A Note on Analysing the Attacker Aims Behind DDoS Attacks

Abhishta Abhishta, Marianne Junger, Reinoud Joosten and Lambert J. M. Nieuwenhuis

Abstract DDoS attacks pose a serious threat to the availability of online resources. In this paper, we analyse the attacker aims for the use of DDoS attacks. We propose a model that can be used to evaluate news articles for determining probable aims of attackers. Thereafter, we apply this model to evaluate 27 distinct attack events from 2016. We make use of a DDoS specific longitudinal news database to select these attack events. We find the proposed model useful in analysing attack aims. We also find that in some cases attackers might target a web infrastructure just because it is virtually invincible.

1 Introduction and Background

Today availability of internet and internet based services is of great importance to all. Malicious actors use cyber attacks to disrupt the normal functioning of internet or to steal digital information. These cyber attacks lead to direct or indirect financial losses [2] for the victimised firms or attacked individuals. Distributed denial of service (DDoS) is one such cyber attack that is used to make web based services inaccessible to the intended user. In order to protect itself a firm needs to evaluate its vulnerabilities and threats so as to plan its defence strategy [20]. These threats can be realised by acknowledging the various reasons for which the firm's IT in-

Abhishta Abhishta
University of Twente, The Netherlands e-mail: `s.abhishta@utwente.nl`

Marianne Junger
University of Twente, The Netherlands, e-mail: `m.junger@utwente.nl`

Reinoud Joosten
University of Twente, The Netherlands, e-mail: `r.a.m.g.joosten@utwente.nl`

Lambert J. M. Nieuwenhuis
University of Twente, The Netherlands, e-mail: `l.j.m.nieuwenhuis@utwente.nl`

frastructure might become a target. Hence, it is important to investigate the aims of attackers for the use of DDoS attacks.

Fig. 1 Aspects of a DDoS Attack

A conventional crime has three aspects that need to be proven before a wrongdoing is determined: Means, Motive and Opportunity. Just like conventional crimes, DDoS attacks require a means to execute, a motive to select the target and an opportunity to attack. In this case, *means* refers to the attack tools or the necessary technical expertise needed to execute the attack, the aim of the attacker points towards the reason for the attacker to act and vulnerabilities in the network provide the opportunity for the attack. Figure 1 shows the three aspects of a DDoS attack.

In this paper, we focus on analysing attacker aims for the use of DDoS attack. The obvious way to investigate the aims of attackers is to interview them. However, it is also possible to model the probable aims based on the information reported by journalists in news articles related to the attack event. Taking into account the socio-cultural, political and economic dimensions of DDoS attacks and the postulates of routine activity theory (RAT), we propose a model to analyse the content of news articles related to an attack. We then use this model to analyse probable attacker aims in 27 different cases from 2016.

2 Previous Works

A few studies have tried to evaluate the attacker aims behind DDoS attacks. Hutchings & Clayton [24] discuss the incentives for booter owners. Paulson & Webber [34] evaluate the use of DDoS attacks for extortion against online gaming companies. Nazario [33] discuss politically motivated DDoS attacks. Later, Sauter [37] highlights the use of DDoS attacks for hacktivism purposes. Finally Zargar *et al.* [46] listed the probable incentives for attackers to use DDoS attacks as follows:

1. Financial/economical gain: This is the motive when an attacker gets paid for the assault.
2. Revenge: The motive of an attacker in this category is to DDoS for retribution.

3. Ideological belief: The attackers in this category attack usually as a portrayal of disagreement.
4. Intellectual Challenge: The attackers in this category experiment and learn from their activities. They are usually hackers who wish to show off their capabilities.
5. Cyber warfare: The attackers in this category belong usually to a military or terrorist group.

However, Zargar *et al.* [46] do not provide any evidence for most of the listed motives. Some other studies also evaluated the non-technical characteristics of cyber attacks as a whole. Liu & Cheng [32] discuss the reasons for cyber attacks to happen. They also explain who these attackers are and how they conduct these attacks. Gandhi *et al.* [18] discuss the socio-cultural, political and economic (SPEC) dimensions of cyber attacks. They analyse selected security events between 1996 and 2010 on the basis of SPEC criteria. Sharma *et al.* [38] proposed a social dimensional threat model by using historical cyber attack events. On the basis of their model they evaluate 14 different news articles concerning cyber attacks. Geers *et al.* [19] analyse the nation-state motives behind cyber attacks. Kumar & Carley [30] used network analysis on the data from Arbor network's digital attack map and World Bank to study the aims behind DDoS attacks. They conclude that there is an increase in the probability of attacks on the country if there are negative sentiments towards the country on social media.

All of the above mentioned studies show that not all attacks are carried out for economic gains. As booters have made DDoS attacks an easy weapon for nearly everyone, a number of aims can trigger attackers to launch an attack. These studies either evaluate the aims of attackers with respect to the SPEC criteria, or assume an aim and provide evidence to show the relevance of the aim in certain attacks. We believe that in case of DDoS attacks, attackers have to make two choices; 1) The victim (company or the individual they wish to attack). 2) Network infrastructure of the victim they wish to target. We propose a hybrid strategy for evaluating attacker aims by analysing the victim with respect to SPEC criteria and analysing the choice of infrastructure by considering the postulates of routine activity theory.

3 Methodology

Here, we discuss the characteristics of the dataset and the sampling strategy used by us to extract DDoS attack events. We then explain the proposed model for content analysis of news articles.

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

3.1 Dataset and Sampling

The dataset is a collection of *Google Alerts* on DDoS attacks¹. The collection process and some possible uses of the dataset are mentioned by Abhishta *et al.* [1]. Table 1 shows the characteristics of the dataset used in this research.

In this paper, we are looking for a sample of DDoS attack events that were discussed at length in the media. Hence, the goal of sampling is to extract the most reported DDoS attacks of 2016. We divide event sampling process into two parts: (1) We identify *eventful* days (2) We evaluate the ‘News’ alerts of an eventful day to extract attack events.

Fig. 2 Histogram depicting selection criterion for *eventful* days.

The statistical criteria for identification of ‘eventful days’ is based on the methodology also used by Kallus [28]. We consider the days on which the number of alerts were greater than θ as ‘eventful’. In order to calculate the threshold θ we make use of the empirical distribution of number of alerts generated each day. Figure 2 shows the empirical distribution of number of ‘News’ alerts that are generated daily over the year. In this paper, we consider the threshold to be at 20 percentile. If we consider top 10 percentile of the alerts than most of the eventful days lie in the second half of 2016 this is due to an enormous increase in reporting of DDoS attacks in the later half of the year. In this case, θ is calculated to be at 31.92 alerts. *Thus, if in a single day greater than or equal to 32 ‘News’ alerts are reported then we consider that as an eventful day.* With this method, we are able to select 43 *eventful* days. We consider the alerts generated on *eventful* days for our study.

¹ Google Alerts is a content change detection and notification service. A user of this service can keep themselves updated about the topic of their choice. The service notifies with two types of alerts: 1) News 2) Web. News alerts report about content posted on news websites, all others are categorised as web alerts.

Fig. 3: Attack time-line showing the extracted attack events for $\theta = 32$

In order to identify the events responsible for the generation of abnormally high number of alerts on *eventful* days, we evaluate the text of all alerts on an *eventful* day and record the reported events as DDoS related events (non-attack) and DDoS attack events. We find that these news alerts report either an attack or an activity associated to an attack e.g. a research report by a DDoS protection company, or steps taken by law enforcement agencies. We manually tag the content of the alerts on selected days to identify attack reporting alerts. The extracted attack events are shown in Figure 3. For this research we only consider the articles reporting a DDoS attack. We identify 27 separate attack events being discussed in these news articles.

3.2 Content Analysis

The decision of the attacker to choose a target for a DDoS attack can be broken down in the following two components: 1) Choice of victim organisation to target. 2) Choice of network infrastructure to target. Figure 4 shows the model followed by us to analyse attacker aims. In Gandhi *et al.* [18] have shown that social, political, economic and cultural circumstances influence the choice of victim for an attacker. Hence, we evaluate the attacker's choice of victim using the SPEC criteria suggested by Gandhi *et al.*. For the choice of network infrastructure, we assume that the attackers are rational i.e. the attacker choose to launch an attack [10]. This assumption enables us to make use of the postulates of RAT. According to Cohen and Felson's (1979) [9] routine activities theory, direct contact predatory victimization occurs with the convergence in both space and time of three components: a motivated offender, the absence of a capable guardian, and a suitable target. According to routine activity theory, the suitability of a infrastructure for predation can be estimated using its four-fold constituent properties: value, inertia, visibility and accessibility, usually rendered in the acronym VIVA [45]. VIVA dimensions can be described as follows:

Value This refers to the importance of the infrastructure to the victim. For example, depending on the online sales of a company, a website can be more or less valuable to the company.

Fig. 4: Model for analysing attacker aims using news articles

- Inertia** Inertia refers to the degree of resistance posed by the infrastructure to an effective predation. So, high inertia infrastructure will be the ones employing better protection strategies against DDoS attacks or the ones that can sustain high intensity network traffic (e.g. distributed servers, websites hosted in the cloud etc.).
- Visibility** Visibility refers to the visibility of the objects an offender wishes to steal [31]. High visibility web infrastructures are mostly public facing such as, a public website.
- Accessibility** It refers to the ability of an offender to get to the target and get away from the scene of crime. An example of a high accessibility infrastructure can be servers whose `ip address` can be easily accessed and are setup without intrusion detection systems or network monitoring applications.

With the help of the concepts discussed above, we develop a model for analysing the probable aims behind attack events. We analyse news articles related to 27 distinct attack events using this model to understand the attacker aims.

4 Results and Discussion

Figure 3 shows the DDoS attack events reported on *eventful* days. As a result of filtering a total of 43 dates were selected as *eventful* days. We evaluate all the alerts on these days and select DDoS attack events on the basis of the criteria mentioned in Section 3.1. The number of alerts collected on *eventful* days is 1929. Hence, these 11.75% of the days of the calendar year account for nearly 43% ((*Number of news*

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	[4]	Nissan Motors	✓			Website	Low	Low	High	High
22/01/2016	[26]	Primier lotteries			✓	Ticket machines and Website	High	Low	High	High
22/01/2016	[21]	Irish government	✓	✓		Website	Low	Low	High	High
29/01/2016	[23]	HSBC			✓	Online Banking Server	High	High	Low	Low
26/02/2016	[3]	Italian government	✓	✓		Website	Low	Low	High	High
26/04/2016	[22]	Ku Klux Klan	✓			Website	Low	Low	High	High
20/07/2016	[35]	Pokemon go			✓	Gaming Server	High	Low	Low	High
03/08/2016	[8]	Blizzard			✓	Gaming Server	High	Low	Low	High
11/08/2016	[5]	Australian Census	✓			Website	High	Low	High	High
01/09/2016	[6]	EA sports			✓	Gaming Server	High	Low	Low	High
23/09/2016	[29]	Brian Kreb		✓		Website	Low	High	High	High
23/09/2016	[15]	Ethereum network			✓	Servers	High	Low	Low	Low
29/09/2016	[42]	OVH			✓	Hosting Server	High	High	Low	High
18/10/2016	[25]	ISPs in India			✓	Network Devices	High	High	Low	High
21/10/2016	[13]	Dyn			✓	Servers	High	High	Low	High
27/10/2016	[11]	StarHub			✓	Network Devices	High	High	Low	High
02/11/2016	[44]	William Hill			✓	Website	High	Low	High	High
08/11/2016	[12]	Canadian migration		✓		Website	Low	Low	High	High
08/11/2016	[43]	Wikileaks		✓		Website	High	Low	High	High
08/11/2016	[36]	Trump and Clinton		✓		Website	Low	Low	High	High
29/11/2016	[14]	Eir			✓	Email Server	High	Low	Low	Low
25/11/2016	[17]	Deutsche Telekom			✓	Network Devices	High	High	Low	High
30/11/2016	[16]	European Commission	✓	✓		Website	Low	Low	High	High
15/12/2016	[40]	Black lives matter	✓			Website	Low	Low	High	High
15/12/2016	[7]	BTC exchange			✓	Servers	High	Low	Low	Low
21/12/2016	[41]	Tumblr			✓	Website	High	Low	High	High
23/12/2016	[39]	Steam			✓	Gaming Servers	High	Low	Low	High

$\text{alerts on eventful days}/(\text{Number of news alerts in the whole year})*100$) of the total ‘news’ alerts. This result supports the findings of Johnson [27] with respect to the concentration of traditional crimes, as traditional crime is also very much concentrated in time and space.

Table 2 summarises the components of each of the selected attack event i.e. victim, attacked infrastructure, SPEC variables and VIVA characteristics of the infrastructure. In the following paragraphs we discuss these attack reports in detail and report our findings in accordance with the criterion discussed in Section 3.2.

In our analysis we see that the selected attack events can be broadly classified in 6 categories: 1) Attacks on large manufacturing companies 2) Attacks targeting public figures and ideological groups 3) Attacks targeting governments 4) Attacks on gaming and gambling platforms 5) Attacks on internet service providers and hosting service providers and 6) Attacks on financial institutions.

The first category includes the attack on Nissan Motors, all the global websites of the automotive company Nissan [4] were reported to suffer downtime. As Nissan does not sell cars online, the website is of relatively low value to the company. However, it was reported that the attack was carried out during Detroit auto show. During auto shows, car manufacturers expect attendants to visit their website to know more about the vehicle. Hence, even though Nissan doesn’t sell cars online, the website has a high visibility during this period. Later reports suggested that Anonymous (hacker group) targeted the website to protest against whale hunting in Japan (justifies choice of the Nissan as a victim). Hence, high visibility of the website was the key input for the choice of target.

The second category include attacks on Ku Klux Klan, website of Brian Krebs, Black Lives Matter, Wikileaks, Donald Trump and Hillary Clinton [22, 29, 40, 36, 43]. The websites of this category of victims are easy targets and have high visibility. As a result of a protest against racism ‘Anonymous’ attacked the website of Ku Klux Klan [22]. According to the reports, websites on Wikileaks, Donald Trump and Hillary Clinton were targeted on the day of election result, showing socio-cultural reasons for the attacks.

The next category comprises of attacks on websites of Irish, Italian and Australian government [3, 21, 5]. These attacks could have been launched for both socio-cultural and political reasons as government websites usually do not cater online services. Italian government websites [3] were targeted by hacker group ‘Anonymous’. The motivation behind the attack was to protest against the participation of local bodies in the Trans Adriatic Pipeline (TAP) project. However, the attack on Australian government website was clearly targeted to interrupt census data collection.

The fourth category includes online gaming platforms and gambling websites. The news sources reported an attack on the Irish lottery website [26] and vending machines that lead to the disruption of the sale of tickets. According to the reports this time the lottery jackpot was the highest in 18 months (*high value*). Hence, more people were expected to buy the tickets (*high visibility*). In July 2016, when the game ‘Nintendo Pokemon Go’ [35] was very popular (*high visibility*), another hacker group ‘PoodleCorp’ attacked the servers of the game. They took responsibility of the attack thus gaining a lot of publicity. Just after this online assault an attack on the servers of blizzard was reported that made the Warcraft servers inaccessible for the gamers.

The fifth category comprises of attacks on ISPs and web hosting providers. In September and October 2016 attacks on ISPs in India [25], OVH (web hosting provider) [42] and Dyn (DNS service provider) [13] were reported. Usually ISPs form a high inertia targets for DDoS attacks. A new internet of things(IOT) based botnet, ‘Mirai’, who’s code was released online was used for these attacks. Each of these attacks were bigger than the other in intensity.

The final category includes the attack on HSBC online banking services. As the attack was launched on last Friday of the month (salary day), the reasons for the attack was clearly economic. This is another example in our sample when the routine period affected the value of the infrastructure.

5 Conclusions and Future Work

In this paper, we propose a model for analysing the attacker aims for using DDoS attacks. This model uses SPEC criteria for evaluating the reasons for choosing the victim and then studies the VIVA characteristics of the choice of infrastructure. We use this model to evaluate news articles related to 27 attack events that were reported in 2016. Our main conclusions are as follows:

- News articles are able to put DDoS attacks in context. Using the proposed model it is possible to evaluate the decisions made by the attacker to choose the victim and infrastructure.
- Companies need to monitor their socio-cultural and political environment at all times, not all attackers look for personal economic gains.
- All infrastructure connected to the internet is vulnerable to DDoS attacks. Companies must be aware of the degree of visibility and accessibility of the infrastructure. They should also consider their routine periods while analysing the VIVA characteristics of the infrastructure.
- Attacks on high inertia targets such as Dyn [13] shows that, sometimes attackers target infrastructures because they are virtually invincible.

In this study, we only use data from 2016, hence we cannot derive conclusions on how often attackers are motivated by a particular aim. In the future, we would like to analyse a larger and more representative sample of all reported attacks. We hope to use the proposed model as a base for automatically detecting attacker aims from news articles reporting DDoS attacks.

Acknowledgements This work is part of the NWO: D3 project, which is funded by the Netherlands Organization for Scientific Research (628.001.018).

References

- [1] Abhishta Abhishta, Reinoud Joosten, Mattijs Jonker, Wim Kamerman, and Lambert J.M. Nieuwenhuis. "Poster: Collecting Contextual Information About a DDoS Attack Event Using Google Alerts". In: 2019. Poster presented at 40th IEEE Symposium on Security and Privacy, San Francisco, CA.
- [2] R. Anderson, C. Barton, R. Bohm, R. Clayton, M. J. G. Van Eeten, M. Levi, T. Moore, and S. Savage. "Measuring the Cost of Cybercrime". In: *Workshop on Economics of Information Security* (2012).
- [3] *Anonymous Attacks Italian Government Portals Because of Gas Pipeline Project*. 2016. URL: <http://news.softpedia.com/news/anonymous-attacks-italian-government-site-because-of-gas-pipeline-project-500977.shtml>.
- [4] *Anonymous takes down Nissan website in protest of Japanese whale killings*. 2016. URL: <http://www.businessinsider.com/anonymous-attacks-nissan-website-to-protest-japanese-whale-killings-2016-1?international=true&r=US&IR=T>.
- [5] *Australian 2016 census sabotage puts a question mark on private cloud*. 2016. URL: <http://www.computerweekly.com/news/450302728/Australian-2016-census-sabotage-puts-a-question-mark-on-private-cloud>.

- [6] *Battlefield 1 Beta: You Have Lost Connection to EA Servers*. 2016. URL: <http://www.pcgameshardware.de/Battlefield-1-2016-Spiel-54981/News/Beta-Server-down-Verbindungsabbrueche-DDOS-1206368/>.
- [7] *Bitcoin Exchange BTC-e Resumes Services after Latest DDoS Attack*. 2016. URL: <https://www.cryptocoinsnews.com/bitcoin-exchange-btc-e-resumes-services-latest-ddos-attack/>.
- [8] *Blizzard hit with another DDoS attack, Overwatch, WoW, Hearthstone and more down*. 2016. URL: <https://www.technobuffalo.com/2016/08/23/blizzard-ddos-battlenet-down-august-23-sombra-theory/>.
- [9] Lawrence E. Cohen and Marcus Felson. "Social Change and Crime Rate Trends: A Routine Activity Approach". In: *American Sociological Review* 44.4 (1979), pp. 588–608.
- [10] Paul Cromwell and James N Olson. "The reasoning burglar: Motives and decision-making strategies". In: *In Their Own Words*. Los Angeles, CA: Roxbury Publishing Company (2006).
- [11] *DDoS attacks caused StarHub broadband outages*. 2016. URL: <http://www.telecomasia.net/content/ddos-attacks-caused-starhub-broadband-outages>.
- [12] *Donald Trump sweeping American Polls, Canadian migration website down*. 2016. URL: <http://www.techworm.net/2016/11/donald-trump-sweeping-american-polls-canadian-migration-website.html>.
- [13] *Dyn Statement on 10/21/2016 DDoS Attack*. 2016. URL: <http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/>.
- [14] *Eir's webmail affected by DDoS attack*. 2016. URL: <https://www.rte.ie/news/business/2016/1125/834480-eirs-webmail-affected-by-ddos-attack/>.
- [15] *Ethereum's network is currently suffering from a computational DDoS attack*. 2016. URL: <http://www.ibtimes.co.uk/ethereum-network-hit-by-computational-ddos-attack-1582935>.
- [16] *European Commission Hit By DDoS Attack*. 2016. URL: <https://www.infosecurity-magazine.com/news/european-commission-hit-by-ddos/>.
- [17] *Failed Mirai botnet attack downed 900000 Germans' internet access*. 2016. URL: <https://www.siliconrepublic.com/enterprise/mirai-botnet-deutsche-telekom>.
- [18] R. A. Gandhi, A. C. Sharma, W. Mahoney, W. Sousan, and Q. Zhu. "Dimensions of cyber-attacks: Cultural, social, economic, and political". In: *IEEE Technology and Society Magazine* 30.1 (2011).
- [19] K. Geers, D. Kindlund, N. Moran, and R. Rachwald. *World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks*. 2013.

- [20] Lawrence A. Gordon and Martin P. Loeb. “The economics of information security investment”. In: *ACM Transactions on Information and System Security* (2002).
- [21] *Govt websites forced offline in DDoS attack*. 2016. URL: <http://www.rte.ie/news/2016/0122/762161-cyber-attack>.
- [22] *Hacker group Anonymous shuts down KKK website*. 2016. URL: <http://www.telegraph.co.uk/technology/2016/04/25/hacker-group-anonymous-shuts-down-kkk-website/>.
- [23] *HSBC online banking is ‘attacked’*. 2016. URL: <http://www.bbc.com/news/business-35438159>.
- [24] Alice Hutchings and Richard Clayton. “Exploring the Provision of Online Booter Services”. In: *Deviant Behavior* 37.10 (2016), pp. 1163–1178. URL: <https://www.tandfonline.com/doi/abs/10.1080/01639625.2016.1169829>.
- [25] *Internet providers claim cyber attack, to meet senior cop*. 2016. URL: <http://www.nyoooz.com/mumbai/635360/internet-providers-claim-cyber-attack-to-meet-senior-cop>.
- [26] *Irish lottery site and ticket machines hit by DDoS attack*. 2016. URL: <http://www.bbc.com/news/technology-35373890>.
- [27] S. D. Johnson. “A brief history of the analysis of crime concentration.” In: *European Journal of Applied Mathematics* 21(4-5) (2010), pp. 349–370.
- [28] Nathan Kallus. “Predicting Crowd Behavior with Big Public Data”. In: *Proceedings of the 23rd International Conference on World Wide Web. WWW ’14 Companion*. Seoul, Korea: ACM, 2014, pp. 625–630.
- [29] *KrebsOnSecurity Hit With Record DDoS*. 2016. URL: <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/>.
- [30] S. Kumar and K. M. Carley. “Understanding DDoS cyber-attacks using social media analytics”. In: *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*. 2016.
- [31] Eric Rutger Leukfeldt and Majid Yar. “Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis”. In: *Deviant Behavior* 37.3 (2016), pp. 263–280. URL: <https://doi.org/10.1080/01639625.2015.1012409>.
- [32] S. Liu and B. Cheng. “Cyberattacks: Why, What, Who, and How”. In: *IT Professional* 11.3 (2009).
- [33] Jose Nazario. “Politically motivated denial of service attacks”. In: *Cryptology and Information Security Series* (2009).
- [34] Richard A. Paulson and James Weber. “Cyberextortion : an Overview of Distributed Denial of Service”. In: (2006).
- [35] *Pokemon Go down: Hacking group claims credit for taking down servers ‘with DDOS attack’*. 2016. URL: <http://www.independent.co.uk/life-style/gadgets-and-tech/gaming/pokemon-go-down-servers-ddos-attack-hackers-poodlecorp-game-unavailable-a7140811.html>.

- [36] *Presidential candidate websites targeted*. 2016. URL: <http://techaeris.com/2016/11/08/presidential-candidate-websites-targeted-unsophisticated-ddos-attacks/>.
- [37] Molly Sauter. ““LOIC Will Tear Us Apart”: The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks”. In: *American Behavioral Scientist* 57 (2013), pp. 983–1007.
- [38] A. C. Sharma, R. A. Gandhi, W. Mahoney, W. Sousan, Q. Zhu, and P. Laplante. “Building a Social Dimensional Threat Model from Current and Historic Events of Cyber Attacks”. In: *2010 IEEE Second International Conference on Social Computing*. 2010.
- [39] *Steam connection servers down in probable DDOS attack*. 2016. URL: <http://www.pcinvasion.com/steam-connection-servers-probable-ddos-attack>.
- [40] *The DDoS vigilantes trying to silence Black Lives Matter*. 2016. URL: https://arstechnica.com/security/2016/12/hack_attacks_on_black_lives_matter/.
- [41] *Tumblr Goes Down After Hacker Attack*. 2016. URL: <http://news.softpedia.com/news/tumblr-goes-down-after-hacker-attack-511251.shtml>.
- [42] *Web Host Hit by DDoS of Over 1Tbps*. 2016. URL: <http://www.infosecurity-magazine.com/news/web-host-hit-by-ddos-of-over-1tbps/>.
- [43] *WikiLeaks comes under 'unrelenting' cyber attack that briefly prevents it from releasing more emails linked to Hillary Clinton on Election Day*. 2016. URL: <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>.
- [44] *William Hill website under siege from DDoS attacks*. 2016. URL: http://www.theregister.co.uk/2016/11/02/william_hill_ddos/.
- [45] Majid Yar. “The Novelty of Cybercrime An Assessment in Light of Routine Activity Theory”. In: *European Journal of Criminology* 2.4 (2005), pp. 407–427.
- [46] S. T. Zargar, J. Joshi, and D. Tipper. “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks”. In: *IEEE Communications Surveys Tutorials* 15 (2013).