Computers in Human Behavior 126 (2022) 106984

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Repeat victimization by website defacement: An empirical test of premises from an environmental criminology perspective

Asier Moneva [a,b,c,1,*], E. Rutger Leukfeldt [a,b], Steve G.A. Van De Weijer [a], Fernando Miró-Llinares [c]

[a] Netherlands Institute for the Study of Crime and Law Enforcement, Postbus 71304, 1008 BH, Amsterdam, the Netherlands
[b] Center of Expertise Cyber Security, The Hague University of Applied Sciences, Postbus 13336, 2501 EH, The Hague, the Netherlands
[c] Crímina Center for the Study and Prevention of Crime, Miguel Hernandez University, Avda. de la Universidad, Hélike Building, 03201, Elche, Spain

ARTICLE INFO

Keywords:
Cybercrime
Environmental criminology
Hacking
Repeat victimization
Website defacement
Zone-H

ABSTRACT

Repeat victimization has been widely studied from the perspective of environmental criminology for several decades. During this period, criminologists have identified a set of repeat victimization premises that are observed for many crimes; however, it is unknown whether these premises are also valid for cybercrime. In this study we rely on more than 9 million Zone-H data records from 2010 to 2017 to test whether these premises apply for the cybercrime of website defacement. We show that the phenomenon of repeat victimization is also observed in defaced cyber places (i.e. websites). In particular, we found that repeats contributed little to crime rates, that repeats occurred even several years after the original incident, that they were committed disproportionately by prolific offenders, and that few offenders returned to victimize previous targets. The results suggest that some traditional premises of repeat victimization may also be valid for understanding cybercrime events such as website defacement, implying that environmental criminology theories also constitute a useful framework for cybercrime analysis. The implications of these results in terms of criminological theory, cybercrime prevention, and the limitations derived from the use of Zone-H data are discussed.

1. Introduction

Our society is increasingly digitized and so is crime. For the past three decades, technological breakthroughs have created new opportunities to commit crimes in digital environments such as the Internet. Sometimes these crimes resemble traditional crimes (i.e. cyber-enabled crimes), but on other occasions they appear as criminal phenomena unparalleled in physical space (i.e. cyber-dependent crimes) (e.g. McGuire & Dowling, 2013). Although cybercrimes have become a regular occurrence, we still know relatively little about them: Why do they occur? How can they be prevented or mitigated? To address these questions, a growing body of research on the human factor of cybercrime has contributed to expanding our knowledge about victims, offenders, cybercrime control, and the role of criminological theory in these three areas (Holt & Bossler, 2014; Leukfeldt, 2017; Leukfeldt & Holt, 2020; Maimon & Louderback, 2019). With regard to criminological theories, it is particularly important to examine whether traditional theories remain useful in explaining cybercrime (Bossler, 2020; Holt & Bossler, 2017; Miró-Llinares & Moneva, 2019). In this sense, this article contributes to the existing literature by empirically assessing the applicability of four repeat victimization premises to better understand cybercrime as an event.

Crime events have a certain baseline risk of occurring, but research has shown that for some property crimes such as burglary, vandalism, and graffiti, this risk increases after the initial occurrence (Farrell, 2005). Sometimes this increase in risk manifests when a specific crime impacts a target more than once, meaning the target suffers repeat victimization. Established research suggests that repeat victimization typically occurs within a short interval after the first victimization (Bowers & Johnson, 2005; Farrell, 2005; Farrell & Pease, 1993; Johnson, Bowers, & Hirschfield, 1997; Johnson & Bowers, 2004b; Pease, 1998), that it has a large impact on crime rates (Farrell & Pease, 2017, 2018; Pease, 1998; Weisel, 2005), and that it is committed by a few prolific offenders (Bernasco, 2008; Farrell, 2005; Farrell & Pease, 1993,

* Corresponding author. Netherlands Institute for the Study of Crime and Law Enforcement, Postbus 71304, 1008 BH, Amsterdam, the Netherlands.
E-mail addresses: amoneva@nscr.nl (A. Moneva), rleukfeldt@nscr.nl (E.R. Leukfeldt), svandeweijer@nscr.nl (S.G.A. Van De Weijer), f.miro@crimina.es (F. Miró-Llinares).
[1] Present address: Netherlands Institute for the Study of Crime and Law Enforcement. Postal address: Postbus 71304, 1008 BH Amsterdam (The Netherlands).

https://doi.org/10.1016/j.chb.2021.106984
Received 11 September 2020; Received in revised form 5 July 2021; Accepted 15 August 2021
Available online 18 August 2021

2017; Lammers, Menting, Ruiter, & Bernasco, 2015; Pease, 1998). Repeat victimization has mainly been studied regarding property crimes such as residential or commercial burglaries, theft from motor vehicles, vehicle theft, robbery, personal larceny, shoplifting, and car vandalism (Bowers, 2001; Bowers & Johnson, 2005; Farrell, 2005; Farrell, Tseloni, & Pease, 2005; Johnson, 2008; Johnson, Summers, & Pease, 2009) .[2] The consistency of the findings on repeat victimization for different types of crime over more than two decades allows their transformation into verifiable premises that can be tested for other crimes. The present study explores whether the traditional premises on repeat victimization also apply to a specific type of cyber-dependent crime: website defacements.

Website defacement is a cyber-dependent crime that involves trespassing on a website to alter its contents (see Maimon & Louderback, 2019 for a review of the current state of research on cyber-dependent crime). "Defacements enable hackers to post messages and images that indicate their perspectives and beliefs, as well as gain status by listing their name and group affiliation" (Holt, 2011, p. 171). When this crime is committed with political motives, it is encompassed within the phenomenon of hacktivism (Romagna, 2019), but there is a wide variety of motives and modus operandi behind defacements, which means it acquires a phenomenological dimension of its own (Holt, Lee, et al., 2020; Madarie, 2017; Romagna & Van den Hout, 2017). For example, some hackers seek recognition after successfully trespassing web servers; the more domains they attack and the greater the difficulty, the more they can flaunt their skills. Recognition seeking is most prominent among defacers, some of whom even leave their contact details embedded in their defacement (Holt, Leukfeldt, & Van De Weijer, 2020). Others might seek revenge, express their ideological alignment, or simply bolster their ego (Holt, Lee, et al., 2020). Either way, the benefit of recognition is a cornerstone for gaining status in the hacker community (Holt, 2019), which can lead to certain individuals or groups being especially prolific or certain domains being disproportionately victimized.

Website defacements can also have direct and indirect economic consequences for both individuals and organizations. Not only must administrators devote resources to restoring the functionality of their websites after an attack to minimize the economic loss from its impact on productivity or services offered, but they must also try to mitigate the associated reputational damage—which can be serious and long-lasting (see Holt, Lee, et al., 2020).

But how can defacements be studied from the quantitative perspective required by repeat victimization studies when there are no official sources of data nor longitudinal panel studies on this type of crime? One of the few alternatives is to rely on secondary data such as Zone H, a database containing millions of self-reported defacement cases. This data has been used for researching defacements in the past and continues to be used with this aim today (Davanzo, Medvet, & Bartoli, 2011; Howell, Burruss, Maimon, & Sahani, 2019; Maimon, Fukuda, Hinton, Babko-Malaya, & Cathey, 2017; Romagna & Van den Hout, 2017; Woo, Kim, & Dominick, 2004). Previous quantitative studies on defacements can be divided into two categories: those that rely on the human factor perspective to understand the phenomenon, and those that apply a computational perspective for its prevention and mitigation. The former category of studies, which is scarcer than the latter, tend to approach the issue from a descriptive perspective—with the exception of some recent studies using more complex methodologies—and from a certain theoretical foundation (Holt, Leukfeldt, & Van De Weijer, 2020; Howell et al., 2019; Romagna & Van den Hout, 2017; van de Weijer, Holt, & Leukfeldt, 2021). The latter are usually brief or preliminary works with an eminently technical component (e.g. Davanzo et al., 2011; Maimon et al., 2017). This paper aims to contribute to criminological literature by bridging the gap between the two groups as it introduces a hitherto unexplored theoretical framework for defacements with a preventive purpose.

The following section presents the theoretical framework for this study, founded on the applicability of environmental criminology theories, and particularly the repeat victimization mechanisms, to crimes committed in cyberspace. Next, the objectives of the study are presented together with the traditional repeat victimization premises and their reformulation to be specifically explored for defacements. The methods section presents the data, as well as the measures used in the analysis. The results are then discussed in the context of the repeat victimization premises along with the preventive implications of the work. The paper concludes with the key insights drawn from the study.

2. Environmental criminology as a theoretical framework for cybercrime

For decades, the environmental criminology theories have served to understand the situational aspects of crime events and propose strategies for their prevention (Bruinsma & Johnson, 2018; Wortley & Townsley, 2017). There are three main environmental criminology theories: The routine activity approach, whose most popular premise is that crime occurs at the micro level in the absence of capable guardians when a motivated offender and a suitable target converge in space and time (Cohen & Felson, 1979); the geometry of crime, which postulates that the distribution of crime events is not random, but occurs in places where the activity spaces of offenders and targets intersect (Brantingham & Brantingham, 1981); and the rational choice perspective, which states that the offenders' decision to commit a crime reflects a weighting of costs and benefits (Cornish & Clarke, 1986). An important advantage of these mid-range theoretical bodies over grand theories is their simple formulation, which has resulted in analytical frameworks that contribute to a better understanding of crime, such as the crime triangle (Eck, 1994) or the repeat victimization premises (e.g. Farrell & Pease, 2018; Pease, 1998). The application of these frameworks has always been heavily influenced by the geography of crime, but their potential scope has yet to be discovered for crimes committed in cyberspace.

The pre-digital context in which the environmental criminology theories were conceived meant their development was essentially geographical, as little was known about cybercrime at that time. The increase of cybercrime as a problem has caused some scholars who previously focused on geographic crime to pay more attention to crime in cyberspace. This shift in focus has served to theoretically develop the frameworks of environmental criminology theories into cybercrime (Miró-Llinares & Johnson, 2018; Miró-Llinares & Moneva, 2019; Moneva, 2020). In this context, whereas some consider that the structural characteristics of cyberspace—the contraction of time and space—complicate the application of environmental theories (e.g. Yar, 2005), others consider that they simply need to be adapted to the particularities of the environment (e.g. Miró-Llinares & Moneva, 2019).

Since then, dozens of empirical studies have been conducted on the application of environmental theories to understand the dynamics of different forms of cybercrime (for a review, see Leukfeldt & Yar, 2016; see also Bossler, 2020). The rational choice perspective was also applied to cybercrime when Newman and Clarke (2003) turned the focus of their analysis to e-commerce crimes. Subsequently, situational crime prevention strategies have been applied to different contexts such as those defined by stolen data markets (Hutchings & Holt, 2017), or financial cybercrimes (Leukfeldt & Jansen, 2020), among many others (e.g. Hinduja & Kooi, 2013; Reyns, 2010). Overall, both the routine activity approach and the rational choice perspective have received attention from academics in the last decade and have consequently evolved and contributed to the development of the discipline.

But when it comes to the geometry of crime, there are but few studies that apply this theory to cybercrime prevention (see Miró-Llinares,

[2] In addition to research that has focused on property crime, the phenomenon of repeat victimization has also been observed in interpersonal crimes such as rape, sexual assault, or violent assault (e.g. Nazaretian & Merolla, 2013; Planty & Strom, 2007; Turanovic, Pratt, & Piquero, 2018).

Moneva, & Esteve, 2018; Williams & Burnap, 2016). This is probably because this theory depends to a great extent on the concept of place, which is usually associated with a physical space. However, it has been argued that cyber places can be understood as digital spaces of convergence where offenders also interact with the environment that defines crime opportunities (Leukfeldt, Kleemans, & Stol, 2017a–c; Miró-Llinares & Johnson, 2018). This reasoning shows that not all concepts within environmental criminology are geographical, as some are merely spatial, like hot spots (Miró-Llinares and Moneva, 2019). Crime hot spots, which are the result of the repeated occurrence of crime events in a given place and over a certain period of time, have traditionally been measured in physical space, but such concentrations can also be observed in crimes occurring in cyberspace. For example, there may be certain web domains that are more prone to victimization by defacement than others and there may be certain time frames in which the activity of defacers is more intense. In this case, spatiotemporal hot spots of cybercrime will be formed in those cyber places or domains that are repeatedly defaced. What is unknown to date is whether the theory behind repeat victimization is also applicable in cyberspace.

3. From repeat victimization patterns in physical places to cyber places

So, why does repeat victimization occur? At least three non-mutually exclusive mechanisms inspired by the geometry of crime can be found to explain repeat victimization patterns: The boost and the flag explanations (Chainey, 2012; Johnson, 2008; Johnson et al., 2009), and random concentrations (Park & Eck, 2013). The boost explanation suggests that an offender's previously successful experience with a target brands it as suitable for future offenses (Johnson & Bowers, 2004a; Johnson et al., 2009; Pease, 1998). For example, when an offender successfully burglarizes a house, it is labelled as suitable in cost-benefit terms and, therefore, it is likely that the same offender returns to victimize the same place again. The flag explanation suggests that there are a number of stationary characteristics in the target that constantly label it as vulnerable in the eyes of potential offenders (Johnson, 2008; Pease, 1998). For example, when a burglar enters a house, it is because that place meets a series of conditions that allow considerable time to be devoted to the task without being detected. It is therefore likely that the same or another offender will return to the same house to burglarize it again since the characteristics of the place that generated crime opportunities in the first place remain stable over time. A third explanation exists outside the analytical framework in which the previous ones are embedded: repeated victimization can also occur by chance (Park & Eck, 2013). Following this assumption, unfortunate repeats would eventually occur in certain individuals and places even if all had a homogeneous risk of victimization. As in physical spaces, targets and places in cyberspace may also 'boost' offenders, be 'flagged' as vulnerable, or simply have the misfortune to suffer repeated victimization. But it is also possible that these mechanisms work differently because of the particular spatiotemporal dimensions of cyberspace that change crime opportunities.

Criminological research has compared the cyber and traditional dimensions of targets and places. Although recent research has shown that cyber offenders and traditional offenders share important similarities in situational and personal crime correlates (Weulen Kranenbarg et al., 2019), and in both the life events (Weulen Kranenbarg et al., 2018) and social ties that impact their criminal careers (Leukfeldt, Kleemans, & Stol, 2017a–c; Leukfeldt, 2014), there may be differences between physical and cyber places that affect crime opportunities. Unlike physical space, distances in cyberspace are non-existent, at least when measured in spatial terms (Miró-Llinares, 2011; Yar, 2005). The cost-benefit balance is then tilted towards profit, since the effort required for an offender to move from one place to another is practically zero. Places are now a click away, and the new measure for the effort required for travel is only the time it takes. In summary, it appears that while the offenders share some similarities, the environments have changed.

These different environments affect the decision-making process of offenders when visiting places and choosing targets. In cybercrimes such as hacking or malware infection, an offender may visit websites designed with a popular Content Management System (e.g. WordPress) to exploit known vulnerabilities, or cyber places such as download sites to find suitable targets, respectively. Note that because each criminal event is different, crime opportunities are unique to each case. In the case of website defacements, for instance, a motivated offender can target a specific website to deface it, or rather to launch mass attacks, in which many websites are targeted simultaneously by a botnet that takes advantage of server vulnerabilities. In the first case, the defacer may give up if the task is too arduous or persevere until the attack is complete. In this scenario the offender already has a fixed target beforehand and criminal opportunities will probably have little effect. What will have the greatest effect will be the effectiveness of the security systems that can act as guardians and harden the target. On the contrary, crime opportunities will play an essential role in the case of mass attacks, since it is precisely the absence of guardianship that makes a target vulnerable and enables the attack. In the first case the repeated selection of targets will depend on a motivated decision making process by the offender (see Cornish & Clarke, 1986), and in the second case it will be the result of the convergence between offender and target in the absence of a guardian (see Cohen & Felson, 1979). Therefore, repeat victimization would not occur at random, but rather follow patterns that can be observed and whose analysis facilitates its prevention (see Brantingham & Brantingham, 1981).

Spatiotemporal crime concentration is one of the most studied phenomena within the Criminology of Place, and whose evidence is robust to the extent that it has been enunciated as a scientific law (Weisburd, 2015)—and corroborated afterwards (Levin, Rosenfeld, & Deckard, 2017). Crime is concentrated not only in places, but also in people (Fagan & Mazerolle, 2011; Fox & Tracy, 1988; Wood & Papachristos, 2019). And the analysis of these crime patterns allows allocated resources to bolster their prevention through strategies such as hot spot policing (e.g. Braga, Turchan, Papachristos, & Hureau, 2019) or focused deterrence (e.g. Braga, Zimmerman, et al., 2019; Kennedy, 2012). Crimes committed in cyberspace are also concentrated in space and time and follow observable patterns. For example, at the macro level, patterns in spam and phishing rates have been observed in a sample of countries (Kigerl, 2012); at the meso level, patterns of time have been found in repeated network attacks on computer systems (Moitra & Konda, 2004) or packet transmission in DDoS attacks (Thapngam, Yu, Zhou, & Beliakov, 2011); and at the micro level, patterns have also been observed in the situational contexts in which repeated online harassment occurs (Moneva, Miró-Llinares, & Hart, 2020), and in metadata in Twitter messages that contain hate speech (Miró-Llinares et al., 2018) and that help identify social bots (Ferrara, Wang, Varol, Flammini, & Galstyan, 2016). There are enough reasons to assume that defacements, like other cybercrimes, also concentrate in space and time and follow observable patterns. Identifying these patterns will allow preventive resources to be deployed in the future to mitigate or reduce the impact of defacements.

4. The present study

In this paper, we aim to empirically test whether the fundamental premises of repeat victimization that apply to some crimes committed in physical space (e.g. burglary, vandalism) are also observed for defacements in cyberspace. For this purpose, the four main premises of repeat victimization have been selected and reformulated for the cybercrime of website defacement.

The first premise states that "high crime rates and hot spots are as they are substantially because of rates of repeat victimization" (Pease, 1998, p. v; see also Farrell & Pease, 2017, 2018). In his original work,

Pease (1998) uses the word "substantial" to refer to the fact that repeat victimization accounts for 68% of the total incidents on which the property crime rate is calculated. In a review of 2007 and 2014 studies, Farrell and Pease (2017) find a similar proportion of repeats for personal larceny (58.3%) and robbery (63.9%), but the authors indicate that the real figures are even bigger because they use survey data and surveys under-estimate repeats. Estimates from the British Crime Survey indicate that 30% of vandalism incidents affect repeat victims (see Weisel, 2005), a figure close to the 16-country average of 27.3% for car vandalism repeats reported in the International Crime Victimization Survey (Farrell et al., 2005). Thus, by adopting a very conservative definition, we can define "substantial part of all defacements" as 50%, and to analyze the variation in crime we can examine their distribution over time. In this paper, we test whether *a substantial share of all defacements and variation in defacements is due to repeat victimization.*

The second premise states that "when victimization recurs it tends to do so quickly" (Pease, 1998; see also; Bowers & Johnson, 2005; Farrell, 2005; Farrell & Pease, 1993; Johnson et al., 1997; Johnson & Bowers, 2004b). Normally, an interval of one year is used to assess repeat victimization (e.g. Chainey, 2012; Farrell & Pease, 1993, 2017). Thus, to determine whether repeat victimization occurs shortly after an initial event, it is necessary to calculate how many domains were defaced more than once within a one-year period. By adapting this premise to website defacements, we test whether *a repeat incident occurs shortly after a first defacement event.*

The third premise states that "repeated crimes are disproportionately the work of prolific offenders" (Pease, 1998, p. vi; see also; Farrell & Pease, 2017). In criminology, this type of Pareto Principle has been studied for both offending and victimization through the analysis of repeat events (Fagan & Mazerolle, 2011; Farrell & Pease, 2017; Pease, 1998), showing that a few victims suffer most crimes, and that a few offenders commit most crimes.[3] So we expect to find similar results for website defacements. However, since it can be argued that the type of repeat defacement (i.e. mass or single) can influence the relationship between the number of offenders and the percentage of defacements for which they are responsible, such a distinction should be examined. The reason would be that a single offender could direct mass defacements to many domains, a considerable difference with respect to single defacements—independent events that could only be directed against one domain at a time. Additionally, total repeat victimization figures could be biased by mass attacks directed to different extensions of the same domain, which would be registered as repeats according to our methodology. In this sense, we test whether the two types of *repeat defacements are disproportionately the work of prolific defacers.*

The fourth premise states that "a major reason for repetition is that offenders take later advantage of opportunities which the first offense throws up" (Pease, 1998, p. v; see also; Bernasco, 2008; Farrell, 2005; Farrell & Pease, 1993; Lammers et al., 2015). This premise requires examining how often the same domains are victimized by the same defacers. In addition to this analysis, a distinction made according to the motivation of the offenders seems appropriate, since recent research suggests that ideologically-motivated defacers are more likely to engage in repeat attacks (Holt, Lee, et al., 2020). For example, it would seem logical that those offenders who have no apparent motive for defacing a specific website are not obsessed with targeting the same website again. But in the same way, it could be argued that those with a political motivation or, especially, those who execute their attack for revenge should have an interest in repeatedly directing their attack towards specific targets. Therefore, we test whether *a major reason for repeats is that offenders repeatedly target domains they have defaced previously.*

[3] Originally, the Pareto Principle—also known as the 80/20 rule—served to establish that about 80% of the results were due to about 20% of the causes.

5. Materials and methods

5.1. Data

We use data from the Zone-H Defacement Archive (http://www.zone-h.org/), a self-reported data source that the defacers themselves supply with their activity. The Zone-H team collects, validates, stores and maintains information about defacement incidents committed by individuals or groups who record their own defacements under a nickname (for an overview of the database, see Romagna & Van den Hout, 2017). Among other variables, this dataset contains information about the date on which defacers submit a request to register an attack, their nickname, their motivation, the type of attack used for the defacement, the URL of the defaced website, and whether the attack is a redefacement of a previously registered domain. In our dataset, the time period in which the defacement incidents are recorded extends from January 1, 2010 to April 4, 2017. After removing 85 records that had incorrectly registered the URL of the defaced website or the type of attack recorded, the dataset contains 9,117,268 registries representing unique defacements to 8,603,658 domains.

5.2. Measures

5.2.1. Repeat victimization: Repeat defacements

To measure repeat victimization, instead of relying on the redefacement variable in the archive,[4] we used the full URLs of the defaced domains; that is, the protocol, the web domain, the path or extension, and additional parameters. Using the stringr R package, we trimmed the URLs of defaced websites with the following regular expression[5]

```
http : / /|http : / / www\\.|https : //|https : / / www\\.|/[ : graph : ]*
```

This removed all characters except the website domain. Then we subsequently identified, aggregated, and stored unique domains in a new variable. Thus, repeat victimized domains can be defined as those that appear more than once in the data. By our own calculations we found that repeat defacements represented 5.6% of all attacks, ranging from 1 to 7 repeats.

It is important to note that the Zone-H administrators have established a one-year restriction on the registration of incidents in order to prevent domains from being massively revictimized because their vulnerability is publicly displayed on Zone-H's platform (Zone-H, personal communication, November 21, 2019). So, if a defacer wants to register an attack on a revictimized domain, it is not possible until this period has elapsed, which creates a one-year gap between potential repeats. However, it seems that this restriction does not always work, as some isolated incidents have been recorded within this interval.

The authors are aware that both these circumstances have obvious implications for the phenomenon of repeat victimization explored in this paper. However, to the best of the authors' knowledge, Zone-H remains the best public source of data for studying website defacements and it continues to be valuable to explore patterns of repeat victimization.

5.2.2. Defacers' motivation

When recording an attack, defacers must fill out a short form that

[4] According to the data, 10.1% of the records are redefacements. However, while inspecting the distribution of the variables that comprise the dataset, we observed an inconsistency in the values of the redefacement variable. We found that 3301 website domains that appeared more than once in the data (i.e. repeats) were not labelled as redefacements. In addition, we also found 409,183 domains that appeared just once in the data but were labelled as redefacements. This may be due to these domains appearing in previous records that are not part of our dataset.

[5] Regular expressions are sequences of characters that create search patterns in a given field, URLs in our case.

includes a drop-down list of possible reasons that motivated the defacement. Defacers can choose one of the following six categories: (1) "Heh … just for fun!", (2) "as a challenge", (3) "I just want to be the best defacer", (4) "political reasons", (5) "patriotism", and (6) "revenge against that website". Since some of these categories are not exclusive and may overlap, we have proceeded to regroup them into four categories: "Fun" includes the first category; "challenge" includes the next two; "politics" includes the fourth and fifth; and "revenge" remains alone. Defacements performed for fun represent 54.8% of the records, those executed as a challenge account for 23.4%, those perpetrated for political reasons account for 9.4%, and those seeking revenge for 4.1% (see also Holt, Leukfeldt, & Van De Weijer, 2020; van de Weijer, Holt, & Leukfeldt, 2021). The motivation behind the remaining defacements is unknown. Although data aggregation causes some loss of information, we believe that the new categories are better delimited and facilitate the interpretation of the results.

5.2.3. Type of attack: Single and mass defacements

Another variable that describes the nature of defacements is the type of attack involved, which can be "single" or "mass". As opposed to single attacks, mass defacements represent attacks that target several websites in a short interval of time. Single attacks account for 23.6% of defacements, compared to 76.4% for mass attacks.

5.3. Analytic strategy

Repeat victimization has been analyzed in the same consistent manner over the past few decades (Farrell & Pease, 1993, 2017). "The preferred way of analyzing repeat victimization is to establish a set assessment period (usually twelve months), then identify initial victimization of each unique target and determine whether the target was re-victimized in the assessment period following that initial victimization" (Chainey, 2012, p. 1). This strategy, known as the rolling period methodology, is also followed in the present paper with a slight modification. Since Zone-H restricts registrations of defacements of the same website within a one-year period, we were not able to maintain a one-year period to assess whether repeat victimization exists. Thus, the analyses were carried out looking at the whole time series to observe whether there is repeat victimization regardless of the time period, and to understand its complete scope.

In addition, our third premise requires analyzing the extent to which repeat defacements are concentrated among the defacers in our sample. To that end, we used Fox and Tracy's (1988) coefficient to measure skewness in offense distributions.[6] This measure facilitates comparison of the results with those obtained from other studies.

Data transformation, string manipulation, and data visualization were executed using the tidyverse R package version 1.2.1 (Wickham, 2017) in RStudio version 1.2.5001 for the R free software version 3.6.1. Data transformation involved: Reshaping data to change its layout; summarizing, grouping, and manipulating cases to return new values; manipulating variables by extracting them or making new ones; and combining data tables. String manipulation was essential in our analyses as it allowed us to define, by means of regular expressions, a new unit of analysis for repeat victimization: web domains. Regarding data visualization we used a staircase or step chart to visualize the results for the first premise, bar charts to compare the results obtained to explore the second premise, and histograms to show the distribution of repeat victimization for premises three and four. Due to the extremely skewed distribution of the data, for some figures we used a transformed y-axis by means of a $\log_{10}(x)$ to facilitate their visualization. Some charts include annotations.

6. Findings

This first premise requires calculating which share of total recorded defacements corresponds to repeats, as shown in Fig. 1. Because 2010 is the initial year—and there is a one-year gap in repeat victimization—and 2017 only contains data for the first four months, we omitted these two years from the data and found that repeats per year only represented a mean of 7.1% of total defacements ($SD = 3.3$) with a minimum of 2.3% in 2011 and a maximum of 11.1% in 2016.[7] Next, a Pearson correlation test was conducted to assess the relationship between total and repeat counts of defacements using aggregate figures per month. We found a very weak non-significant relationship between the two figures ($r(70) = 0.072$, $p = 0.545$) showing that the contribution of repeat defacements to the annual variation in the crime rate was minimal. For the same Figure with an unmodified y-axis see Appendix A (Figure A. 1).

To test the second premise following the rolling period methodology, repeat victimization sequences were identified and a number was assigned based on their order (i.e. 1st victimization, 2nd victimization, etc.). Next, the distribution of repeats was analyzed to calculate the amount of time between the intervals (Table 1). This revealed that the mean (weighted) time interval between repeat victimizations was 670.4 days. Although the mean duration between the first defacement and the first repeat victimization was almost 690 days, this figure decreased after each repeat. This seems to be influenced by those defacements that were recorded on the same day as the original victimization causing a reduction in the mean value. Considering the highly skewed distribution of the repeats, it is worthwhile to highlight the figures corresponding to the first quartile, which are consistently around a year in every interval after the first repeat victimization.

Fig. 2 serves to illustrate that these patterns were still visible even after several years, although with each victimization that occurred the number of repeats was lower. Note that Fig. 2 displays a modified y-axis to visualize this otherwise unnoticeable pattern. For the same Figure with an unmodified y-axis see Appendix B (Figure B. 1).

There were 66,648 defacers responsible for 9,117,268 defacements. Of these, 30,935 (46.4%) defacers only executed one attack, suggesting that clustering exists. However, while most defacers performed few attacks, others launched many ($Min = 1$; $Q1 = 1$; $Mdn = 2$; $3Q = 9$; $Max = 303{,}442$; $M = 136.8$; $SD = 2764.7$). And there were others who concentrated their attacks on the same website domains; specifically, 17,026 defacers did so, committing 513,610 repeats. To test our third premise, we analyzed what percentage of these repeats were carried out by a particular percentage of offenders.

The results in Fig. 3 show that 1% of redefacers committed 57.8% of repeat defacements, and that 50% of redefacers committed 98.2% of repeat defacements. Fox and Tracy's (1988) measure for skewness shows a very high concentration of repeat defacements among defacers ($\alpha = 0.906$). The same distribution was also examined according to the type of attack, whether single or mass. As illustrated in Fig. 3, this distinction shows that single attacks ($\alpha = 0.881$) were slightly more concentrated per offender than mass attacks ($\alpha = 0.877$). Regardless of the type of attack, 1% of redefacers were responsible for more than 46% of repeat defacements, and 50% of redefacers for more than 96% of repeat defacements. A detailed data table can be found in Appendix C (Table C. 1).

After grouping all defacements by offender, the analysis shows that offenders rarely defaced the same domains that they had previously defaced; in fact, this only occurred 0.3% of the time (Table 2). When

[6] By formula, $\alpha = 2\sum Pn_k\left(\frac{Po_k}{2} + cPo_{k+1}\right) - 1$, where Pn_k is the proportionate size of our sample of defacers with exactly k offenses; Po_k is the proportion of defacements executed by defacers with exactly k defacements, and cPo_{k+1} is the proportion of the defacements executed by defacers with at least $k+1$ offenses.

[7] We repeated the analysis including all data points and obtained a slightly lower proportion of repeats of 6.3% ($SD = 3.7$), with a minimum of 0.2% in 2010, and a maximum of 11.1% in 2016.

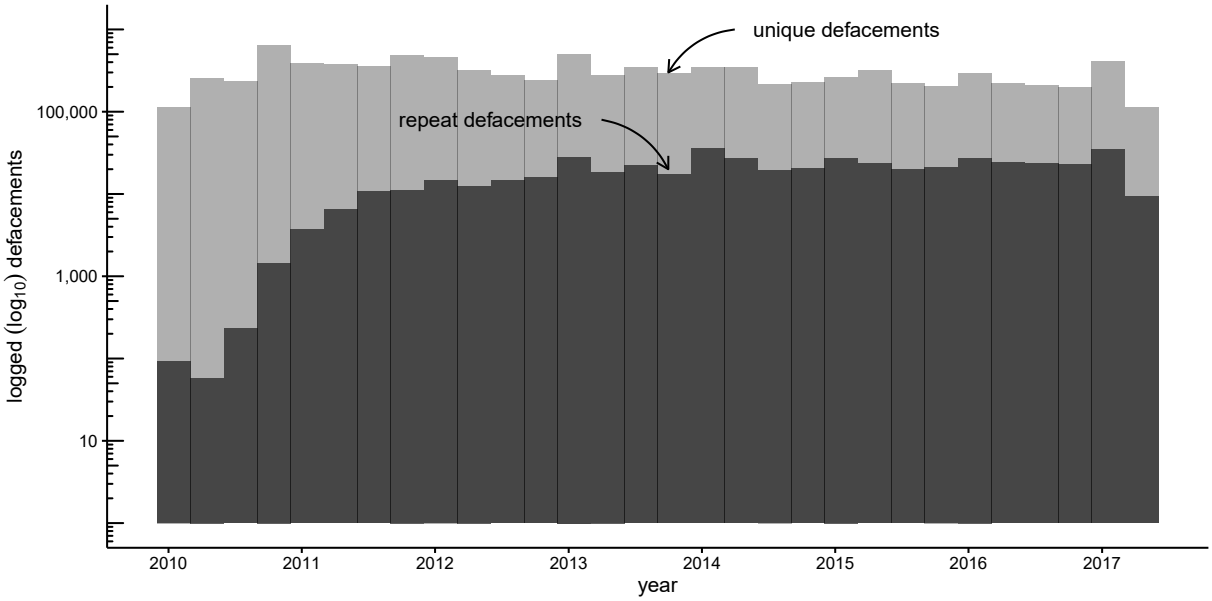

Fig. 1. Distribution of repeat defacements to total defacements. The Figure displays a transformed y-axis by means of $\log_{10}(x)$. Histogram bins = 30.

Table 1
Time lapse between repeat victimization intervals.

Repeat victimization interval	Repeats per interval		Time in days between repeats						
	n	%	Min	1Q	Mdn	3Q	Max	M	SD
First	450,278	4.9	0.0	402.8	527.2	832.3	2638.4	689.6	408.0
Second	52,336	0.6	0.0	373.3	426.6	617.1	2347.2	548.9	275.1
Third	9054	0.1	0.0	369.0	390.2	493.2	1737.9	472.2	185.9
Fourth	1696	0.0	0.0	366.7	371.8	413.1	2283.7	421.5	127.8
Fifth	218	0.0	0.0	366.4	372.4	398.7	914.7	410.4	102.7
Sixth	26	0.0	0.0	366.2	366.2	378.5	459.3	364.7	78.2
Seventh	2	0.0	0.0	–	–	–	366.2	183.1	258.9

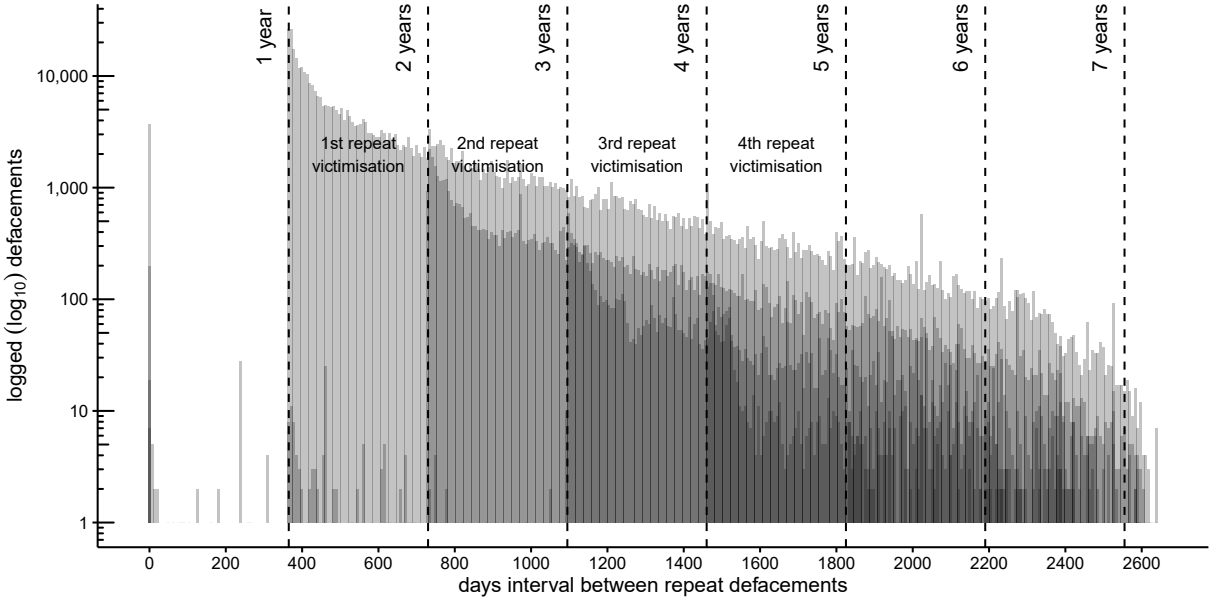

Fig. 2. Repeat victimization time pattern for website defacements. The Figure displays a transformed y-axis by means of $\log_{10}(x)$. Histogram binwidth = 7.

repeats are distinguished according to the motivation of the offenders, the results show that most of the defacers who did it, did so for fun. Interestingly, revenge-driven defacers committed the least repeat attacks against the same website.

To test the fourth premise, we analyzed whether the number of times the same offenders attacked the same domains was a major reason for

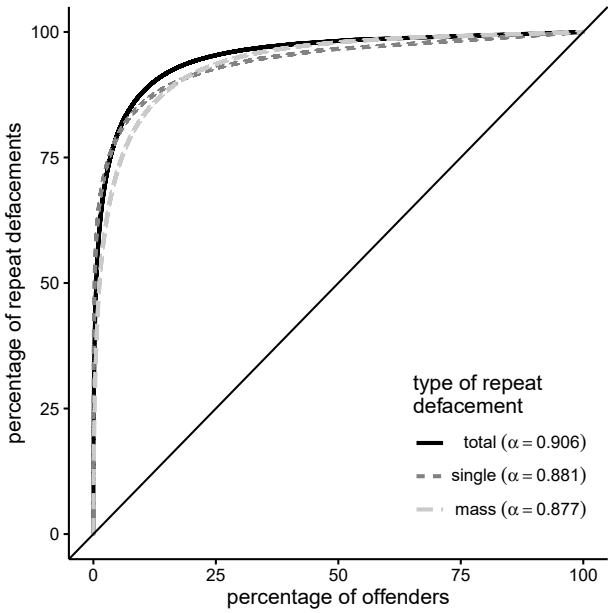

Fig. 3. Percentage of offenders responsible for a percentage of defacements.

repeat victimization. This can be calculated as follows:

$$\frac{n \text{ repeats by the same offender to the same domain}}{n \text{ total repeats}} = \frac{31,841}{513,610}$$

The results show that 6.2% of repeat victimization was due to the same offenders defacing the same domains repeatedly.

7. Discussion

In line with criminological research that has explored the utility of environmental criminology theories to understand cybercrime (Bossler, 2020; Holt & Bossler, 2017; Miró-Llinares & Moneva, 2019), this paper draws on a unique database containing millions of self-reported cases to test whether the main premises of repeat victimization of traditional crimes also apply to website defacements. After noting that the phenomenon of repeat victimization was also observed for this particular cybercrime, we examined: Whether it constituted a substantial fraction of crime rates and their variation over time, whether it occurred shortly after the first incident, whether a few defacers were responsible for most repeats, and whether this was largely due to the same offenders defacing the same domain over again. The results suggest that some of the traditional premises of repeat victimization could also be valid in the case of website defacements.

Firstly, we observed that, despite the fact that Zone-H does not register defacements on the same domain within one-year after the first defacement, the contribution of repeat events to the total website defacement rate was still relevant. However, the volume it represented is minimal compared to that observed for traditional property crimes. While repeats represented 63.9% of robberies, 58.3% of personal larceny (Farrell & Pease, 2017), 30% of vandalism incidents (Weisel, 2005), and an average of 27.3% of car vandalism (Farrell et al., 2005), repeat defacements represented a mean of 7.1% between 2011 and 2016 in our data. The most likely explanation for this large discrepancy is that repeat victimization patterns observed in Zone-H are limited by the one-year time interval after the original incident for a phenomenon that is essentially characterized by being temporarily concentrated shortly after the first event (Bowers & Johnson, 2005; Farrell, 2005; Farrell & Pease, 1993; Johnson & Bowers, 2004b; Johnson et al., 1997; Pease, 1998). However, another explanation could be that repeated attacks are mitigated by the rapid adoption of preventive measures by website owners—a measure that cannot be implemented in physical space as easily. Thus, while it is likely that the results are highly underestimating the share of repeats, this premise is not supported by the Zone-H data.

Secondly, we observed that some website domains registered in Zone-H suffered between 1 and 7 repeats after the initial defacement, but the prevalence decreased exponentially after each repetition. Our results also indicate that some repeat events were still recorded within the one-year restricted registration period, suggesting that this measure established by Zone-H has some flaws. Because of the large data set used in this study, it was possible to detect patterns of repeat victimization that might have gone unnoticed with less data. In this sense, even though we cannot determine whether repeat victimization occurs shortly after the first incident due to the one-year period established as a restriction to record repeat attacks, the highly skewed distribution of the data, with a number of redefacements shortly after the end of the one-year restriction, suggests that a large volume of defacements would be observed in that initial period if there were no such restriction. This claim is reinforced by the results of a study on network attacks on computer systems, in which researchers found that repeat victimization was most likely to occur within the first week after a previous attack (Moitra & Konda, 2004). Hence, crime prevention measures such as cyber-attack detection systems should be specifically intensified immediately after the first victimization so that they can have an effect on the peak hours, when most events occur. Prevention efforts could also benefit from enforcing guardianship by incorporating place managers such as SSL security certificates and ensuring they do not expire to prevent man-in-the-middle attacks.

Thirdly, while research on traditional crime shows that most offenses are committed by few offenders, repeat cyber offenders seem to be more prolific (van de Weijer, Holt, & Leukfeldt, 2021). This phenomenon was observed when exploring the third premise and represents an exacerbation of the Pareto Principle identified in previous criminological studies. For example, a cross-national comparative study in London and Stockholm showed that about half of the offenses were committed by 2% of the offenders (Farrington & Wikstrom, 1994), and using data from the Philadelphia birth cohort, researchers found that 6% of young males in the sample accounted for 52% of arrests (Fox & Tracy, 1988). In this particular study, Fox and Tracy show that the concentration of offenses was considerably high in the cohorts of 1945 (α = 0.816) and 1958 (α =

Table 2
Frequency with which a domain has been victimized by the same offender and its motivation.

Number of times victimized by the same offender	Any motivation		For fun		As a challenge		Political reasons		For revenge	
	n	%	n	%	N	%	n	%	n	%
1	9,052,741	99.7	4,958,735	99.6	2,124,096	99.8	851,171	99.8	367,475	99.9
2	31,036	0.3	17,786	0.4	3537	0.2	1477	0.2	369	0.1
3	775	0.0	341	0.0	58	0.0	23	0.0	4	0.0
4	23	0.0	13	0.0	4	0.0	2	0.0	0	0.0
5 +	7	0.0	3	0.0	4	0.0	0	0.0	0	0.0

Note: Total defacements by any motivation $= \sum_{i=m}^{n} i^{*}a = 9,117,268$; where i = number of times victimized, and a = frequency of victimization. Total defacements in the dataset is greater than total motivations due to a small number of defacements being of unknown motivation.

0.838). Compared to the alpha coefficients described by Fox and Tracy (1988), the concentration of repeat offenses among defacers was even higher, both in absolute terms ($\alpha = 0.906$) and for each type of defacement (single, $\alpha = 0.881$; mass, $\alpha = 0.877$).[8] Our results show that 1% of offenders accounted for over 57% of the repeat offenses. Moreover, when the repeat event was a single attack, these figures were further accentuated, as 1% of defacers were responsible for 64% of repeats.

Note that instead of analyzing which percentage of offenders commits which percentage of crimes, in our study we examined how repeated attacks were concentrated as a function of the percentage of defacers. Looking at these figures, it is likely that defacements will be even more concentrated if we consider all victimizations rather than just repeats. It should also be noted that defacers registered in Zone-H may not exclusively be individual offenders, but groups of offenders jointly registering their attacks. Conversely, hackers may change their identity by registering a new attack using an alternative nickname. In any case, the concentration figures would probably vary. Considering all possible scenarios, it is safe to claim that the concentration of crime perpetration among a few prolific offenders is also observed for website defacements Therefore, it is possible that focused deterrence strategies that have served to reduce violent crime in physical space (Braga, Zimmerman, et al., 2019; Kennedy, 2012) can be adapted to the particularities of defacers to be effective in reducing the impact of repeats in this type of cybercrime.

Lastly, our analysis shows that a few offenders returned to deface the same domains even one year after their initial attack, regardless of their motivation. It seems that the benefits obtained by these offenders from the first attack were sufficient to again exploit the opportunities that allowed the previous defacement. This suggests that the theoretical rationale for repeat victimization based on the "boost" could still be valid for website defacements. However, we also found that repeat defacements from the same offenders on the same domains contributed little to the total ratio of repeats (6.2%) compared to burglaries (see Bernasco, 2008; Lammers et al., 2015). So, although a few defacers were responsible for a large part of repeat victimizations, these were not concentrated within the same domains. Instead, because defacements occurred on many different websites, it could be argued that their vulnerabilities are constant and can be exploited by any defacer. In fact, hacking through known vulnerabilities is one of the most prevalent hack modes used to deface websites (Holt, Leukfeldt, & Van De Weijer, 2020; Romagna & Van den Hout, 2017). It would seem, therefore, that the "flag" explanation could explain repeat defacements too. Nevertheless, the one-year gap in the data might be a reason for the low number of observed repeats that were also executed by the same offender. After a year, defacer's motivations may change: the political agenda may be different, feelings of revenge may ease, and new challenges and sources of fun other than website defacement can be found. In such cases, our findings would be under-representing the phenomenon of repeated victimization.

Finally, the adoption of situational crime prevention measures could be a valid option for preventing defacements that has already been explored for other cybercrimes (Hutchings & Holt, 2017; Leukfeldt & Jansen, 2020; Reyns, 2010). These measures would include target hardening techniques such as patches for known vulnerabilities and exploits that would help to prevent SQL injections. Such measures could both discourage the boosted offender and reverse the flagged vulnerability of website domains.

8. Conclusion

In this paper we tested four premises of repeat victimization on website defacements from an environmental criminology perspective. Our results show that repeat victimization contributes little to high crime rates of defacement; that it occurred even several years after the initial attack; that most repeat defacements were also committed by only a few offenders; and that in only a few cases offenders repeatedly targeted those domains that they had successfully defaced in the past. These results suggest that some of the traditional premises of repeat victimization may also apply to this type of cybercrime, thus advancing the discipline in the field of criminological theory. This work also contributes to crime prevention by uncovering distinct spatiotemporal patterns of crime that can be tackled with appropriate resources and strategies.

However, this work also has limitations. Although we used the richest existing data source to study website defacements, Zone-H's one-year data recording restriction policy undermines understanding the full extent of repeated victimization. Yet, even when random repeats were not examined, the more than 9 million website defacements analyzed reveal previously unstudied victimization patterns which are useful to generate both basic knowledge about the phenomenon and applied knowledge for prevention. Another aspect that must be interpreted with caution is the defacers' motivation. It should be noted that Zone-H records motivation categories that are neither mutually exclusive nor exhaustive, and that such measure has not undergone empirical validation.

In order to examine the application of criminological theories to cybercrime, more research is needed that focuses on well-defined premises applied to specific cybercrimes. Since this paper presents an initial assessment of repeat victimization, a possible course of action would be an in-depth examination of the boost and flag explanations. This would contribute to better understand why repeat victimization occurs in cyber places. In order to assess the external validity of our findings, upcoming studies should also seek to replicate the analyses presented here using different sources of data, other types of cybercrime, and more information about the victims and targets involved. Until we understand how causal mechanisms work on a small scale, we will be unable to fully grasp the bigger picture of the most complex theories.

Credit Author Statement

Asier Moneva: Conceptualization, Methodology, Software, Validation, Formal analysis, Data curation, Writing – original draft, Visualization, Funding acquisition. **E. Rutger Leukfeldt:** Conceptualization, Resources, Writing – review & editing, Supervision, Project administration. **Steve G. A. Van De Weijer:** Methodology, Validation, Formal analysis, Resources, Writing – review & editing. **Fernando Miró-Llinares:** Conceptualization, Supervision.

Declarations of interest

None.

[8] An important difference between this study and those of Fox and Tracy (1988), and Farrington and Wikstrom (1994), is that their samples also include non-offenders. So, if 50% of their sample does not commit a crime, then 50% of the offenders would be responsible for 100% of the crime. Since in our study we calculated the concentration in a sample of offenders only, it is possible that our figures are even underestimated in comparison.

[8] An important difference between this study and those of Fox and Tracy (1988), and Farrington and Wikstrom (1994), is that their samples also include non-offenders. So, if 50% of their sample does not commit a crime, then 50% of the offenders would be responsible for 100% of the crime. Since in our study we calculated the concentration in a sample of offenders only, it is possible that our figures are even underestimated in comparison.

Acknowledgements

This work was supported by the Spanish Ministry of Science, Innovation and Universities under Grant FPU16/01671, and under Grant EST18/00043.

We thank Prof. Steven Kemp, University of Girona, for performing the English editing of the manuscript.

Appendices.

A. *Additional information for the first premise*

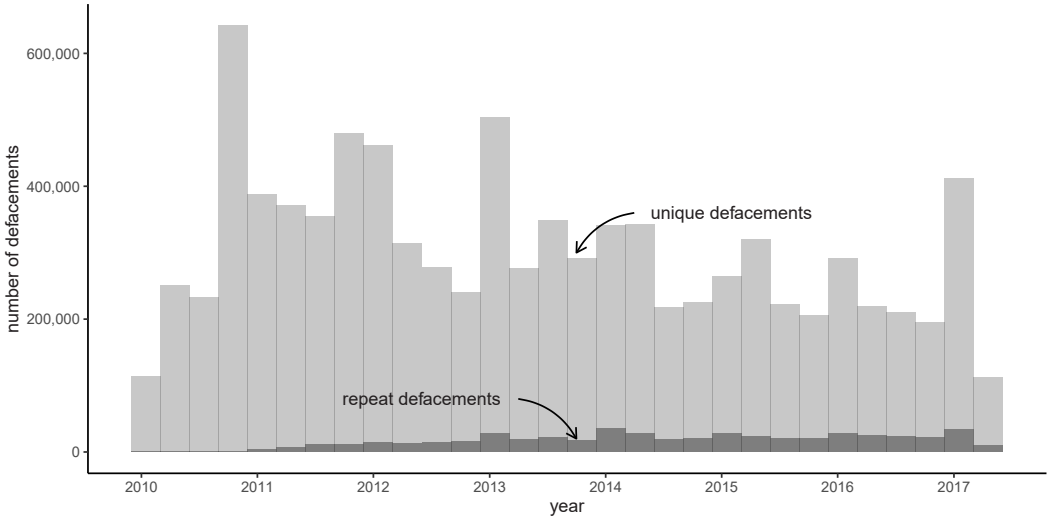

Fig. A. 1. Distribution of repeat defacements to total defacements. Histogram bins = 30

B. *Additional information for the second premise*

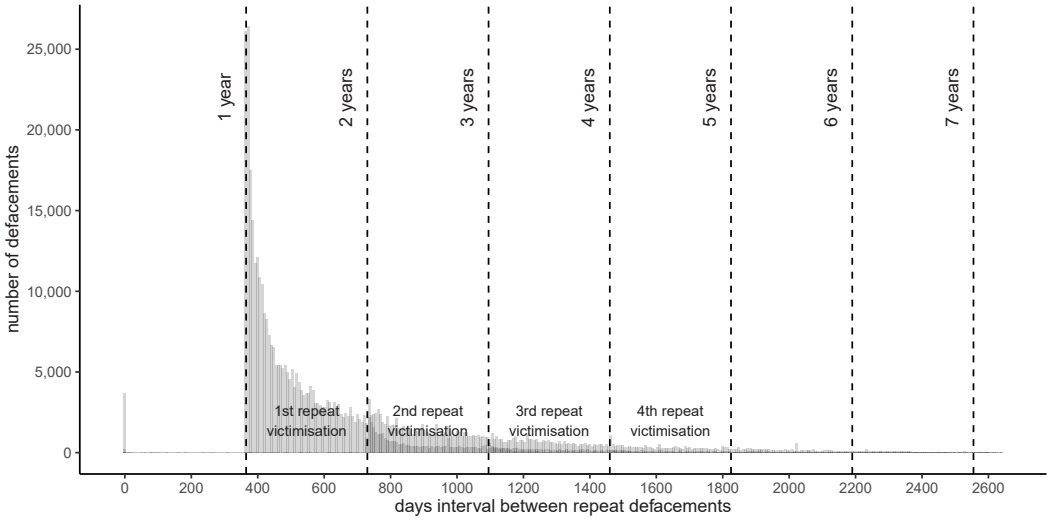

Fig. B. 1. Repeat victimization time pattern for website defacements. Histogram binwidth = 7

C. Additional information for the third premise

Table C. 1
Percentage of offenders responsible for each type of defacement

Percentage of offenders	Repeat defacements					
	Total		Single		Mass	
	n	%	n	%	n	%
1	297,062	57.8	126,920	64.0	145,436	46.1
2	346,187	67.4	139,796	70.5	181,728	57.6
5	410,351	79.9	157,399	79.3	228,863	72.6
10	451,778	88.0	170,115	85.8	261,788	83.0
50	504,461	98.2	191,683	96.6	308,770	97.9
100	513,610	100.0	198,365	100.0	315,245	100.0

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.chb.2021.106984.

References

Bernasco, W. (2008). Them again?: Same-offender involvement in repeat and near repeat burglaries. *European Journal of Criminology, 5*(4), 411–431. https://doi.org/10.1177/1477370808095124

Bossler, A. M. (2020). Contributions of criminological theory to the understanding of cybercrime offending and victimization. In E. R. Leukfeldt, & T. J. Holt (Eds.), *The human factor of cybercrime* (pp. 29–59). Routledge.

Bowers, K. J. (2001). Small business crime: The evaluation of a crime prevention initiative. *Crime Prevention and Community Safety, 3*(1), 23–42. https://doi.org/10.1057/palgrave.cpcs.8140079

Bowers, K. J., & Johnson, S. D. (2005). Domestic burglary repeats and space-time clusters: The dimensions of risk. *European Journal of Criminology, 2*(1), 67–92. https://doi.org/10.1177/1477370805048631

Braga, A. A., Turchan, B., Papachristos, A. V., & Hureau, D. M. (2019). Hot spots policing of small geographic areas effects on crime. *Campbell Systematic Reviews, 15*(3). https://doi.org/10.1002/cl2.1046

Braga, A. A., Zimmerman, G., Barao, L., Farrell, C., Brunson, R. K., & Papachristos, A. V. (2019). Street gangs, gun violence, and focused deterrence: Comparing place-based and group-based evaluation methods to estimate direct and spillover deterrent effects. *Journal of Research in Crime and Delinquency, 56*(4), 524–562. https://doi.org/10.1177/0022427818821716

Brantingham, P. L., & Brantingham, P. J. (1981). Notes on the geometry of crime. In P. J. Brantingham, & P. L. Brantingham (Eds.), *Environmental criminology* (pp. 27–54). Sage Publications.

Bruinsma, G. J. N., & Johnson, S. D. (Eds.). (2018). *The oxford handbook of environmental criminology*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190279707.001.0001.

Chainey, S. (2012). Repeat victimisation. In *JDiBrief series* (pp. 1–5). UCL Jill Dando Institute of Security and Crime Science. https://www.ucl.ac.uk/jdibrief/analysis/repeat_victimisation.

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

Cornish, D. B., & Clarke, R. V. (Eds.). (1986). *The reasoning criminal: Rational choice perspectives on offending*. Springer-Verlag.

Davanzo, G., Medvet, E., & Bartoli, A. (2011). Anomaly detection techniques for a web defacement monitoring service. *Expert Systems with Applications, 38*(10), 12521–12530. https://doi.org/10.1016/j.eswa.2011.04.038

Eck, J. E. (1994). *Drug markets and drug places: A case-control study of the spatial structure of illicit drug dealing*. University of Maryland.

Fagan, A. A., & Mazerolle, P. (2011). Repeat offending and repeat victimization: Assessing similarities and differences in psychosocial risk factors. *Crime & Delinquency, 57*(5), 732–755. https://doi.org/10.1177/0011128708321322

Farrell, G. (2005). Progress and prospects in the prevention of repeat victimization. In T. Nick (Ed.), *Handbook of crime prevention and community safety* (pp. 145–172). Willan.

Farrell, G., & Pease, K. (1993). Once bitten, twice bitten: Repeat victimisation and its implications for crime prevention. In *Home office, police research group* (pp. 1–38). Crime Prevention Unit Series. No. 46 https://webarchive.nationalarchives.gov.uk/20110218140829/http://rds.homeoffice.gov.uk/rds/prgpdfs/fcpu46.pdf.

Farrell, G., & Pease, K. (2017). Preventing repeat and near repeat crime concentrations. In N. Tilley, & A. Sidebottom (Eds.), *Handbook of crime prevention and community safety* (2nd ed., p. 626). Routledge. https://doi.org/10.4324/9781315724393.

Farrell, G., & Pease, K. (2018). Repeat victimization. In G. J. N. Bruinsma, & D. Weisburd (Eds.), *Encyclopedia of criminology and criminal justice* (pp. 4371–4381). Springer New York. https://doi.org/10.1007/978-1-4614-5690-2_128.

Farrell, G., Tseloni, A., & Pease, K. (2005). Repeat victimization in the ICVS and the NCVS. *Crime Prevention and Community Safety, 7*(3), 7–18. https://doi.org/10.1057/palgrave.cpcs.8140221

Farrington, D. P., & Wikstrom, P.-O. H. (1994). Criminal careers in London and Stockholm: A cross-national comparative study. In E. G. M. Weitekamp, & H.-J. Kerner (Eds.), *Cross-national longitudinal research on human development and criminal behavior* (pp. 65–89). Springer Netherlands. https://doi.org/10.1007/978-94-011-0864-5_2.

Ferrara, E., Wang, W.-Q., Varol, O., Flammini, A., & Galstyan, A. (2016). Predicting online extremism, content adopters, and interaction reciprocity. In E. Spiro, & Y.-Y. Ahn (Eds.), *Social informatics* (Vol. 10047, pp. 22–39). Springer International Publishing. https://doi.org/10.1007/978-3-319-47874-6_3.

Fox, J. A., & Tracy, P. E. (1988). A measure of skewness in offense distributions. *Journal of Quantitative Criminology, 4*(3), 259–274. https://doi.org/10.1007/BF01072453

Hinduja, S., & Kooi, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security Journal, 26*(4), 383–402. https://doi.org/10.1057/sj.2013.25

Holt, T. J. (2011). The attack dynamics of political and religiously motivated hackers. In T. Saadawi, & L. Jordan, Jr. (Eds.), *Cyber infrastruture protection* (pp. 159–180). Strategic Studies Institute.

Holt, T. J. (2019). Computer hacking and the hacker subculture. In *The palgrave handbook of international cybercrime and cyberdeviance* (pp. 1–18). Springer International Publishing. https://doi.org/10.1007/978-3-319-90307-1_31-1.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209

Holt, T. J., & Bossler, A. M. (2017). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge, Taylor & Francis Group.

Holt, T. J., Lee, J. R., Freilich, J. D., Chermak, S. M., Bauer, J. M., Shillair, R., et al. (2020). An exploratory analysis of the characteristics of ideologically motivated cyberattacks. *Terrorism and Political Violence*, 1–16. https://doi.org/10.1080/09546553.2020.1777987

Holt, T. J., Leukfeldt, R., & Van De Weijer, S. (2020). An examination of motivation and routine activity theory to account for cyberattacks against Dutch web sites. *Criminal Justice and Behavior, 47*(4), 487–505. https://doi.org/10.1177/0093854819900322

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*, 1–15. https://doi.org/10.1080/0735648X.2019.1691859

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: Disruption and intervention approaches. *Global Crime, 18*(1), 11–30. https://doi.org/10.1080/17440572.2016.1197123

Johnson, S. D. (2008). Repeat burglary victimisation: A tale of two theories. *Journal of Experimental Criminology, 4*(3), 215–240. https://doi.org/10.1007/s11292-008-9055-3

Johnson, S. D., & Bowers, K. J. (2004a). The stability of space-time clusters of burglary. *British Journal of Criminology, 44*(1), 55–65. https://doi.org/10.1093/bjc/44.1.55

Johnson, S. D., & Bowers, K. J. (2004b). The burglary as clue to the future: The beginnings of prospective hot-spotting. *European Journal of Criminology, 1*(2), 237–255. https://doi.org/10.1177/1477370804041252

Johnson, S. D., Bowers, K. J., & Hirschfield, A. (1997). New insights into the spatial and temporal distribution of repeat victimization. *British Journal of Criminology, 37*(2), 224–241. https://doi.org/10.1093/oxfordjournals.bjc.a014156

Johnson, S. D., Summers, L., & Pease, K. (2009). Offender as forager? A direct test of the boost account of victimization. *Journal of Quantitative Criminology, 25*(2), 181–200. https://doi.org/10.1007/s10940-008-9060-8

Kennedy, D. M. (2012). In *Deterrence and crime prevention: Reconsidering the prospect of sanction* (1st ed.). Routledge. https://doi.org/10.4324/9780203892022.

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review, 30*(4), 470–486. https://doi.org/10.1177/0894439311422689

Lammers, M., Menting, B., Ruiter, S., & Bernasco, W. (2015). Biting once, twice: The influence of prior on subsequent crime location choice. *Criminology, 53*(3), 309–329. https://doi.org/10.1111/1745-9125.12071

Leukfeldt, E. R. (2014). Cybercrime and social ties: Phishing in Amsterdam. Trends in organized crime. https://doi.org/10.1007/s12117-014-9229-5.

Leukfeldt, E. R. (Ed.). (2017). *The human factor in cybercrime and cybersecurity: Research agenda*. Eleven International Publishing. https://www.elevenpub.com/criminology/catalogus/research-agenda-the-human-factor-in-cybercrime-and-cybersecurity-1.

Leukfeldt, E. R., & Holt, T. J. (Eds.). (2020). *The human factor of cybercrime*. Routledge.

Leukfeldt, E. R., & Jansen, J. (2020). Financial cybercrimes and situational crime prevention. In E. R. Leukfeldt, & T. J. Holt (Eds.), *The human factor of cybercrime* (pp. 216–239). Rutledge.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017a). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology, 57*(3), 704–722. https://doi.org/10.1093/bjc/azw009

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017b). A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change, 67*(1), 21–37. https://doi.org/10.1007/s10611-016-9662-2

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017c). The use of online crime markets by cybercriminal networks: A view from within. *American Behavioral Scientist, 61*(11), 1387–1402. https://doi.org/10.1177/0002764217734267

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Levin, A., Rosenfeld, R., & Deckard, M. (2017). The law of crime concentration: An application and recommendations for future research. *Journal of Quantitative Criminology, 33*(3), 635–647. https://doi.org/10.1007/s10940-016-9332-7

Madarie, R. (2017). Hackers' motivations: Testing Schwartz'S theory of motivational types of values in A sample of hackers. *International Journal of Cyber Criminology, 11*(1), 1–20. https://doi.org/10.5281/zenodo.495773

Maimon, D., Fukuda, A., Hinton, S., Babko-Malaya, O., & Cathey, R. (2017). In *On the relevance of social media platforms in predicting the volume and patterns of web defacement attacks* (pp. 4668–4673). IEEE International Conference on Big Data (Big Data). https://doi.org/10.1109/BigData.2017.8258513.

Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology, 2*(1), 191–216. https://doi.org/10.1146/annurev-criminol-032317-092057

McGuire, M., & Dowling, S. (2013). Cyber-dependent crimes. In *No. 75; cyber crime: A review of the evidence* (pp. 1–35). Home Office https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf.

Miró-Llinares, F. (2011). La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista Electrónica de Ciencia Penal y Criminología, 13*(7), 1–55.

Miró-Llinares, F., & Johnson, S. D. (2018). Cybercrime and place: Applying environmental criminology to crimes in cyberspace. In G. J. N. Bruinsma, & S. D. Johnson (Eds.), *The oxford handbook of environmental criminology* (pp. 883–906). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190279707.013.39.

Miró-Llinares, F., & Moneva, A. (2019). Environmental criminology and cybercrime: Shifting focus from the wine to the bottles. In T. J. Holt, & A. M. Bossler (Eds.), *The palgrave handbook of international cybercrime and cyberdeviance* (pp. 1–22). Springer International Publishing. https://doi.org/10.1007/978-3-319-90307-1_30-1.

Miró-Llinares, F., Moneva, A., & Esteve, M. (2018). Hate is in the air! But where? Introducing an algorithm to detect hate speech in digital microenvironments. *Crime Science, 7*(15), 1–12. https://doi.org/10.1186/s40163-018-0089-1

Moitra, S. D., & Konda, S. L. (2004). An empirical investigation of network attacks on computer systems. *Computers & Security, 23*(1), 43–51. https://doi.org/10.1016/S0167-4048(04)00067-7

Moneva, A. (2020). *Cyber places, crime patterns, and cybercrime prevention: An environmental Criminology and crime Analysis approach through data science [Doctoral thesis]*. Miguel Hernandez University.

Moneva, A., Miró-Llinares, F., & Hart, T. C. (2020). Hunter or prey? Exploring the situational profiles that define repeated online harassment victims and offenders. *Deviant Behavior, 1–16*. https://doi.org/10.1080/01639625.2020.1746135

Nazaretian, Z., & Merolla, D. M. (2013). Questioning Canadian criminal incidence rates: A Re-analysis of the 2004 Canadian victimization survey. *Canadian Journal of Criminology and Criminal Justice, 55*(2), 239–261. https://doi.org/10.3138/cjccj.2012.E18

Newman, G. R., & Clarke, R. V. (2003). *Superhighway robbery preventing e-commerce crime*. Routledge Chapman & Hall.

Park, S. min, & Eck, J. E. (2013). Understanding the random effect on victimization distributions: A statistical analysis of random repeat victimizations. *Victims and Offenders, 8*(4), 399–415. https://doi.org/10.1080/15564886.2013.814612

Pease, K. (1998). In *Repeat vicimisation: Taking stock (No. 90; crime detection and prevention series* (pp. 1–40). Home Office, Police Research Group.

Planty, M., & Strom, K. J. (2007). Understanding the role of repeat victims in the production of annual US victimization rates. *Journal of Quantitative Criminology, 23*(3), 179–200. https://doi.org/10.1007/s10940-007-9026-2

Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention and Community Safety, 12*(2), 99–118. https://doi.org/10.1057/cpcs.2009.22

Romagna, M. (2019). Hacktivism: Conceptualization, techniques, and historical view. In T. J. Holt, & A. M. Bossler (Eds.), *The palgrave handbook of international cybercrime and cyberdeviance* (pp. 1–27). Springer International Publishing. https://doi.org/10.1007/978-3-319-90307-1_34-1.

Romagna, M., & Van den Hout, N. J. (2017). In *Hacktivism and website defacement: Motivations, capabilities and potential threats* (pp. 1–11).

Thapngam, T., Yu, S., Zhou, W., & Beliakov, G. (2011). Discriminating DDoS attack traffic from flash crowd through packet arrival patterns. In *IEEE conference on computer communications workshops* (pp. 952–957). INFOCOM WKSHPS. https://doi.org/10.1109/INFCOMW.2011.5928950.

Turanovic, J. J., Pratt, T. C., & Piquero, A. R. (2018). Structural constraints, risky lifestyles, and repeat victimization. *Journal of Quantitative Criminology, 34*(1), 251–274. https://doi.org/10.1007/s10940-016-9334-5

van de Weijer, Steve, G. A., Holt, Thomas, J., & Leukfeldt, E. Rutger (2021). Heterogeneity in trajectories of cybercriminals: A longitudinal analyses of web defacements. *Computers in Human Behavior Reports, 4*. https://doi.org/10.1016/j.chbr.2021.100113

Weisburd, D. (2015). The law of crime concentration and the criminology of place. *Criminology, 53*(2), 133–157. https://doi.org/10.1111/1745-9125.12070

Weisel, D. L. (2005). *Analyzing repeat victimization* (pp. 1–80). U.S. Department of Justice, Office of Community Oriented Policing Services.

Weulen Kranenbarg, M., Holt, T. J., & van Gelder, J.-L. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior, 40*(1), 40–55. https://doi.org/10.1080/01639625.2017.1411030

Weulen Kranenbarg, M., Ruiter, S., van Gelder, J.-L., & Bernasco, W. (2018). Cyber-offending and traditional offending over the life-course: An empirical comparison. *Journal of Developmental and Life-Course Criminology, 4*(3), 343–364. https://doi.org/10.1007/s40865-018-0087-8

Wickham, H. (2017). In *Tidyverse: Easily install and load the 'tidyverse'*. https://CRAN.R-project.org/package=tidyverse.

Williams, M. L., & Burnap, P. (2016). Cyberhate on social media in the aftermath of woolwich: A case study in computational criminology and big data. *British Journal of Criminology, 56*(2), 211–238. https://doi.org/10.1093/bjc/azv059

Wood, G., & Papachristos, A. V. (2019). Reducing gunshot victimization in high-risk social networks through direct and spillover effects. *Nature Human Behaviour*. https://doi.org/10.1038/s41562-019-0688-1

Woo, H., Kim, Y., & Dominick, J. (2004). Hackers: Militants or merry pranksters? A content analysis of defaced web. *Media Psychology, 6*(1), 63–82. https://doi.org/10.1207/s1532785xmep0601_3

Wortley, R., & Townsley, M. (Eds.). (2017). *Environmental criminology and crime analysis* (2nd ed.). Routledge, Taylor & Francis Group.

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407–427. https://doi.org/10.1177/147737080556056

Asier Moneva is a postdoctoral researcher at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), and the Center of Expertise Cyber Security of The Hague University of Applied Sciences. His research interests pivot on the human factor in cybercrime including cybercrime analysis and prevention from a situational perspective.

Eric Rutger Leukfeldt is a senior researcher and cybercrime cluster coordinator at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), and director of the Center of Expertise Cyber Security at The Hague University of Applied Sciences. His research interests pivot on the human factor in cybercrime including organized crime and criminal networks.

Steve van de Weijer is a researcher at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR). His research interests include intergenerational transmission of crime, genetic influences on criminal behavior, life-course criminology, and cybercrime.

Fernando Miró-Llinares is a Professor of Criminal Law and Chair of the Crímina Research Center for the Study and Prevention of Crime at Miguel Hernandez University of Elche. His research interests include cybercrime, artificial intelligence in criminal justice, ethics, and crime prevention.