Why would we get attacked? An analysis of attacker's aims behind DDoS attacks

Abhishta Abhishta*, Wouter van Heeswijk, Marianne Junger,
Lambert J. M. Nieuwenhuis, and Reinoud Joosten
University of Twente, The Netherlands
{s.abhishta, w.j.a.vanheeswijk, m.junger, l.j.m.nieuwenhuis, r.a.m.g.joosten}@utwente.nl

Received: February 20, 2020; Accepted: June 2, 2020; Published: June 30, 2020

Abstract

Reliable availability to the internet and internet-based services is crucial in today's world. DDoS attacks pose a severe threat to the availability of such online resources – especially owing to booters – virtually everyone can execute them nowadays. In order to appropriately protect oneself against such attacks, it is essential to have a good insight into the threats that exist. This paper proposes a novel hybrid model that combines postulates from various models on crime opportunity, analyzing the targeted victim and the targeted infrastructure in conjunction. We apply this model to analyze 27 distinct attack events that occurred in 2016. To construct this dataset, we utilize a longitudinal news database specific to DDoS-related events, aiding to select relevant attack events. We outline the procedure to replicate the dataset construction process. Looking at DDoS attacks solely as a technical issue is not enough, news articles can be an important resource in providing contextual relevance to this problem. Our analysis reveals several motives underlying DDoS attacks; economic reasons are but one of the possible aims. For this reason, we advise companies to also monitor the socio-cultural and political environment. In terms of infrastructure, visibility and accessibility are the main instigators for an attack. A holistic perspective is imperative to accurately map the threats that companies face and to take appropriate protective measures.

Keywords: DDoS attacks, Routine Activity Theory, Cyber Crime, Aims, Cyber Attacks

1 Introduction

In today's world, it is crucial that the internet and internet-based services are constantly available. Individuals and organizations derive great benefits from network services in areas such as communication, employment, education and health. The daily performance of enterprises also critically hinges on reliable internet availability, with operations such as sales, planning, and information exchange taking place online. In most cases when online availability unexpectedly goes down, it is typically not possible to find or set up a short-term substitute offline. Depending on the information or service that is unavailable, the effect may vary from inconvenient to right out disastrous. Either directly or indirectly, the firm or individual is subject to a financial loss as a consequence of unavailability [1]. For a web shop being unavailable for two hours the financial impact may be easier to derive than for an individual who cannot access his/her insurance information, but negative financial effects exist in both cases.

An important cause of internet services' downtime is the work of malicious actors. By means of cyber attacks, they aim to disrupt the normal functioning of the internet or to steal digital information.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 11(2):3-22, June 2020
DOI:*10.22667/JOWUA.2020.06.30.003*

*Corresponding author: Department of Industrial Engineering and Business Information Systems, University of Twente, The Netherlands, Tel: +31-534-89-6565

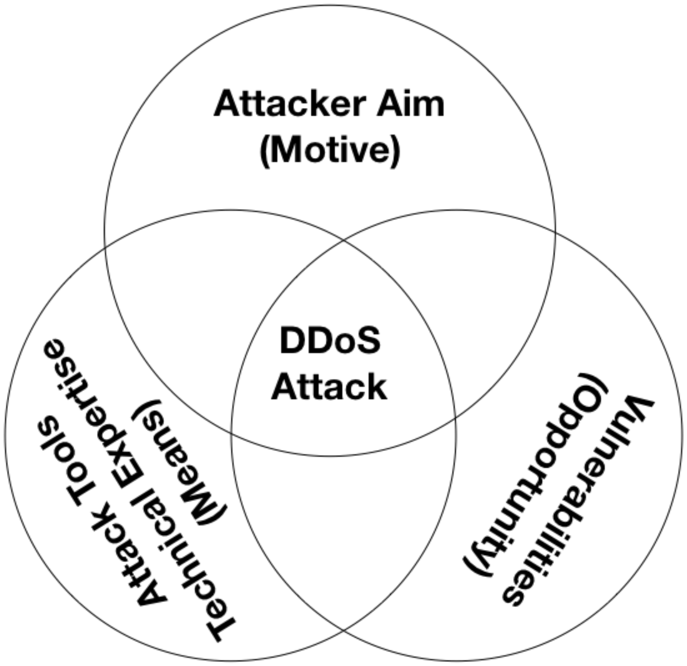


Figure 1: Aspects of a DDoS Attack.

This paper focuses on Distributed Denial of Service (DDoS) attacks, which temporarily make web-based services unavailable to the intended user base. These attacks rely on overloading the targeted system with a large number of communication requests – mostly automated by using a botnet – such that the system becomes so slow that it cannot adequately respond to legitimate requests. DDoS attacks can be used to bring down any network connected infrastructure.

For a firm to adequately defend its online infrastructure, it is important that they ask themselves the question: *why would we get attacked?* Hence, have a good insight into the reasons why anyone would attack their systems. Mapping these reasons enables the firm to make a realistic assessment of the external threats they face and respond with an appropriate defense strategy, reducing vulnerabilities and insuring against losses.

To gain insights into the external threats, it is important to realize that a DDoS attack is no different from a conventional crime. For conventional crimes, three aspects need to be proven before any wrongdoing is determined: means, motive, and opportunity [2]. In the context of DDoS attacks, the *means* refer to the sufficient availability of both attack tools and technical capability required to execute the attack. The *motive* describes the attacker's reasons to target a specific firm or infrastructure. Finally, the *opportunity* refers to the vulnerabilities of the targeted system that may be exploited in an attack. The three aspects of a DDoS attack are shown in Figure 1.

This paper addresses the attacker's aims to perform DDoS attacks, building on the preliminary work sketched in [3]. In this article, we provide insights on the decision-making process of an attacker based on the steps he/she has to take in order to launch an attack. We analyze attacker aims by taking into account the socio-cultural, political and economic (abbreviated to SPEC) dimensions of DDoS attacks, as well as the postulates of routine activity theory (RAT). Based on these aspects of RAT and SPEC, we propose a model to analyze the content of news articles related to a specific DDoS attack. Previous studies such as [4, 5, 6, 7] that have analyzed attacker's aims behind DDoS attacks have done so by studying DDoS attacks associated with a single aim. However, these studies do not provide a framework for analyzing aims. We show that news articles reporting DDoS attacks can be used as a source of information for analyzing attacker's aims. Subsequently, we apply our model to analyze probable attacker aims in 27 unique cases that occurred in the year 2016.

The remainder of the paper is structured as follows: Section 2 positions our work in the body of existing literature and addresses our contribution. In Section 3, we describe our methodology, more specifically the procedure to construct the dataset and the model utilized to analyze its content. Section 4 describes and discusses the results of our analysis. Section 5 concludes the paper and provides several directions for future research.

2 Literature

This section provides a brief overview of existing literature and is composed of four elements. First, we describe the Routine Activity Theory (RAT) and the Rational Choice Model (RCM); these theories on crime opportunity forms the rational basis for our analysis. Second, we discuss the properties of value, inertia, visibility, and accessibility (VIVA), which are related to RAT and describe the conditions under which a victim is likely to be targeted; we will use these criteria to evaluate infrastructure targeting. Third, we discuss the properties of the socio-cultural, political and economic (SPEC) model, which describes the underlying motives to select a specific victim. Fourth, we discuss a number of existing studies on the analysis of motives behind both DDoS attacks and cyber attacks in general.

The Routine Activity Theory (RAT) is a sub-domain of the theory on crime opportunity, which addresses the situational circumstances of crimes. RAT as mentioned previously was proposed by Cohen & Felson in 1979 [8], becoming one of the most widely accepted theories on crime since. It is rooted in theories on rational choice and human ecology. It considers a crime as an event that is closely tied to human ecology and the environment of the attacker. According to the Routine Activities Theory (RAT), a crime occurs when there is a suitable target, a motivated offender in the absence of a capable guardian [8, 9].

A motivated offender is often present and is described by the Rational Choice Model (RCM) of crime [10]. The RCM states that offenders are rational actors who are goal oriented. They make a crude cost-benefit calculation to decide whether or not to commit an offense. Of course, this rational evaluation is usually a bounded rationality, limited by various contextual aspects (e.g., incompleteness of information) and offender characteristics (such as on an impulse or drug use) that limit the offender's judgment. The RCM does not imply offenders are only or even mainly economically motivated. All sorts of motives can provide motives for crime. Revenge or anger constitute equally valid motivations that can then be pursued by rational means. The rationality is largely situated in the selection of the suitable targets and the choice of modus operandi, given a chosen goal [10].

Both RAT and the RCM do not assume crime is deeply motivated. On the contrary, making crime more difficult or more risky to commit will often deter many offenders, as studies on situation crime prevention show [11].

Besides a motivated offender, RAT has stressed the importance of opportunities to commit a crime and the means to execute it [12, 13]. A specific context provides opportunities, that is, favorable conditions for specific crimes. A house with an open window is conducive to burglary, whilst a car's open door to car theft. A computer system that was not updated creates opportunities for cyber criminals [14, 15]. This means that opportunities are crime specific and should be studied one type of crime at the time.

Related to the RAT are the properties of value, inertia, visibility, and accessibility, usually rendered in the acronym VIVA [12]. These four dimensions influence the probability of a victim being targeted. *Value* links to the worth that the victim has to the attacker; this value may differ based on the perspective of the attacked. Second, *inertia* refers to the size of the target; smaller crimes occur more often as they are easier to accomplish. Third, *visibility* describes to what extent the target is exposed to the offender, i.e., the degree to which the offender knows the target. Fourth, *access* is a property that captures how easily offenders can reach the target and the obstacles that may hamper a successful attack. The higher the target scores on these properties, the higher the chance of being attacked. In Section 3.2, we will tailor these properties specifically towards DDoS attacks.

The next topic we discuss are the social, political, economic, and cultural (SPEC) dimensions that describe potential motives for targeting a specific victim. Many variants of this framework with appropriate acronyms exist; arguably the PEST framework – which adds a technological dimension that we treat separately from the victim, namely in the analysis of the infrastructure – is the most well-known. We briefly discuss the various dimensions. The social and cultural dimensions are typically combined into a socio-cultural one, which among others includes cultural aspects, the demography of the population, career attitudes and the emphasis on safety. The political dimension encapsulates, for instance, goods and services which are (or are not) provided by the government, as well as policies on national matters such as labor, privacy, health, and education. Finally, the economic dimension includes factors such as economic growth, inflation, and interest. Economic factors strongly influence the way individuals and firms make decisions. In terms of criminology, each of these dimensions may provide strong motives for an attacker to select a certain victim. Again, Section 3.2 reflects on these dimensions in the context of DDoS attacks.

We proceed to discuss literature geared towards the aims behind DDoS attacks. So far, only few studies have been performed in this direction. Hutchings & Clayton [4] discuss the incentives for booter owners. They observe that these services provide "easy money" for youngsters that own them. Paulson & Webber [5] discuss the deployment of DDoS attacks with the aim of extortion. In their study, they focus on online gaming companies that are being targeted for this purpose. Narario [6] discusses DDoS attacks that are politically motivated. Nazario analyzed a sample of Internet backbone traffic, botnet activities, BGP routing changes, and community chatter about politically motivated attacks to show that DDoS attacks may be used as a simple, blunt force political weapon to silence critics or opponents. The work of Sauter [7] addresses DDoS attacks performed for ideological (or hacktivism) purposes. Finally, Zargar et al. [16] summarized a list several incentives – although most of them are not backed by evidence in the paper – that attackers might have to execute DDoS attacks:

- Financial/economic gain: The attacker is paid for an assault on a specific target;
- Revenge: The attacker seeks to extract retribution on an individual or firm with an assault;
- Ideological beliefs: The attacker targets its victim to voice a form of disagreement;
- Intellectual challenge: The attacker is experimenting and trying to learn from the activity or seeking to showcase their capabilities;
- Cyber warfare: The attacker is part of a military- or terrorist organization that aims to damage an enemy.

In addition to studies that explicitly focus on the aims behind DDoS attacks, several studies address the non-technical characteristics of cyber attacks in their entirety, e.g., not restricted to DDoS attacks only. In this category, Liu & Cheng [17] discuss various reasons for cyber attacks to happen (e.g. due to existence of vulnerabilities and higher dependence of enterprises on IT). In addition, they explain that attackers can both be inside and outside a victim organization and can use cyber attacks in a planned step-by-step manner to make profits. Gandhi et al. [18] apply the SPEC dimensions to the domain of cyber attacks. They make a selection of security events that occurred between 1996 an 2010 and analyze these events using the SPEC dimensions. Sharma et al. [19] propose a social dimensional threat model,

Table 1: Characteristics of the dataset.

Dates		#Articles		#Articles/day		Standard Deviation	
Start	End	Web	News	Web	News	Web	News
01-01-2016	31-12-2016	9387	4458	25.6	12.18	7.55	8.67

making use of historical cyber attack events. They apply their model to evaluate a selection of 14 news articles on cyber attacks. Geers et al. [20] analyze the nation-state motives behind cyber attacks. Kumar & Carley [21] perform network analysis on the data from Arbor network's digital attack map and Twitter data. They find a link between the probability of an attack aimed at a specific country and the sentiments towards that country on social media, stating that a negative sentiment increases the likelihood of an attack.

A widely-supported conclusion of the existing literature is that cyber attacks are not carried out solely for the purpose of financial gain. Booters have made the execution of DDoS attacks an easy weapon to deploy for nearly every individual, implying that a number of aims may trigger attackers to launch an assault. The studies that have been performed so far may roughly be classified in two categories. The first category evaluates the aims of attackers with respect to the SPEC dimensions, trying to find some socio-cultural, political or economic motive for an attack. The second category *a priori* hypothesizes a specific aim and subsequently seeks to provide evidence in support of the relevance of that motive.

DDoS attacks can be used to make any network infrastructure unavailable by consuming its resources. An attacker needs to make two choices in order to execute an attack, namely (i) the selection of a victim (the firm or the individual that they wish to attack) and (ii) the network infrastructure of the victim that they target. To this end, we propose a coherent hybrid model to evaluate attacker aims. Our evaluation strategy consists of analyzing the victim on the SPEC dimensions and rationalizing the choice of infrastructure based on the postulates of RAT. This model will be crystallized in Section 3.

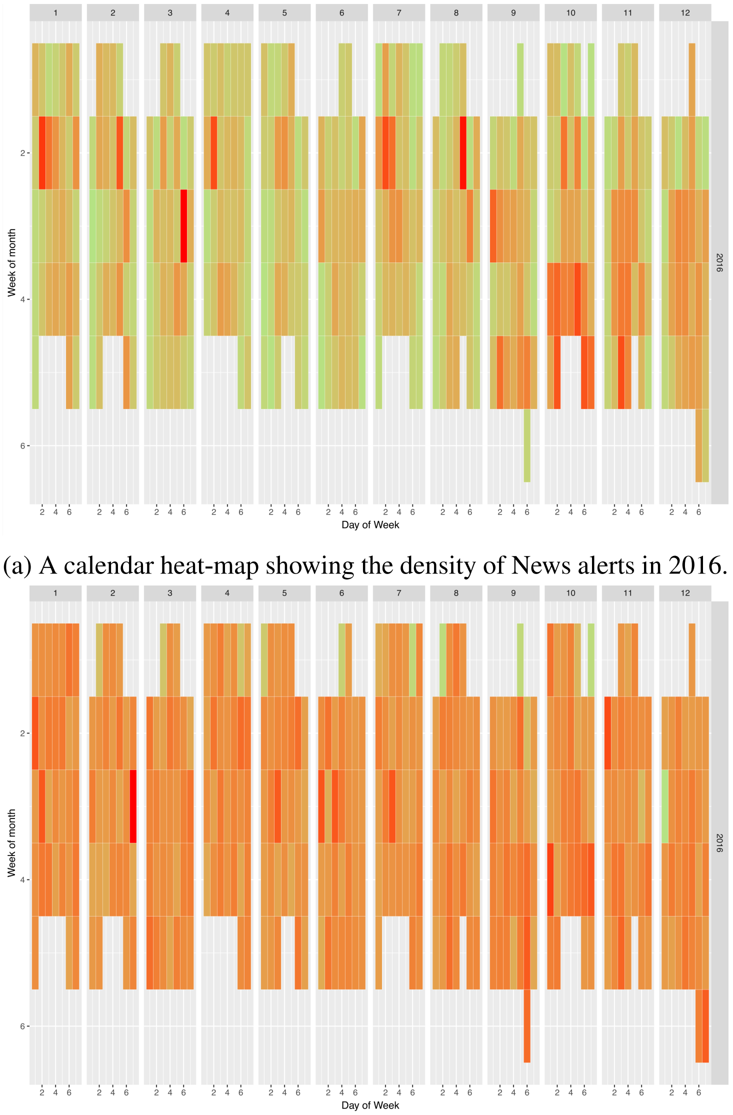
The contributions of our work are as follows. First, we propose a novel hybrid model that draws from existing frameworks on analyzing crime opportunity, enabling to evaluate both the victim and its corresponding infrastructure on various relevant metrics. Second, we analyze a distinct dataset, as such contributing to the insights that others have obtained by analyzing different datasets. Third, we show our procedure on constructing a dataset in such a way that it can easily be reproduced by other researchers. Fourth, we aim find empirical support for incentives listed by Zargar et al. [16].

3 Methodology

This section discusses the characteristics of the dataset and the sampling strategy deployed to extract DDoS attack events. We proceed to explain the proposed model for content analysis of news articles. Section 3.1 describes how the dataset is constructed. Section 3.2 describes the hybrid model that we develop to analyze the news alerts related to DDoS attacks.

3.1 Dataset and Sampling

The dataset [22] used for our analysis consists of a collection of *Google Alerts* on DDoS attacks. Google Alerts is a service that offers content change detection and real-time notifications on user-selected keywords. Its alerts are distinguished into two categories, namely (i) News and (ii) Web. The former category relates to all content posted on news outlets, the latter contains all other content. Figure 2 shows the density of 'News' and 'Web' alerts collected on each day. Collection of 'News' alerts are concentrated on



(a) A calendar heat-map showing the density of News alerts in 2016.

(b) A calendar heat-map showing the density of Web alerts in 2016.

Figure 2: Calendar heat-maps showing the density of alerts in 2016.

certain days, this suggests that these alerts are event-driven. Since we want to gather information related to DDoS attack events, in this study we only consider ‘News’ alerts. For gathering all other news articles required for this study we make use of LexisNexis’ proprietary data which has been used for a variety of studies that involve analysing news articles [23, 24].

For our analysis, we restrict ourselves to the most high-impact DDoS attacks; as these events received the most media coverage, they are most suitable to deduce insights on the underlying motives for these attacks. We propose a sampling procedure to filter out these events. The objective of this sampling procedure is to extract the most reported DDoS attacks of the year 2016.

To classify a day as ‘eventful’, we utilize the methodology that was also used by Kallus et al. [25]. First, we define a statistically relevant threshold θ. If the number of alerts on a given day exceeds this threshold, we classify that day as ‘eventful’. The threshold θ is calculated based on the empirical distribution of the number of alerts that have generated for each day. In Figure 3, we show the empirical

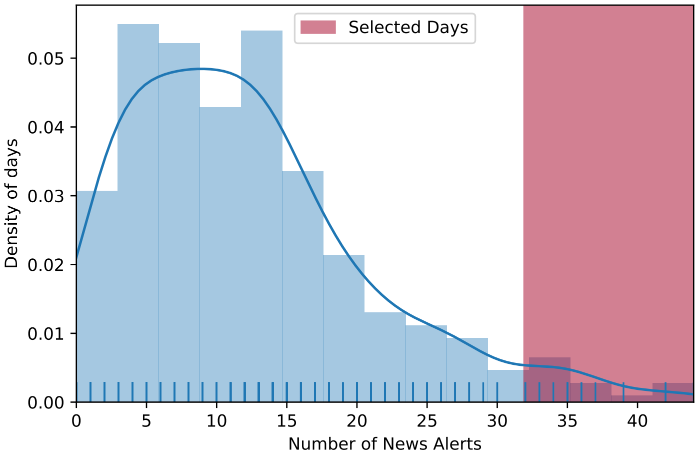


Figure 3: Histogram depicting selection criterion for *eventful* days.

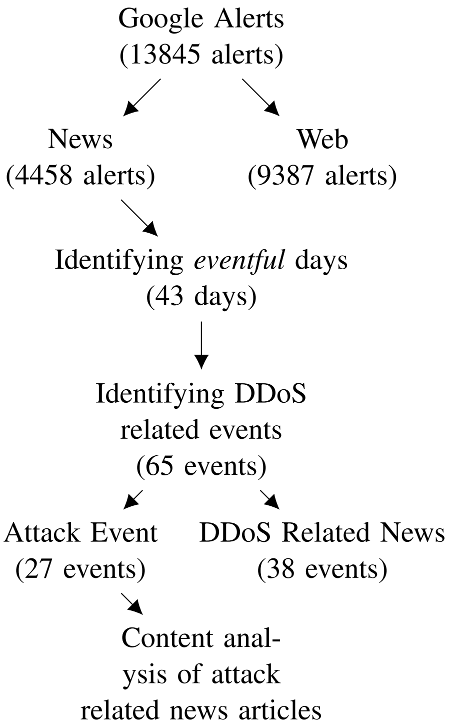


Figure 4: Summary of DDoS attack event extraction process.

distribution for the number of ‘News’ alerts that have been generated daily over the course of the year. To construct our dataset, we fix our threshold parameter θ such that exceeding it lands a day into the top 20 percentile. Thus, the dataset of ’eventful’ days contains the 20% of most eventful days in terms of news alert. The corresponding threshold θ is 31.92 alerts, which we round to the nearest integer. Therefore, if in a single day 32 or more ‘News’ alerts are reported, we consider this day as ‘eventful’. By applying this threshold, we obtain a set consisting of 43 eventful days. The alerts that have been generated on any of these days are included in our study.

The next step is to translate the number of eventful days into the actual number of events. It is important to note that a single attack may be covered in the news for multiple days. We identify the events that are responsible for generating abnormally high numbers of alerts on the eventful days as follows. First, we evaluate the texts of all alerts on an eventful day and classify the reported events into *DDoS-related* events (i.e., news alerts that mention the subject of DDoS but do not cover an actual attack) and *DDoS-attack* events (i.e., news alerts that cover an actual attack that occurred). Appendix A lists all the events (DDoS attack and related events) identified by us.

Figure 4 shows a breakdown of the methodology used by us to extract DDoS attack reporting news articles. Common themes in the news report are, for instance, a research report that was published by a company that protects against DDoS attacks, or measures that have been taken by law enforcement agencies. The content of each event has been manually tagged on the eventful days to identify the alerts that reported an attack. Finally, we gather all the news articles in our dataset regarding the identified DDoS attack events by using a simple word search[1] and analyze their content.

3.2 Content Analysis

The decisions of the attacker when selecting a target for a DDoS attack may be decomposed into the following two components: (i) the choice of the victim organization to target and (ii) the choice of the network infrastructure to target. Figure 6 shows the hybrid model that we developed to analyze the aims of attackers. In [26], we have shown that victim routines can have significant impact on value, inertia, visibility and accessibility of the network infrastructure. For example, the web servers of academic institutions are of higher value & visibility during working days than on holidays due to the absence of academic activities. The proposed model captures this dimension as well.

We describe the hybrid model in more detail. To evaluate the attacker's choice of victim, we follow the socio-cultural, economic and political (SPEC) criteria that were suggested and applied by Gandhi et al. [18]. We recall that their study has demonstrated that these dimensions indeed affect the selection of victims, therefore we incorporate them in our model as well. For the choice of the network infrastructure that is targeted, we make the assumption that attackers are rational decision makers, i.e., the attackers consciously decide which infrastructure to target. By adopting this assumption, we are able to utilize the postulates of the routine activities theory (RAT). We remind that the conjunction of (i) a motivated offender, (ii) the absence of a capable guardian and (iii) a suitable target are an ideal breeding ground for an attack. We apply the theory to analyze the targeting of infrastructures. Our model estimates the suitability of an infrastructure for predation based on the VIVA criteria (value, inertia, visibility and accessibility). In the context of infrastructure targeting in DDoS attacks, we detail the VIVA dimensions as follows:

- Value: The importance of the infrastructure to the victim. For instance, when a company makes a great percentage of its sales online, its web-shop would be of high value.
- Inertia: The degree of resistance posed by the infrastructure when being attacked. A high inertia infrastructure may deploy better protection strategies against DDoS attacks or is simply able to sustain highly intense network traffic (e.g., distributed servers, websites hosted in the cloud).
- Visibility: The extent to which the infrastructure is visible on the web [27]. Highly visible web infrastructures are mostly public facings, e.g., a publicly available website.
- Accessibility: The attacker's ability to reach the target and get away from the crime scene with impunity. An example of an infrastructure with high accessibility would be a server whose *IP*

[1] The keywords used for this search are shown in Appendix A

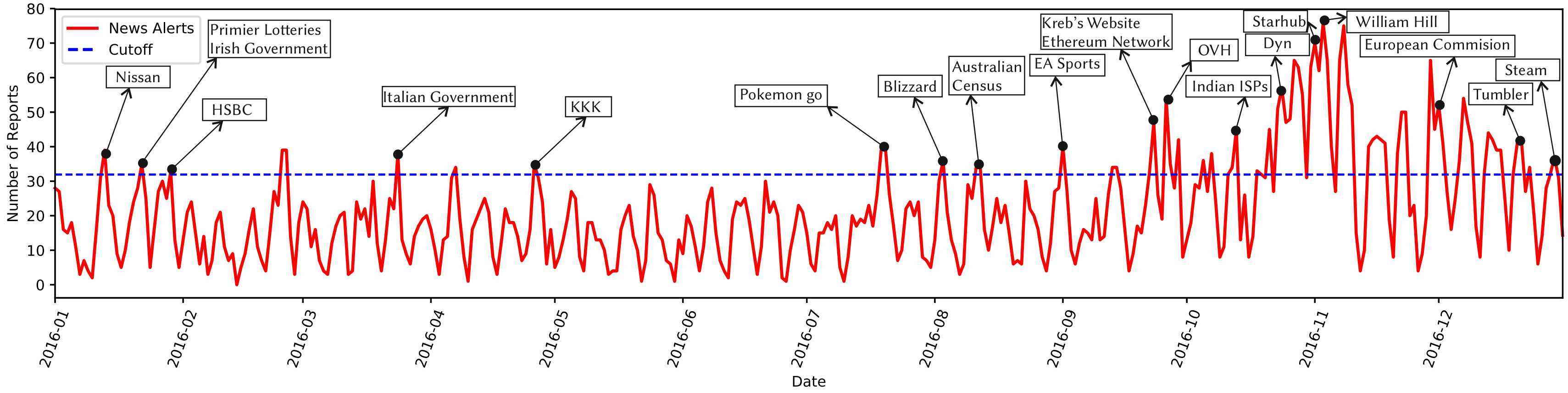


Figure 5: Attack time-line showing the extracted attack events for $\theta = 32$.

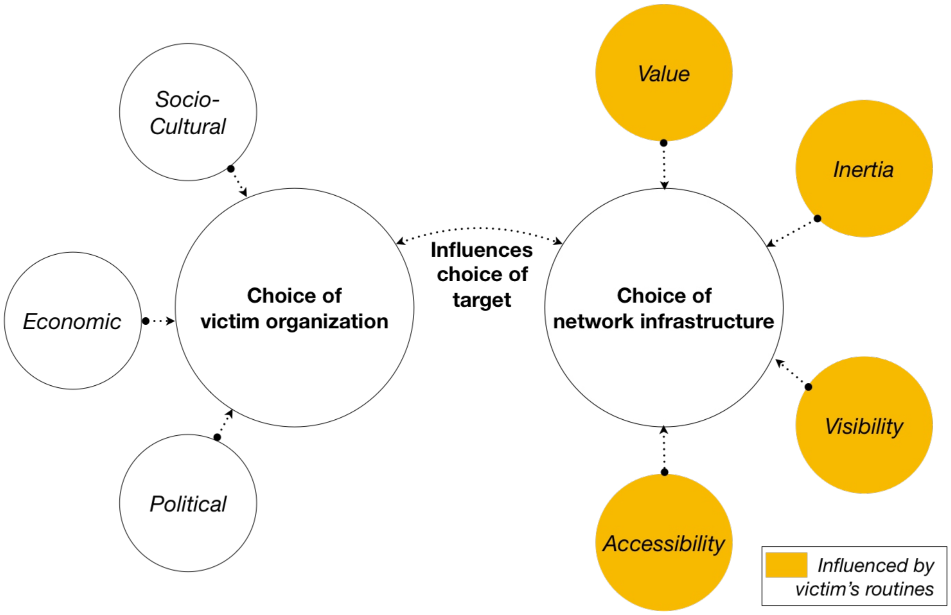

Socio-Cultural
Economic
Political
Choice of victim organization
Influences choice of target
Choice of network infrastructure
Value
Inertia
Visibility
Accessibility
Influenced by victim's routines

Figure 6: Model for analyzing attacker aims using news articles.

address may easily be accessed and has been set up without network monitoring applications of intrusion detection systems in place.

Integrating the concepts that have been discussed in this section, we are able to analyze the probable aims behind attack events. Having defined the hybrid model, we proceed to apply it for the analysis of our constructed dataset in Section 4. We expect certain links between the dimensions of victim targeting and infrastructure targeting to materialize. For instance, if a victim would be targeted for political reasons, we would expect that the targeted infrastructure is one of high visibility, as the goal would likely involve reaching a wide audience. Similarly, when the victim is mainly chosen based on economic incentives, the value of the infrastructure should be the main determinant in its selection.

In order to use the proposed model to evaluate the news articles we first determine the victim (organization) and the network infrastructure under attack. We then analyze the socio-cultural, economic and political circumstances of the organization in the period before the attack. This is done by evaluating all news articles about the firm published in the one month time period before the attack. In the next step, we analyze the VIVA characteristics of the targeted network infrastructure. In practice, organizations may identify high value, high inertia, high visibility and high accessibility network infrastructures by organizing a cyber risk assessment exercise [28]. Finally, on the basis of the information collected we discuss the probable aims behind the attack.

4 Results and Discussion

Having presented the dataset and the hybrid model to analyze it, we proceed with our analysis. At this point we would like to remind the reader from Section 3.1 that after filtering the alerts over the year 2016, we were initially left with 43 eventful days. The number of alerts that were collected on these eventful days is 1929. Although the eventful days constitute only 11.75% of the days of the calendar year, they account for nearly 43% of all ‘News’ alerts. We find this result in alignment with the findings of Johnson [29], who states that traditional crimes are also strongly concentrated in space and time. Thus, in this aspect DDoS attacks do not deviate from traditional crimes, displaying a similar occurrence pattern.

Table 2 summarizes the key components for each of the selected attack events. We evaluate the victim on the SPEC dimensions and the targeted infrastructure on the VIVA dimensions, utilizing the news sources that cover the attack. The remainder of this section discusses these attack reports in detail. We report our findings in accordance with the hybrid model designed in Section 3.2. The full evaluation results are shown in Table 2; in the main text we highlight the most salient observations.

Table 2: Analysis of each of the selected attack event.

Date	*Reference*	*Victim*	**Socio-Cultural**	**Political**	**Economic**	*Infrastructure*	**Value**	**Inertia**	**Visibility**	**Accessibility**
13/01/2016	[30]	Nissan Motors	●			Website	Low	Low	High	High
22/01/2016	[31]	Premier lotteries			●	Ticket machines and Website	High	Low	High	High
22/01/2016	[32]	Irish government	●	●		Website	Low	Low	High	High
29/01/2016	[33]	HSBC			●	Online Banking Server	High	High	Low	Low
26/02/2016	[34]	Italian government	●	●		Website	Low	Low	High	High
26/04/2016	[35]	Ku Klux Klan	●			Website	Low	Low	High	High
20/07/2016	[36]	Pokémon Go			●	Gaming Server	High	Low	Low	High
03/08/2016	[37]	Blizzard Entertainment			●	Gaming Server	High	Low	Low	High
11/08/2016	[38]	Australian Census	●			Website	High	Low	High	High
01/09/2016	[39]	EA Sports			●	Gaming Server	High	Low	Low	High
23/09/2016	[40]	Brian Kreb		●		Website	Low	High	High	High
23/09/2016	[41]	Ethereum network			●	Servers	High	Low	Low	Low
29/09/2016	[42]	OVH			●	Hosting Server	High	High	Low	High
18/10/2016	[43]	ISPs in India			●	Network Devices	High	High	Low	High
21/10/2016	[44]	Dyn			●	Servers	High	High	Low	High
27/10/2016	[45]	StarHub			●	Network Devices	High	High	Low	High
02/11/2016	[46]	William Hill			●	Website	High	Low	High	High
08/11/2016	[47]	Canadian migration		●		Website	Low	Low	High	High
08/11/2016	[48]	WikiLeaks		●		Website	High	Low	High	High
08/11/2016	[49]	Trump and Clinton	●	●		Website	Low	Low	High	High
29/11/2016	[50]	Eir			●	Email Server	High	Low	Low	Low
25/11/2016	[51]	Deutsche Telekom			●	Network Devices	High	High	Low	High
30/11/2016	[52]	European Commission	●	●		Website	Low	Low	High	High
15/12/2016	[53]	Black Lives Matter	●			Website	Low	Low	High	High
15/12/2016	[54]	BTC exchange			●	Servers	High	Low	Low	Low
21/12/2016	[55]	Tumblr			●	Website	High	Low	High	High
23/12/2016	[56]	Steam			●	Gaming Servers	High	Low	Low	High

Based on our analysis, we are able to broadly classify the selected attack events into the following six categories: (i) attacks on large manufacturing companies, (ii) attacks targeting public figures and ideological groups, (iii) attacks targeting governments, (iv) attacks on gaming and gambling platforms, (v) attacks on internet service providers ans hosting service providers and (vi) attacks on financial institutions.

The first category (large manufacturing companies) includes the attack on the Japanese car manufacturer Nissan Motors. During this attack, all the global websites of the automotive company Nissan were reported to have suffered downtime. Nissan does not have an online shop for its cars, therefore the websites are of relatively low value to the firm. However, the attack was carried out during the Detroit auto show. When such shows are being held, car manufacturers expect the attending visitors to visit their websites in order to learn more about the cars they viewed. As such, the website had a high visibility during that time period, even though Nissan does not sell cars online. In later reports covering the attack, it was suggested that the hacker group Anonymous was behind the attack, targeting the website as a protest against whale hunting in Japan. Thus, it may be concluded that the high visibility of the website during that time period was the key input for the target selection.

The second category (public figures and ideological groups) includes attacks on the websites of Brian Krebs (an investigative reporter covering profit-seeking cybercriminals), Black Lives Matter, the Ku Klux Klan, WikiLeaks, Donald Trump and Hillary Clinton (the latter two running for presidency in 2016). The websites of victims within this category are easy targets that have a high visibility. As part of a protest against racism, the hacker group Anonymous targeted the website of the Ku Klux Klan, clearly displaying a socio-cultural aim. The reports state that the attacks on WikiLeaks, Donald Trump and Hillary Clinton were targeted on the day the election result was announced, indicating socio-cultural and political motivations for the attack.

The third category (governments) comprises attacks on websites of the Australian, Irish and Italian governments. These attacks were likely performed due to both socio-cultural and political reasons. These government websites did not offer online services to citizens, meaning that their high visibility was likely a more important reason for targeting. From the reports, it follows that the motive for attacking the Australian government website was to interrupt the collection of census data. The reason for the attacks against Italian government websites was a protest against the participation of local bodies in the Trans Adriatic Pipeline project. Again, these attacks were executed by the hacker group Anonymous.

The fourth category (gaming and gambling platforms) includes attacks on online services that offer gambling games or other online games. An Irish lottery website and its associated vending machines were attacked in such a way that it disrupted the sale of lottery tickets. The news reports that covered the event state that at the time of the attack, the lottery jackpot was the highest in 18 months. Thus, the choice of infrastructure was influenced both by high value (the jackpot) and high visibility (many people were expected to purchase lottery tickets). The smart phone game 'Nintendo Pokémon Go' was very popular during the summer of 2016. During this time, the hacker group PoodleCorp attacked the servers of this game. Thus, high visibility appeared to be the main motive for the targeted infrastructure. The hacker group took responsibility for the attack, giving them the ability to showcase their abilities and generating plenty of publicity. Shortly after this attack had occurred, it was reported that the American game producer Blizzard Entertainment was under attack. This strike made the servers for the popular online game Warcraft inaccessible to the people that played it. The short time span between these attacks might also support the notion that DDoS attacks tend to be clustered over time.

The fifth category (internet service providers and hosting service providers) consists of attacks on various providers. In September and October 2016, massive attacks on web hosting provider OVH and DNS service provider Dyn were reported. There were also reported attacks on internet service providers in India. Due to their size and protective measures, internet service providers are a difficult target for DDoS attacks, displaying high inertia. At the same time they are high visibility as they form the backbone of the internet infrastructure. The massive attacks on OVH and Dyn were made possible by the botnet 'Mirai' that was based on the Internet of Things [57]. Its code was released online not long before the assaults, enabling successful attacks on even high inertia targets. Over the course of time multiple actors including hacktivism groups have taken credit for these attacks [58]. This shows that DDoS attacks on high visibility targets are used by groups to attract attention to their ideological agenda. On the other hand reports have also indicated that these attacks may even be initiated by *script kiddies* [59], in which case bringing down a high inertia network infrastructure could be taken as a challenge by these kids.

Finally, the sixth category (financial institutions) includes the attack on the British HSBC Bank, targeting its online banking services. The attack was launched during the last Friday of the month, on which salaries to employees are usually paid out. The timing of the attack therefore clearly suggests an underlying economic motive. This attack constitutes another example in our dataset for which the routine period affects the value of the infrastructure.

We conclude this section with some generic insights derived from the analysis. Although the number of events studied is too small to draw robust conclusions, we try to derive some tentative insights from the numbers. We find that in 16 out of 27 events, economic motives were at least one of the probable aims in selecting a victim. The data clearly shows that socio-cultural and political aims are important as well, even though economic aims remain the primary motives. With respect to infrastructure targeting, accessibility is the main driver that instigates crime opportunity. Only in four cases, the accessibility of the infrastructure was low. High value and low inertia also increase the likelihood of being targeted; the former is especially sensible when combined with economic motives of targeting a victim. With respect to visibility, the analysis shows mixed results, yet there appears to be a positive link between socio-cultural/political motives for victim targeting and high visibility of the targeted infrastructure. When motives are of a purely financial nature, visibility appears to be less important. We reiterate that, despite causal explanations existing for several links between victim targeting and infrastructure targeting, the sample size of this study is small.

5 Conclusions

In this article, we propose a novel hybrid model to analyze the motives of attackers that perform DDoS attacks. The model combines theories from several crime opportunity theories and tailors them towards the domain of DDoS attacks. To evaluate the reasons for selecting a victim, we make use of socio-cultural, economic and political (SPEC) dimensions. For the choice of target infrastructure, we utilize the dimensions of value, inertia, visibility and accessibility (VIVA).

Using the Google Alerts service, we constructed a dataset of eventful days that occurred in the year 2016. We filter the days with the most news alerts (the top 20 percentile) with respect to DDoS attacks to sample a relevant dataset. Subsequently, we apply the proposed model to this dataset to evaluate the attacker's motives for targeting specific victims and infrastructures. Our main conclusions from the analysis may be summarized as follows:

- By utilizing news articles, it is possible to position DDoS attacks into an appropriate context. By applying the proposed hybrid model, we may evaluate decisions made by attackers in the selection of both victims and infrastructures.

- Not all attackers are interested in personal financial gains. For this reason, it is imperative that companies monitor the socio-cultural, economic and political environment at all times.

- Every infrastructure that is connected to the internet is vulnerable to DDoS attacks. Companies should be aware of the degree to which their infrastructures are visible and accessible.

- Intuitively, high value infrastructures are more likely to attract attacks due to economic reasons. Our analysis shows high value and low inertia increases the likelihood of being targeted. Hence, organizations should identify high value infrastructures and protect them against DDoS attacks.

- Attacks on high inertia targets – such as internet service providers – imply that in some cases attackers may target infrastructures simply for the challenge and to showcase their capabilities.

- As indicated by the various dimensions of both victim and infrastructure that may trigger an attack, a holistic perspective is imperative to accurately map threats and take appropriate protective measures against DDoS attacks.

This study only utilizes data from the year 2016, yielding a relatively small data set. For this reason, we cannot derive finite conclusions on how often attackers are motivated by a particular aim. A natural direction for future research would be to analyze a larger and more representative sample of reported attacks that spans multiple years. By applying the dataset construction method as proposed in this model, such larger datasets could be generated in a consistent manner. A next step would be to automate the procedure, using machine learning approaches on news articles that report on DDoS attacks in combination with other datasets (e.g. network data on DDoS attacks) to automatically deduce attacker aims.

Appendix A Complete list of identified events.

Date	News Item	Event Type	Query Keywords
13-1-2016	Europol arrests key suspects of DD4BC extortion group.	Related News	
13-1-2016	Attack on Nissan website.	Attack Event	nissan
22-1-2016	Attack on Irish lottery site and ticket machines.	Attack Event	irish, lottery
22-1-2016	Attack on Irish government websites.	Attack Event	irish, govt
29-1-2016	Kaspersky lab released a report on DDoS attacks.	Related News	
29-1-2016	Attack on HSBC online banking.	Attack Event	hsbc
25-2-2016	Google's Project Shield starts protecting news websites.	Related News	
26-2-2016	Attack on Italian government websites.	Attack Event	italian, government
24-3-2016	US to charge Iran for attacks against banks.	Related News	
7-4-2016	Github suffers major outage.	Related News	
26-4-2016	Attack on KKK website.	Attack Event	kkk
20-7-2016	Attack on Pokémon Go.	Attack Event	pokemon
3-8-2016	Attack on Blizzard's servers.	Attack Event	blizzard
11-8-2106	DDoScoin is introduced.	Related News	
11-8-2016	Attack on Australian Census Website.	Attack Event	australian, census
12-8-2016	Attack on Australian Census Website.	Related News	
1-9-2016	EA Sports servers suffer DDoS attack.	Attack Event	ea, sports, battlefield
13-9-2016	Two teens from Israel arrested for running a booter website. Vdos gets taken down.	Related News	
14-9-2016	Two teens from Israel arrested for running a booter website. Vdos gets taken down.	Related News	
23-9-2016	Attack on Brian Kreb's website.	Attack Event	brian, kreb, website
23-9-2016	IBM held responsible for failing the attack on Australian Census Website.	Related News	
23-9-2016	Ethereum network under computational DDoS attack.	Attack Event	ethereum

(to be continued on next page)

Date	News Item	Event Type	Query Keywords
26-9-2016	Hijacked IOT devices used for the attacks.	Related News	
26-9-2016	Google saves Brian Kreb's website.	Related News	
29-9-2016	Attack on hosting provider OVH.	Attack Event	ovh, hosting
29-9-2016	Hijacked IOT devices used for the attacks.	Related News	
5-10-2016	Mirai IOT malware responsible for attack on Brian Kreb's website.	Related News	
5-10-2016	Feds accuse two 19-year olds for lizard stresser and poodlecorp.	Related News	
7-10-2016	Feds accuse two 19-year olds for lizard stresser and poodlecorp.	Related News	
7-10-2016	Reports on Mirai botnet.	Related News	
13-10-2016	Reports on Mirai botnet.	Related News	
13-10-2016	Singtel and Akamai announce strategic partnership to fight DDoS attacks.	Related News	
18-10-2016	Attacks on ISPs in India.	Attack Event	mumbai, pune
21-10-2016	Attack on Dyn.	Attack Event	dyn
24-10-2016	New World Hackers take responsibility for Dyn attack.	Related News	
24-10-2016	Reports on Dyn attack.	Related News	
25-10-2016	Xiongmai recalls 10000 webcams.	Related News	
25-10-2016	Reports on Dyn attack.	Related News	
27-10-2016	Reports on Dyn attack.	Related News	
27-10-2016	Attack on StarHub broadband.	Attack Event	starhub
1-11-2016	Reports on StarHub attack.	Related News	
1-11-2016	British Teen charged for Spamhaus attack. 2013.	Related News	
1-11-2016	Reports on Dyn attack.	Related News	
2-11-2016	William Hill website under attack.	Attack Event	william, hill
3-11-2016	Reports on Mirai botnet.	Related News	
8-11-2016	Canadian migration website attacked.	Attack Event	canadian, migration
8-11-2016	Attack against WikiLeaks.	Attack Event	wikileaks

(to be continued on next page)

Date	News Item	Event Type	Query Keywords
8-11-2016	Attempted DDoS against Trump and Clinton's website.	Attack Event	trump, clinton
16-11-2016	Reports on IOT security.	Related News	
22-11-2016	Oracle buys Dyn.	Related News	
23-11-2016	Reports on Oracle acquiring Dyn.	Related News	
29-11-2016	Eir's email system under attack.	Attack Event	eir
29-11-2016	Attack on Deutsche Telekom.	Attack Event	deutsche, telekom
30-11-2016	Attack against European Commission.	Attack Event	european, commission
1-12-2016	AWS launches shield against DDoS attacks.	Related News	
7-12-2016	Hackers gamify DDoS attacks.	Related News	
7-12-2016	New Mirai variant infecting home routers.	Related News	
13-12-2016	UK police crack down on people paying for DDoS attacks.	Related News	
15-12-2016	FBI bust Indian student for conducting DDoS attacks.	Related News	
15-12-2016	Attack on Black Lives Matter website.	Attack Event	black, lives, matter
15-12-2016	BTC exchange taken down by an attack.	Attack Event	btc, exchange
16-12-2016	Reports on the attack on BTC.	Related News	
21-12-2016	Attack on Tumblr.	Attack Event	tumblr
23-12-2016	Attack on Steam servers.	Attack Event	steam, servers
29-12-2016	Student charged for conducting DDoS attacks.	Related News	

References

[1] A. Abhishta, "The blind man and the elephant: Measuring economic impacts of ddos attacks," Ph.D. dissertation, University of Twente, December 2019.

[2] M. Innes, "Investigation order and major crime inquiries," in *Handbook of criminal investigation*. Willan Publishing Cullompton, 2007, ch. 10, pp. 255–276.

[3] A. Abhishta, M. Junger, R. Joosten, and L. J. Nieuwenhuis, "A note on analysing the attacker aims behind ddos attacks," in *Proc. of the 2019 International Symposium on Intelligent and Distributed Computing (IDC'19), Petersburg, Russia*. Springer, Cham, October 2019, pp. 255–265.

[4] A. Hutchings and R. Clayton, "Exploring the provision of online booter services," *Deviant Behavior*, vol. 37, no. 10, pp. 1163–1178, May 2016.

[5] R. A. Paulson and J. E. Weber, "Cyberextortion: an overview of distributed denial of service attacks against online gaming companies," *Issues in Information Systems*, vol. 7, no. 2, pp. 52–56, January 2006.

[6] J. Nazario, "Politically motivated denial of service attacks," *The Virtual Battlefield: Perspectives on Cyber Warfare*, pp. 163–181, 2009.

[7] M. Sauter, ""LOIC Will Tear Us Apart": The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks," *American Behavioral Scientist*, vol. 57, pp. 983–1007, March 2013.

[8] L. E. Cohen and M. Felson, "Social change and crime rate trends: A routine activity approach," *American Sociological Review*, vol. 44, no. 4, pp. 588–608, August 1979.

[9] M. Felson, *Crime and nature*. Sage publications, March 2006.

[10] D. B. Cornish and R. V. Clarke, *The reasoning criminal: Rational choice perspectives on offending*. Taylor & Francis Group, 2017.

[11] R. V. G. Clarke, *Situational crime prevention*. Criminal Justice Press, 1997.

[12] M. Felson and R. L. Boba, *Crime and everyday life*. Pine Forge Press, 2016.

[13] B. W. Reyns, "Routine activity theory and cybercrime: A theoretical appraisal and literature review," in *Technocrime and criminological theory*. Routledge, 2017, ch. 3, pp. 35–54.

[14] R. V. Clarke, "Opportunity makes the thief. really? and so what?" *Crime Science*, vol. 1, no. 3, pp. 1–9, December 2012.

[15] N. Tilley, A. Sidebottom, M. Krohn, and J. Lane, "Routine activities and opportunity theory," in *The handbook of juvenile delinquency and juvenile justice*. Wiley Online Library, May 2015, ch. 21.

[16] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks," *IEEE communications surveys & tutorials*, vol. 15, no. 4, pp. 2046–2069, March 2013.

[17] S. Liu and B. Cheng, "Cyberattacks: Why, what, who, and how," *IT professional*, vol. 11, no. 3, pp. 14–21, May 2009.

[18] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu, and P. Laplante, "Dimensions of cyber-attacks: Cultural, social, economic, and political," *IEEE Technology and Society Magazine*, vol. 30, no. 1, pp. 28–38, March 2011.

[19] A. C. Sharma, R. A. Gandhi, W. Mahoney, W. Sousan, and Q. Zhu, "Building a social dimensional threat model from current and historic events of cyber attacks," in *Proc. of the 2nd IEEE International Conference on Social Computing, Minneapolis, Minnesota, USA*. IEEE, August 2010, pp. 981–986.

[20] K. Geers, D. Kindlund, N. Moran, and R. Rachwald, "World war c: Understanding nation-state motives behind today's advanced cyber attacks," October 2013.

[21] S. Kumar and K. M. Carley, "Understanding ddos cyber-attacks using social media analytics," in *Proc. of the 14th IEEE Conference on Intelligence and Security Informatics (ISI'16), Tucson, Arizona, USA*. IEEE, September 2016, pp. 231–236.

[22] A. Abhishta, R. Joosten, M. Jonker, W. Kamerman, and L. J. Nieuwenhuis, "Poster: Collecting contextual information about a ddos attack event using google alerts," in *Proc. of the 40th IEEE Symposium on Security and Privacy (S&P'19), San Francisco, California, USA*. IEEE, May 2019.

[23] R. Poynder, "Lexis-nexis: Past and future," *Online and CD-Rom Review*, vol. 22, no. 2, pp. 73–80, February 1998.

[24] G. M. Steede, C. Meyers, N. Li, E. Irlbeck, and S. Gearhart, "A content analysis of antibiotic use in livestock in national us newspapers," *Journal of Applied Communications*, vol. 103, no. 1, pp. 1–18, 2019.

[25] N. Kallus, "Predicting crowd behavior with big public data," in *Proc. of the 23rd International Conference on World Wide Web (WWW'14), Seoul, Korea*. ACM, April 2014, pp. 625–630.

[26] A. Abhishta, M. Junger, R. Joosten, and L. J. Nieuwenhuis, "Victim routine influences the number of ddos attacks: Evidence from dutch educational network," in *Proc. of the 2019 IEEE Security and Privacy Workshops (SPW'19), San Francisco, California, USA*. IEEE, May 2019, pp. 242–247.

[27] M. Yar, "The novelty of 'cybercrime': An assessment in light of routine activity theory," *European Journal of Criminology*, vol. 2, no. 4, pp. 407–427, October 2005.

[28] I. Kotenko and A. Chechulin, "A cyber attack modeling and impact assessment framework," in *Proc. of the 2013 5th International Conference on Cyber Conflict (CYCON'13), Tallinn, Estonia*. IEEE, June 2013, pp. 1–24.

[29] S. D. Johnson, “A brief history of the analysis of crime concentration.” *European Journal of Applied Mathematics*, vol. 21, no. 4-5, pp. 349–370, October 2010.

[30] “Anonymous takes down nissan website in protest of japanese whale killings,” http://www.businessinsider.com/anonymous-attacks-nissan-website-to-protest-japanese-whale-killings-2016-1 [Online; accessed on June 15, 2020], January 2016.

[31] “Irish lottery site and ticket machines hit by ddos attack,” http://www.bbc.com/news/technology-35373890 [Online; accessed on June 15, 2020], January 2016.

[32] “Govt websites forced offline in ddos attack,” http://www.rte.ie/news/2016/0122/762161-cyber-attack [Online; accessed on June 15, 2020], January 2016.

[33] “Hsbc online banking is ’attacked’,” http://www.bbc.com/news/business-35438159 [Online; accessed on June 15, 2020], January 2016.

[34] “Anonymous attacks italian government portals because of gas pipeline project,” http://news.softpedia.com/news/anonymous-attacks-italian-government-site-because-of-gas-pipeline-project-500977.shtml [Online; accessed on June 15, 2020], February 2016.

[35] “Hacker group anonymous shuts down kkk website,” http://www.telegraph.co.uk/technology/2016/04/25/hacker-group-anonymous-shuts-down-kkk-website/ [Online; accessed on June 15, 2020], April 2016.

[36] “Pokemon go down: Hacking group claims credit for taking down servers ’with ddos attack’,” http://www.independent.co.uk/life-style/gadgets-and-tech/gaming/pokemon-go-down-servers-ddos-attack-hackers-poodlecorp-game-unavailable-a7140811.html [Online; accessed on June 15, 2020], July 2016.

[37] “Blizzard hit with another ddos attack, overwatch, wow, hearthstone and more down,” https://www.technobuffalo.com/2016/08/23/blizzard-ddos-battlenet-down-august-23-sombra-theory/ [Online; accessed on June 15, 2020], August 2016.

[38] “Australian 2016 census sabotage puts a question mark on private cloud,” http://www.computerweekly.com/news/450302728/Australian-2016-census-sabotage-puts-a-question-mark-on-private-cloud [Online; accessed on June 15, 2020], August 2016.

[39] “Battlefield 1 beta: You have lost connection to ea servers,” http://www.pcgameshardware.de/Battlefield-1-2016-Spiel-54981/News/Beta-Server-down-Verbindungsabbrueche-DDOS-1206368/ [Online; accessed on June 15, 2020], February 2016.

[40] “Krebsonsecurity hit with record ddos,” https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/ [Online; accessed on June 15, 2020], 2016.

[41] “Ethereum’s network is currently suffering from a computational ddos attack,” http://www.ibtimes.co.uk/ethereum-network-hit-by-computational-ddos-attack-1582935 [Online; accessed on June 15, 2020], September 2016.

[42] “Web host hit by ddos of over 1tbps.” http://www.infosecurity-magazine.com/news/web-host-hit-by-ddos-of-over-1tbps/ [Online; accessed on June 15, 2020], September 2016.

[43] “Internet providers claim cyber attack, to meet senior cop.” http://www.nyoooz.com/mumbai/635360/internet-providers-claim-cyber-attack-to-meet-senior-cop [Online; accessed on June 15, 2020], 2016.

[44] “Dyn statement on 10/21/2016 ddos attack,” http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/ [Online; accessed on June 15, 2020], September 2016.

[45] “Ddos attacks caused starhub broadband outages.” http://www.telecomasia.net/content/ddos-attacks-caused-starhub-broadband-outages [Online; accessed on June 15, 2020], October 2016.

[46] “William hill website under siege from ddos attacks.” http://www.theregister.co.uk/2016/11/02/william_hill_ddos/ [Online; accessed on June 15, 2020], 2016.

[47] “Donald trump sweeping american polls, canadian migration website down.” http://www.techworm.net/2016/11/donald-trump-sweeping-american-polls-canadian-migration-website.html [Online; accessed on June 15, 2020], November 2016.

[48] “Wikileaks comes under ’unrelenting’ cyber attack that briefly prevents it from releasing more emails linked to hillary clinton on election day.” http://www.dailymail.co.uk/news/article-3917996/WikiLeaks-comes-unrelenting-cyber-attacks-briefly-prevented-releasing-emails-linked-Hillary-Clinton-Americans-polls-Election-Day.html [Online; accessed on June 15, 2020], November 2016.

[49] "Presidential candidate websites targeted." http://techaeris.com/2016/11/08/presidential-candidate-websites-targeted-unsophisticated-ddos-attacks/ [Online; accessed on June 15, 2020], November 2016.

[50] "Eir's webmail affected by ddos attack." https://www.rte.ie/news/business/2016/1125/834480-eirs-webmail-affected-by-ddos-attack/ [Online; accessed on June 15, 2020], 2016.

[51] "Failed mirai botnet attack downed 900000 germans' internet access." https://www.siliconrepublic.com/enterprise/mirai-botnet-deutsche-telekom [Online; accessed on June 15, 2020], November 2016.

[52] "European commission hit by ddos attack," https://www.infosecurity-magazine.com/news/european-commission-hit-by-ddos/ [Online; accessed on June 15, 2020], November 2016.

[53] "The ddos vigilantes trying to silence black lives matter," https://arstechnica.com/security/2016/12/hack_attacks_on_black_lives_matter/ [Online; accessed on June 15, 2020], December 2016.

[54] "Bitcoin exchange btc-e resumes services after latest ddos attack." https://www.cryptocoinsnews.com/bitcoin-exchange-btc-e-resumes-services-latest-ddos-attack/ [Online; accessed on June 15, 2020], December 2016.

[55] "Tumblr goes down after hacker attack." http://news.softpedia.com/news/tumblr-goes-down-after-hacker-attack-511251.shtml [Online; accessed on June 15, 2020], December 2016.

[56] "Steam connection servers down in probable ddos attack." http://www.pcinvasion.com/steam-connection-servers-probable-ddos-attack [Online; accessed on June 15, 2020], December 2016.

[57] A. Abhishta, R. van Rijswijk-Deij, and L. J. Nieuwenhuis, "Measuring the impact of a successful ddos attack on the customer behaviour of managed dns service providers," *ACM SIGCOMM Computer Communication Review*, vol. 48, no. 5, pp. 70–76, January 2019.

[58] E. Geller and T. Romm, "Wikileaks supporters claim credit for massive u.s. cyberattack, but researchers skeptical," https://www.politico.com/story/2016/10/websites-down-possible-cyber-attack-230145 [Online; accessed on June 15, 2020], 2016.

[59] N. Lomas, "Dyn dns ddos likely the work of script kiddies, says flashpoint," https://techcrunch.com/2016/10/26/dyn-dns-ddos-likely-the-work-of-script-kiddies-says-flashpoint/ [Online; accessed on June 15, 2020], October 2016.

Author Biography

Abhishta Abhishta is an assistant professor of Finance and Cyber Risk Management at the department of Industrial Engineering and Business Information Systems at the University of Twente. He received his Ph.D. degree at University of Twente in security economics. His doctoral research was funded by the Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) under award number: 628.001.018. His research focuses on empirically measuring the economic impact caused by cyber attacks to help organisations make better investments in cyber security.

Wouter van Heeswijk is an assistant professor at the University of Twente, the Netherlands. He holds a master's degree in Financial Engineering and obtained his Ph.D. in Operations Research in 2017. As a researcher, he has been affiliated to the National Research Center for Mathematics and Computer Science (CWI) in Amsterdam and to the Technical University of Denmark (DTU) in Kongens Lyngby. Wouter is currently active in the domains of Financial Engineering and Operations Research, focusing his research activities primarily on the application of reinforcement learning in aforementioned domains.

Marianne Junger is a professor of Cyber Security and Business Continuity at the University of Twente. Her research investigates the human factors of fraud and of cybercrime, more specifically she investigates victimization, disclosure and privacy issues. The aim of her research is to develop interventions that will help to protect users against social engineering and to increase compliance. She is a member of the Scientific Advisory Council (WAR) of the Dutch Defense Academy. She founded the Crime Science journal together with Pieter Hartel and was an associate-editor for 6 years (`https://crimesciencejournal.springeropen.com/`). Her research was sponsored, among others, by the Dutch Police, a EU grant and ZonMw (for health research). She published more than 270 scientific publications, including books and journals.

Lambert J. M. Nieuwenhuis is full professor at the Department of High-Tech Business and Entrepreneurship of the Faculty of Behavioral, Management and Social sciences (BMS) of the University of Twente (UT). He is chair of the Research Group Entrepreneurship, Strategy & Innovation Management (NIKOS) and member of the Research Group Business Information Systems and Industrial Engineering. He is owner of the consultancy firm Knowledge for Business. Professor Nieuwenhuis graduated (cum laude) as an Electrical Engineer at the UT. From 1980 to 2001, he worked for the R&D organization of KPN, the telecom operator in The Netherlands. In 1991 while working for KPN, he received a PhD degree in Computer Science for his research on fault tolerant computing. Bart Nieuwenhuis was project leader of several European public-private research programs. In 1995, Dr Nieuwenhuis was appointed as full professor at the University of Groningen. In 2000, he continued his academic career at the University of Twente to work on open distributed service platforms at the Computer Science Faculty. Since 2001, professor Nieuwenhuis is working for consultancy firms in assignments for both public and private organizations. In 2007, he founded his own consultancy firm. In the same year, he accepted a new full professor position at the BMS Faculty to do research and lecturing on Business and IT Services.

Reinoud Joosten is an assistant professor at the Industrial Engineering and Business Information Systems department of the University of Twente, The Netherlands. He obtained his Ph.D. from Maastricht University in 1996. He spent several years as a Post Doc at Maastricht University and the Max Planck Institute for Economics in Jena, Germany. He has been at the University of Twente since 2001. His research interests include game theory, operations research, economics, finance, and more specifically: strategic and economic aspects of DDoS attacks. He is an advisory editor of the Journal of Evolutionary Economics.