it is important to note that the differences between groups were small and that the multinomial regression analyses did not predict group membership very well. As a result, future study is needed to assess the pathways individuals take to become defacers, and transition away from the behavior over time toward other forms of hacking or totally cease their hacking behaviors (Brewer et al., 2019; Holt & Bossler, 2015; Holt et al., 2020; Jordan & Taylor, 2004). Future studies should therefore take into account other characteristics of defacers and the content that they use in defacements as a means to compare attackers by their trajectory and motivation (see also Holt et al., 2020; Woo et al., 2004).

The results of this analysis also provide critical direction for law enforcement and policy-makers, as defacers appear able to operate with a degree of impunity over time leading to potentially lengthy defacement careers. As a small group of chronic offenders is responsible for the large majority of all defacements, it is imperative that intervention strategies be developed and targeted at them to effectively minimize their long-term, persistent attacks against various websites (Brewer et al., 2019; Holt & Bossler, 2015; Hutchings, 2015; Maimon & Louderback, 2019; NCA, 2017). The specific findings of this study regarding the targeting practices of high chronic defacers being more likely to attack secondary pages and to exploit known vulnerabilities could be used to develop interventions to reduce their attacks over time. Since these high chronic defacers reported that they wanted to be the best defacer in many cases suggests that there may be value in identifying alternate pathways for technologically proficient youth, which could enable them to apply and develop their skills and solve problems without violating the law, thereby minimize long term offender trajectories (Hutchings, 2015; NCA, 2017; Steinmetz, 2016).

Although this study offers various new insights into the longitudinal offending patterns of web defacers, it is also limited in several ways. First, the data used in this analysis does not provide information on the age of the attackers. It is impossible to estimate where the developmental trajectory of defacements intersects with an individual's biological age to better asses the life-course of cybercriminality. Instead, the trajectories used reflect only the times the individual appears in this data set, beginning with the first quarter of the year in which a defacer affected their first website. Thus, defacers could be classified into the same trajectory group, though they are at very different stages of physical and mental development. This makes it difficult to compare these results to trajectory studies of street criminals, which are usually estimated over the individual's life-course (DeLisi & Piquero, 2011; Piquero, 2008). Longitudinal data are needed in order to better understand cybercriminality and its relationship to biological age and physical development over the life-course, particularly among juvenile samples (Holt, Navarro, & Clevenger, 2019; Hutchings, 2015; Maimon & Louderback, 2019).

A second limitation is that the online nickname or handle of the person that reports the defacement is our only measure for individuals in the data. The identity of the reporter was not independently verified, making it difficult to know the extent to which all hacker handles were attributable to unique individuals. A single person could have used multiple nicknames within the research period, or a group of actors may have shared a single handle (e.g. Holt, Freilich, & Chermak, 2017; Taylor, 1999). This count issue potentially calls to question the validity of our categories, and requires careful interpretation of these findings. Future research is needed to disentangle the role of single versus group account hacks and explore the behavior of cybercriminals using longitudinal panel designs to assess individual activities and their engagement with larger collectives of hackers. Such inquiry would greatly expand our understanding of hacking and the pathways that shape hacker trajectories over time (see Holt et al., 2019).

Third, the substantial number of defacements reported during the period of study demonstrates the massive scope of hacks that occur on a daily basis. Not all defacers may, however, be willing to report their activities to an online service which will verify their attacks and post the information publicly. Consequently, the findings of this study are only generalizable to defacers who are willing to share their attacks with others (Holt et al., 2020; Howell et al., 2019). Finally, this study was limited to one specific type of hacking, which limits our ability to assess the broader criminal activities of defacers on- and off-line. Future research is needed to explore the extent to which cybercriminals are specialists, such as only engaging in web defacements, or generalists who engage in a range of offenses (Holt et al., 2020; Leukfeldt et al., 2017; Maimon & Louderback, 2019). Such research would greatly improve our understanding of the contours of cybercriminality and its relationship to off-line crimes.

In conclusion, this study provides evidence for heterogeneity within the population of website defacers, with regard to the timing and frequency of their performed defacements. In line with research on traditional types of crime, a small group of chronic defacers accounted for the majority of defacements against websites while the majority of defacers only defaced websites sporadically. The motivations, methods, and targeting practices of defacers differed based on the frequency with which they performed defacements generally, but did not predict group membership very well. Therefore, more research into the characteristics of chronic defacers is necessary to help to identify these active defacers at an early stage and to guide interventions to effectively deter them from a long term offender trajectory.

Funding details

This work was supported by the US Department of Homeland Security under Grant ASUB00000368.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix

	Low declining	High declining	Low chronic	High chronic	High declining
Reference Group:	**High Sporadic**				**Low Declining**
Motivation:	**OR (95% CI)**	**OR (95% CI)**	**OR (95% CI)**	**OR (95% CI)**	**OR (95% CI)**
Fun	(ref.)	(ref.)	(ref.)	(ref.)	(ref.)
Challenge	0.933 (0.780–1.114)	1.024 (0.860–1.220)	1.002 (0.824–1.219)	0.959 (0.753–1.221)	1.098 (0.916–1.317)
To be the best	0.716*** (0.610–0.840)	0.999 (0.861–1.159)	0.972 (0.822–1.148)	1.268* (1.049–1.533)	1.395*** (1.186–1.642)
Patriotism	0.878 (0.720–1.071)	0.918 (0.753–1.118)	0.840 (0.670–1.053)	0.870 (0.659–1.148)	1.045 (0.850–1.286)
Political	0.986 (0.839–1.157)	1.049 (0.894–1.230)	1.126 (0.946–1.340)	1.284* (1.045–1.579)	1.064 (0.904–1.253)
Revenge	1.038 (0.866–1.245)	1.122 (0.939–1.340)	1.232* (1.015–1.495)	1.174 (0.925–1.489)	1.080 (0.900–1.296)

(*continued on next column*)

(*continued*)

	Low declining	High declining	Low chronic	High chronic	High declining
Reference Group:	**High Sporadic**				**Low Declining**
Motivation:	**OR (95% CI)**	**OR (95% CI)**	**OR (95% CI)**	**OR (95% CI)**	**OR (95% CI)**
Not reported	1.036 (0.901–1.192)	0.988 (0.857–1.138)	0.927 (0.790–1.088)	0.811* (0.662–0.994)	0.953 (0.826–1.099)
Target:					
Mass defacements	0.734*** (0.661–0.815)	1.219*** (1.104–1.347)	1.135* (1.015–1.270)	0.849* (0.739–0.976)	1.660*** (1.494–1.846)
Redefacements	1.578*** (1.374–1.812)	1.022 (0.882–1.183)	1.252** (1.069–1.466)	1.299** (1.081–1.561)	0.647*** (0.562–0.746)
Homepage	1.034 (0.939–1.138)	0.926 (0.842–1.018)	0.907 (0.816–1.009)	0.630*** (0.556–0.714)	0.896* (0.812–0.988)
Linux	1.008 (0.897–1.133)	1.327*** (1.176–1.498)	1.084 (0.950–1.236)	1.270** (1.082–1.490)	1.316*** (1.162–1.491)
Hacking method:					
SQL injections	(ref.)	(ref.)	(ref.)	(ref.)	(ref.)
Known vulnerabilities	0.603*** (0.518–0.703)	0.828* (0.712–0.963)	0.714*** (0.599–0.851)	1.113 (0.913–1.357)	1.372*** (1.171–1.608)
File inclusion	0.693*** (0.569–0.845)	0.906 (0.746–1.100)	1.200 (0.974–1.477)	1.110 (0.861–1.431)	1.307** (1.067–1.601)
Server inclusion	0.802** (0.691–0.930)	0.921 (0.794–1.069)	1.074 (0.911–1.267)	1.108 (0.908–1.352)	1.149 (0.987–1.337)
Other methods	0.824** (0.727–0.934)	0.933 (0.822–1.059)	1.001 (0.868–1.155)	0.986 (0.829–1.172)	1.132 (0.996–1.285)
Not reported	0.944 (0.800–1.114)	1.105 (0.935–1.305)	1.205 (1.000–1.453)	1.099 (0.870–1.387)	1.170 (0.992–1.381)
Overall N	**66,553**				
Nagelkerke R^2	**0.020**				
	Low chronic	High chronic	Low chronic	High chronic	High chronic
Reference Group:	**Low Declining**		**High Declining**		**Low Chronic**
Motivation:	**OR (95% CI)**	**OR (95% CI)**	**OR (95% CI)**	**OR (95% CI)**	**OR (95% CI)**
Fun	**(ref.)**	**(ref.)**	**(ref.)**	**(ref.)**	**(ref.)**
Challenge	1.075 (0.879–1.315)	1.028 (0.804–1.315)	0.979 (0.803–1.193)	0.936 (0.734–1.195)	0.957 (0.738–1.240)
To be the best	1.357*** (1.134–1.624)	1.771*** (1.449–2.166)	0.972 (0.820–1.153)	1.269* (1.047–1.539)	1.305* (1.061–1.606)
Patriotism	0.957 (0.757–1.209)	0.991 (0.746–1.316)	0.915 (0.725–1.155)	0.948 (0.714–1.258)	1.036 (0.764–1.403)
Political	1.142 (0.956–1.364)	1.303* (1.058–1.606)	1.073 (0.899–1.281)	1.225 (0.994–1.508)	1.141 (0.916–1.422)
Revenge	1.186 (0.974–1.445)	1.130 (0.888–1.438)	1.098 (0.904–1.334)	1.046 (0.824–1.328)	0.953 (0.742–1.224)
Not reported	0.894 (0.761–1.050)	0.782* (0.638–0.959)	0.938 (0.798–1.103)	0.821 (0.669–1.008)	0.875 (0.704–1.088)
Target:					
Mass defacements	1.546*** (1.375–1.739)	1.157* (1.002–1.335)	0.931 (0.832–1.042)	0.697*** (0.606–0.801)	0.748*** (0.645–0.868)
Redefacements	0.793** (0.681–0.924)	0.823* (0.688–0.985)	1.225* (1.043–1.439)	1.271* (1.055–1.532)	1.038 (0.854–1.261)
Homepage	0.878* (0.787–0.979)	0.609*** (0.537–0.692)	0.980 (0.880–1.091)	0.680*** (0.600–0.772)	0.694*** (0.607–0.794)
Linux	1.075 (0.940–1.230)	1.260** (1.071–1.481)	0.817** (0.711–0.938)	0.957 (0.811–1.129)	1.172 (0.986–1.393)
Hacking method:					
SQL injections	(ref.)	(ref.)	(ref.)	(ref.)	(ref.)
Known vulnerabilities	1.183 (0.985–1.420)	1.844*** (1.504–2.262)	0.862 (0.719–1.032)	1.344** (1.098–1.645)	1.559*** (1.249–1.946)
File inclusion	1.731*** (1.393–2.150)	1.601*** (1.233–2.080)	1.324** (1.070–1.639)	1.225 (0.946–1.586)	0.925 (0.707–1.211)
Server inclusion	1.340*** (1.133–1.585)	1.382** (1.130–1.691)	1.167 (0.986–1.379)	1.203 (0.983–1.471)	1.031 (0.833–1.277)
Other methods	1.215** (1.053–1.402)	1.196* (1.005–1.423)	1.073 (0.929–1.240)	1.057 (0.887–1.259)	0.984 (0.817–1.187)
Not reported	1.276* (1.060–1.537)	1.164 (0.922–1.468)	1.091 (0.905–1.314)	0.994 (0.788–1.255)	0.912 (0.711–1.168)
Overall N	**66,553**				
Nagelkerke R^2	**0.020**				

Note: *p < .05; **p < .01; p < .001.

References

Andress, J., & Winterfeld, S. (2013). *Cyber warfare: Techniques, tactics and tools for security practitioners*. Elsevier.

Banerjee, S., Swearingen, T., Shillair, R., Bauer, T. J., & Ross, A. (2021). Using machine learning to examine cyberattack motivations on web defacement data. *Social Science Computer Review*.

Blokland, A. A., Nagin, D., & Nieuwbeerta, P. (2005). Life span offending trajectories of a Dutch conviction cohort. *Criminology, 43*(4), 919–954.

Bossler, A. M., & Burruss, G. W. (2010). The general theory of crime and computer hacking: Low self-control hackers?. In *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 1499–1527). Hersey, PA: IGI Global.

Brenner, S. W. (2009). *Cyberthreats: The emerging fault lines of the nation state*. Oxford University Press.

Brewer, R., De Vel-Palumbo, M., Hutchings, A., Holt, T. J., Goldsmith, A., & Maimon, D. (2019). *Cybercrime prevention: Theory and applications*. New York: Palgrave.

Burruss, G. W., Howell, C. J., Maimon, D., & Wang, F. (2021). Website defacer classification: A finite mixture model approach. *Social Science Computer Review*.

D'unger, A. V., Land, K. C., McCall, P. L., & Nagin, D. S. (1998). How many latent classes of delinquent/criminal careers? Results from mixed Poisson regression analyses. *American Journal of Sociology, 103*(6), 1593–1630.

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.

Denning, D. E. (2011). Cyber conflict as an emergent social phenomenon. In *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 170–186). Hershey, PA: IGI Global.

Dupont, B., Côté, A. M., Boutin, J. I., & Fernandez, J. (2017). Darkode: Recruitment patterns and transactional features of "the most dangerous cybercrime forum in the world". *American Behavioral Scientist, 61*(11), 1219–1243.

Farrington, D. P. (2003). Key results from the first forty years of the Cambridge study in delinquent development. In *Taking stock of delinquency* (pp. 137–183). Boston, MA: Springer.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on-and off-line experiences on deviant subcultures. *Deviant Behavior, 28*(2), 171–198.

Holt, T. J. (2010). Examining the role of technology in the formation of deviant subcultures. *Social Science Computer Review, 28*(4), 466–481.

Holt, T. J., & Bossler, A. M. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (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, 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.

Holt, T. J., Kilger, M., Chiang, L., & Yang, C. S. (2017). Exploring the correlates of individual willingness to engage in ideologically motivated cyberattacks. *Deviant Behavior, 38*(3), 356–373.

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.

Holt, T. J., Navarro, J. N., & Clevenger, S. (2019). *Exploring the moderating role of gender in juvenile hacking behaviors*. Crime & Delinquency, 0011128719875697.

Howell, C. J., 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.

Hutchings, A. (2015). Cybercrime trajectories: An integrated theory of initiation, maintenance and desistance. In T. J. Holt (Ed.), *Crime online: Correlates, causes, and context* (pp. 117–140). Durham: Carolina Academic Press.

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology, 55*(3), 596–614.

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: Disruption and intervention approaches. *Global Crime, 18*(1), 11–30.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review, 46*(4), 757–780.

Jordan, T., & Taylor, P. A. (2004). *Hacktivism and cyberwars: Rebels with a cause?* Psychology Press.
Kigerl, A. C. (2013). Infringing nations: Predicting software piracy rates, bittorrent tracker hosting, and p2p file sharing client downloads between countries. *International Journal of Cyber Criminology, 7*(1), 62.
Leukfeldt, E. R. (Ed.). (2017). *Research agenda the human factor in cybercrime and cybersecurity*. Eleven international publishing.
Leukfeldt, R., Kleemans, E., & Stol, W. (2017). The use of online crime markets by cybercriminal networks: A view from within. *American Behavioral Scientist, 61*(11), 1387–1402.
Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263–280.
Lussier, P., Van Den Berg, C., Bijleveld, C., & Hendriks, J. (2012). A developmental taxonomy of juvenile sex offenders for theory, research, and prevention: The adolescent-limited and the high-rate slow desister. *Criminal Justice and Behavior, 39*(12), 1559–1581.
Maggi, F., Balduzzi, M., Flores, R., Gu, L., & Ciancaglini, V. (2018). Investigating web defacement campaigns at large. In *Proceedings of the 2018 on asia conference on computer and communications security* (pp. 443–456).
Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology, 52*(1), 33–59.
Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology, 2*, 191–216.
Maimon, D., 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*.
Nagin, D. S. (1999). Analyzing developmental trajectories: A semiparametric, group-based approach. *Psychological Methods, 4*(2), 139.
Nagin, D. (2005). *Group-based modeling of development*. Boston, MA: Harvard University Press.
NCA. (2017). *Intelligence assessment: Pathways into cybercrime. National cyber crime unit/ prevent team.* London: National Crime Agency. https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file.
Newman, G., & Clarke, R. (2003). *Superhighway robbery: Preventing e-commerce crime*. Cullompton: Willan Publishing.
Passeri, P. (2014). August 2014 cyber attacks statistics. Hackmageddon. September 8 http://hackmageddon.com/2014/09/08/august-2014-cyber-attacks-statistics.
Piquero, A. R. (2008). Taking stock of developmental trajectories of criminal activity over the life course. In *The long view of crime: A synthesis of longitudinal research* (pp. 23–78). New York, NY: Springer.
Piquero, A. R., Farrington, D. P., & Blumstein, A. (2003). The criminal career paradigm. *Crime & Justice, 30*, 359–506.
Piquero, A. R., Farrington, D. P., & Blumstein, A. (2007). *Key issues in criminal career research: New analyses of the cambridge Study in delinquent development*. Cambridge University Press.
Sampson, R. J., & Laub, J. H. (2003). Life-course desisters? Trajectories of crime among delinquent boys followed to age 70. *Criminology, 41*(3), 555–592.
Smith, R. G., Grabosky, P., & Urbas, G. (2004). *Cyber criminals on trial*. Cambridge University Press.
Steinmetz, K. F. (2016). *Hacked: A radical approach to hacker culture and crime*. NYU Press.
Taylor, P. A. (1999). *Hackers: Crime in the digital sublime*. London: Routledge.
Van Koppen, M. V., Blokland, A., Van Der Geest, V., Bijleveld, C., & van de Weijer, S. (2014). *Late-blooming offending. Oxford handbook online criminology*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199935383.013
Van Onna, J. H., Van Der Geest, V. R., Huisman, W., & Denkers, A. J. (2014). Criminal trajectories of white-collar offenders. *Journal of Research in Crime and Delinquency, 51*(6), 759–784.
Woo, H. J., Kim, Y., & Dominick, J. (2004). Hackers: Militants or merry pranksters? A content analysis of defaced web pages. *Media Psychology, 6*(1), 63–82.
Yar, M. (2005). The novelty of 'cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407–427.
Zone-H. (2018). News. http://www.zone-h.org/news/id/4737.

Steve G.A. van de Weijer is Senior Researcher at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), Amsterdam, the Netherlands. His research focuses on life-course criminology, cybercrime, intergenerational transmission of crime, and genetic influences on criminal behaviour.

Thomas J. Holt is a Professor and Director of the School of Criminal Justice at Michigan State University. His research focuses on cybercrime and cyberterrorism, with an emphasis on computer hacking, malware, and data breaches. Dr. Holt's work has appeared in myriad outlets, including British Journal of Criminology, Criminal Justice and Behavior, and Terrorism & Political Violence.

E. Rutger Leukfeldt is Senior Researcher at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) and Academic Director of Centre of Expertise Cybersecurity of the Hague University of Applied Sciences. His work focusses on the human factor in cybercrime and cybersecurity. Rutger is currently the chair of the Cybercrime Working Group of the European Society of Criminology (ESC).