Victim Routine Influences the Number of DDoS Attacks: Evidence from Dutch Educational Network

Abhishta Abhishta
University of Twente
s.abhishta@utwente.nl

Marianne Junger
University of Twente
m.junger@utwente.nl

Reinoud Joosten
University of Twente
r.a.m.g.joosten@utwente.nl

Lambert J.M. Nieuwenhuis
University of Twente
l.j.m.nieuwenhuis@utwente.nl

***Abstract*—We study the influence of daily routines of Dutch academic institutions on the number of DDoS attacks targeting their infrastructures. We hypothesise that the attacks are motivated and harness the postulates of Routine Activity Theory (RAT) from criminology to analyse the data. We define *routine periods* in order to group days with similar activities and use 2.5 years of NetFlow alerts data measured by SURFnet to compare the number of alerts generated during each of these periods. Our analysis shows clear correlation between academic schedules and attack patterns on academic institutions. This leads us to believe that most of these attacks are not random and are initiated by someone who might benefit by disrupting scheduled educational activities.**

***Index Terms*—NetFlow Analysis, Routine Activity Theory, DDoS Attacks, Aims.**

I. Introduction

Over the years academic institutions have become more and more dependent on information and communications technology (ICT) to impart education. Today the majority of the assignments submitted by students are via the web and a number of examinations are conducted online. Several e-learning strategies [1] are used by teachers to develop interactive content for students. Hence, ICT has become an indispensable resource for modern day educational institutions.

Network resources form the backbone of communication technologies and are under a constant scare of cyber attacks. Distributed denial of service (DDoS) attacks constantly threaten the availability of network resources. Even attackers with no prior knowledge of cyber attacks can order a DDoS attack using Booters [2]. In recent years several academic institutions have become victim of such attacks [3]. This raises the question: *why academic institutions are being targeted by DDoS attacks? Are these just random attacks on their network infrastructure or do attackers target them in a planned manner?*

In this paper, we answer this question by analysing the timing of attacks that in the past have targeted the network infrastructure of SURFnet[1]. We hypothesise that the attacks are motivated and harness the postulates of Routine Activity Theory (RAT) from criminology to analyse the data.

Many studies in the field of criminology have shown the impact of attacker routines on crime rates [4]. Routine activity theory (RAT) suggests that changes in crime rates should be associated with days that affect the daily routines [5]. Holidays not only have an impact on attacker routines but also the routines of the victim. For instance, in the case of academic institutions all teaching related activities (classes and examinations) are on a halt during holidays. If the attacker's aim is to disrupt teaching related activities by means of a cyber attack then there is no incentive in launching such an attack during holidays. During vacations and weekends no lectures or examinations are scheduled. We leverage this feature of academic institutions to analyse if statistically significant number of attacks are driven by academic routines. We hypothesise that as greater disruption can be caused to academic activities during working days, we would observe more attempted DDoS attacks during this period.

Maimon et al. [6] tested a similar hypothesis using the Intrusion Prevention System (IPS) data of a single university and showed that attacks on university are more likely to happen during business hours. We look to generalise the findings by Maimon et al. by using data collected by SURFnet. As SURFnet provides network services to all academic institutions in The Netherlands, they are able to record all the attacks on Dutch academic institutions. On the basis of our analysis we show:

- how routine activity theory can be used to evaluate the influence of victim routines on attack patterns.
- that most of the attacks on academic institutions are not random. Daily routines of academic institutions heavily influence the rate of attack alerts.
- that the number of denial of service attacks targeting academic institutions in the Netherlands are significantly (statistically) higher during the working hour of working days as compared to holidays.
- that attack patterns do not change significantly (statistically) with type of holidays.

II. Method

The data in this research consists of alerts based on 1/100 sampled netflow using two different software: 1) NfSen [7] 2) Arbor Peakflow [8]. Both software were used to measure different alerts to avoid double counting. The alerts were based on packet rate triggers from both the software and are indicative of an attempted denial of service attack. The data were measured by SURFnet between 12:00:00 a.m. on

[1]SURFnet is the primary supplier of advanced networking to Colleges, universities and research institutions.

DOI 10.1109/SPW.2019.00052

1st January 2015 and 12:00:00 a.m. on 30th June 2017. Thus, we make use of 2.5 years of attack alerts to test our hypotheses.

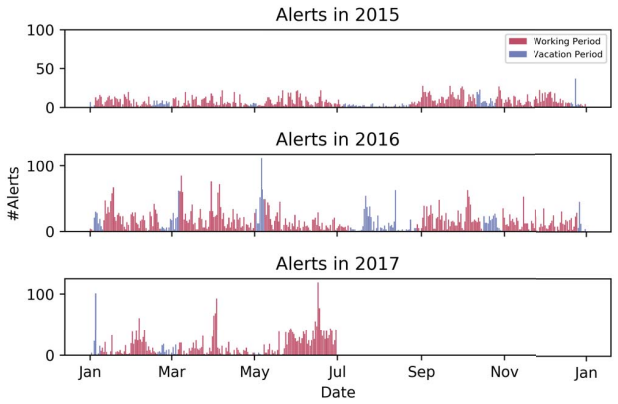


Figure 1: #Alerts collected in Working and Vacation periods.

To analyse the impact of daily routines of academic institutions on the number of denial of service attacks we follow these steps:

- **Step 1:** Define routine periods on the basis of academic calendar.
- **Step 2:** Clean the data by filtering anomalies and exceptions.
- **Step 3:** Group alerts in one hour periods and use dummy variables (1,0) to prepare the dataset for hypothesis testing.
- **Step 4:** Formulate hypotheses using the postulates of RAT.
- **Step 5:** Use an apt statistical method to test the null hypotheses.

In order to prepare data for hypothesis testing, it is important for us to define the *routine periods*. According to the academic calendar [9] in the years 2015, 2016 and 2017 we divide the calendar year in the following routine periods:

- **Winter Vacation:** 1 and 52
- **Spring Vacation:** 8 and 9
- **May Vacation:** 18
- **Summer Vacation:** 28,29,30,31,32,33 and 34
- **Autumn Vacation:** 42 and 43
- **Working Weeks:** All other weeks

On a few occasions there was a week's difference between the start of vacations in the north and other regions of the Netherlands, in such a case we have considered the union of the vacation weeks from all regions as a *routine period*. In total 691 days of data belonged to working weeks and 221 days of data belonged to vacation weeks. We divide each week into *weekdays* and *weekends* (Saturday and Sunday) as the routines of academic institutions will be dissimilar in these periods. We group all the days belonging to the *vacation periods* and weekends as *holiday period* and others as *working period*. Based on this more broad division we get 417 days in the *holiday period* and rest of the 495 days in the *working period*.

In Section II-A we explain the steps taken by us to prepare the dataset, then in Section II-B we formulate our hypotheses and finally explain the statistical test used to test the hypotheses in Section II-C.

Table I: Dataset

Year	#Alerts	#Alerts/day
2015	2780	7.62
2016	6022	16.45
2017	2975	16.44

A. Dataset

Here we discuss the dataset, the assumptions used by us to filter the anomalies in the data and method used to prepare the dataset for hypothesis testing. The 2.5 year long dataset consisted of 13,337 alerts before filtering and 11,777 alerts after filtering for multi-vector attacks and other anomalies. The year-wise distribution of the alerts are shown in Table I. Figure 1 shows the number of alerts collected on each day.The number of attacks substantially increased since 2016. We can see that on an average greater number of alerts were collected in 2016 and 2017 as compared to 2015. However, no changes in measurement systems were carried out by SURFnet.

In order to count multi-vector attacks as a single attack, we merge alerts having the same time-stamp as a single alert. To account for larger attacks that might generate multiple alerts, we merge all alerts where the difference in time-stamps is less than 5 minutes. If we encounter a *Large SYN* alert (alert generated due an oversized SYN packet) followed by *TCP SYN* alerts, then we filter these alerts as it is indicative of an active botnet on SURFnet's network that might have been used to attack some other network infrastructure. In this paper we assume that this filtered dataset provides the number of alerts are representative of the number of attempted denial of service attacks on SURFnet's infrastructure. To prepare the data were then grouped into one-hour periods by calculating the total number of alerts generated each hour.

Dummy variable (1,0) coding was used to assess the differences between each of the *routine periods*. A similar coding was done to distinguish between the larger groups; *holiday period* and *working period*. We also code the dataset to show working and non-working hours of the day. As most educational activities are planned between 8:00 a.m. and 6:00 p.m., we consider these hours as *working hours* and others as *non-working hours*.

B. Hypotheses

Hypothesis testing is required to test the statistical significance of the differences that we might observe with the help of descriptive statistics. In this section we develop the hypotheses and formulate the corresponding null hypotheses that we will test using the dataset described in the previous section. We base all our hypotheses on the following postulate of RAT: *change in victim routines will impact rate of attacks on the victim*. Hence, in case of academic institutions we hypothesize that *routine periods* will impact the number of denial of service attacks targeting their network infrastructure. In total we develop 9 different hypothesis to compare the number of attempted attacks in each of the routine periods.

Table II: Hypotheses and corresponding null hypotheses.

Hypothesis	Null Hypothesis
H1: The average number of attack alerts generated during the *working period* is higher than in the *holiday period*.	$H1_0$: There is no significant difference in the average number of alerts generated during the *working period* and the *holiday period*.
H2: The average number of attack alerts generated during the weekdays of *working weeks* period is higher than in the weekends.	$H2_0$: There is no significant difference in the average number of alerts generated during the weekdays and weekends of *working weeks* period.
H3: There is no significant difference in the average number of alerts generated during the weekdays and weekends of vacation period.	$H3_0$: There is no significant difference in the average number of alerts generated during the weekdays and weekends of vacation period.
H4: The average number of attack alerts generated during the *working weeks* period is higher than in the Vacation *routine periods*.	$H4_0$: There is no significant difference in the average number of alerts generated during *working weeks* period and the Vacation *routine periods*.
H5: There is no significant difference in the average number of alerts generated during the weekends of vacation and *working weeks* period.	$H5_0$: There is no significant difference in the average number of alerts generated during the weekends of vacation and *working weeks* period.
H6: There is no significant difference in the average number of alerts generated during any of the *vacation periods*.	$H6_0$: There is no significant difference in the average number of alerts generated during any of the *vacation periods*.
H7: The average number of alerts generated in the working hours of *working weeks* period are higher than in the non-working hours.	$H7_0$: There is no significant difference in the average number of alerts generated during the working and non-working hours of *working weeks* period.
H8: There is no significant difference in the average number of alerts generated during the working and non-working hours of vacation periods	$H8_0$: There is no significant difference in the average number of alerts generated during the working and non-working hours of vacation periods.
H9: There is no significant difference in the average number of alerts generated during the working and non-working hours on the weekends.	$H9_0$: There is no significant difference in the average number of alerts generated during the working and non-working hours on the weekends.

Table II shows all the hypotheses and the corresponding null hypotheses. The hypothesis is a proposition made on the basis of RAT. The null hypothesis is proposition that assumes no significant difference between the routine periods subjected to a statistical test. Hence, in cases where on the basis of RAT we expect no difference in attack patterns, the hypothesis and the null hypothesis are the same.

For the 1st hypothesis we consider the two large groups: *holiday period* and *working period*. As greater damage can be done to an academic institution when it is a working day. For the second hypothesis we consider the weekdays and weekends of the *working weeks* period. Alternatively, one could also argue that in the vacation weeks statistically there is going to be no difference in the rate of attacks on academic institutions during weekdays and weekends. In case of H3 we test this aspect of the dataset. As vacation *routine periods* and *working weeks* period have contrasting routines for the academic institutions, we formulate 4th hypothesis on this basis. For the 5th hypothesis we compare the number of alerts generated during the weekends of vacation and *working weeks* period. In the 6th hypothesis, we test whether type of vacation period (summer, spring, etc.) has an impact on the number of alerts.

In the next three hypothesis, we analyse the impact of hour of the day on attack pattern. As mentioned in the previous section, we group the hours of a day in working hour and non-working hour category. The routines of academic institution vary during working and non-working hours, there are several other businesses where this might not be the case (e.g. e-commerce). In the 7th hypothesis we analyse the difference in attack patterns during the working and non-working hours on a weekday in the *working weeks* period. Through H8 and H9 we analyse if there is an impact of working and non-working hour categories on the weekend and vacation periods.

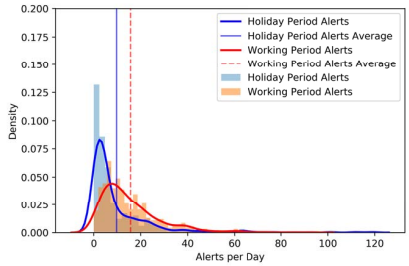
C. Testing

In order to test the null hypotheses we make use of Analysis of variance (ANOVA). Analysis of variance (ANOVA) is a collection of statistical models and their associated estimation procedures (such as the "variation" among and between groups) used to analyse the differences among group means in a sample. Studies have used ANOVA to analyse NetFlow samples to detect anomalies [10]. A *student's t-test* may also be used to analyse the differences among means of two samples but it cannot be used for more than two samples as required in the case of hypothesis H6. We use a one-way ANOVA in order to test the statistical significance of differences between *routine periods* [11].

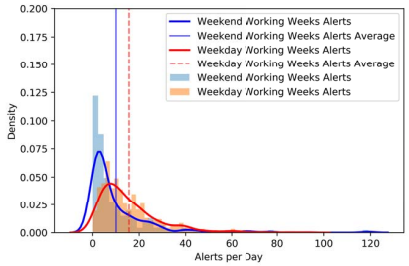
III. Results

In this section we discuss the results of the statistical tests. First, we look at the descriptive statistics, then we discuss the results of ANOVA to establish statistical significance for each hypothesis. Figure 2 shows the descriptive statistics for each of the pair of *routine periods* for which a hypothesis is tested. In each sub-figure we plot number of alerts on the *x-axis* and density (proportion of days on which corresponding number of alerts were generated). We also show the average number of alerts in each *routine period* in the plot. Table III shows the test statistic (F-statistic) and the significance of the test statistic. It also shows if on the basis of the results we are able to reject the null hypothesis or not.

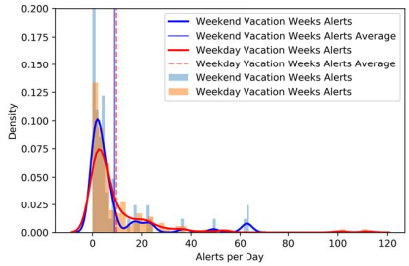
Figure 2a shows the descriptive statistics for the pair of periods considered in H1. With the help of this figure we can clearly observe that the average number of alerts generated in the *working period* is considerably higher than the average



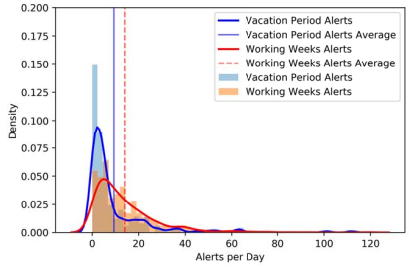
(a) Difference between *working* period and *holiday period*



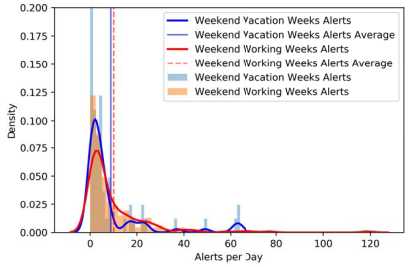
(b) Difference between Weekdays and Weekends (Working Weeks)



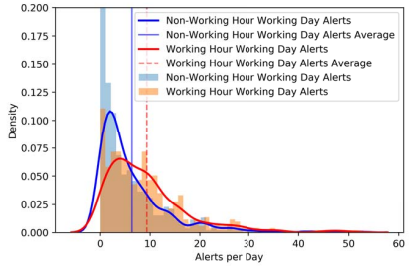
(c) Difference between Weekdays and Weekends (Vacation Weeks)



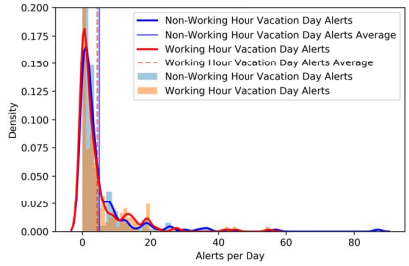
(d) Difference between Vacation Weeks and Working Weeks



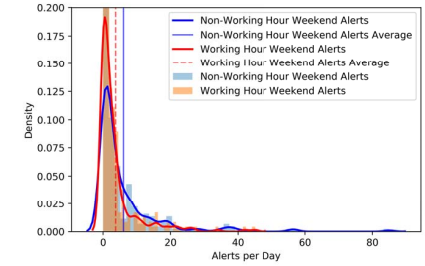
(e) Difference between the weekends of Vacation periods and Working Weeks Period



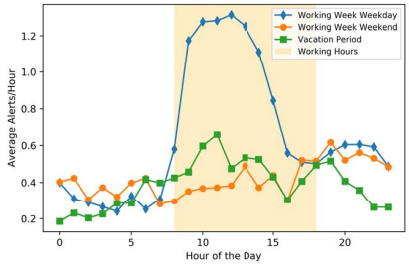
(f) Difference between Working hour and non-working hour Alerts (Working Weeks)



(g) Difference between Working hour and non-working hour Alerts (Vacation Weeks)



(h) Difference between Working hour and non-working hour Alerts (Weekends)



(i) Number of alerts per hour in various routine periods.

Figure 2: Empirical Distributions showing difference in the number of alerts generated per day during various *routine periods*.

Table III: Results of ANOVA

Hypothesis	F-Statistic	Significance (p-value)	Null Hypothesis Status
H1	32.911	0.000	Rejected
H2	22.570	0.000	Rejected
H3	0.000	0.989	Not Rejected
H4	12.470	0.000	Rejected
H5	0.000	0.985	Not Rejected
H6	1.774	0.151	Not Rejected
H7	33.475	0.000	Rejected
H8	0.506	0.477	Not Rejected
H9	8.739	0.003	Rejected

number of alerts generated in the *holiday period*. Based on the density plot we can see that there are more number of days with a higher number of alerts in the working period, most of days in the holiday period has very few number of alerts recorded. ANOVA analysis of $H1_0$ resulted in a F-statistic of 32.911 and a p-value of 0.000. This shows that the difference between the average number of alerts generated during the *working period* and *holiday period* is very high. A low p-value shows high confidence of the statistical test. Hence, we can reject null hypothesis $H1_0$.

The descriptive statistics related to $H2_0$ are shown in Figure 2b. We observe that the average number of alerts generated in the weekdays of *working weeks* period are greater than the average number of alerts generated in the weekends of the same period. The density plots again show that high number of alerts are generated on more occasions on weekdays. ANOVA analysis of $H2_0$ resulted in a F-statistic of 22.570 and a p-value of 0.000. Hence, in this case as well we reject the null hypothesis with high degree of confidence.

Figure 2c shows the descriptive statistics of alerts generated during the weekdays and weekends of vacation periods. According to this figure we observe that the average number of alerts generated during the weekday in the vacation period is nearly equal to the average number of alerts generated on a weekend (Saturday or Sunday) in the vacation period. Both density plots in this case also show a considerable overlap. ANOVA analysis of $H3_0$ also resulted in a F-statistic of 0.000

and a high p-value 0.989. Thus, we cannot reject the null hypothesis.

For analysing null hypothesis $H4_0$ we take help of Figure 2d. Here we compare the number of alerts generated during the *working weeks* period and the vacation periods. The descriptive statistics in this care are similar to the ones in the case of $H1_0$ and $H2_0$. The average number of alerts generated in the *working weeks* period is higher that the average number of alerts generated in the vacation periods. As the ANOVA analysis also resulted in a high F-statistic of 12.470 and a low p-value of 0.000, we reject the null hypothesis $H4_0$.

Figure 2e compares the number of alerts generated during the weekends of vacation periods with the number of alerts generated during the weekends of working weeks periods. We hardly observe any difference in the average number of alerts generated in the two periods. We also see a significant overlap in the density plots. In this case, the ANOVA analysis resulted in a low F-statistic of 0.000 and a high p-value of 0.985. Hence, we do not reject the null hypothesis $H5_0$.

With the help of null hypothesis $H6_0$ we test if there is a difference between the average number of alerts generated during the five vacation periods. The ANOVA analysis in this case resulted in a low F-statistic of 1.774 and a relatively high p-value of 0.151. As the p-value is greater than 0.05, it is not possible to reject the null hypothesis.

Figure 2f differentiates between number of alerts generated during the working and non-working hours of the *working weeks* period. We observe that a significantly higher number of attack alerts are generated during the working hour of a working day as compared to the non-working hour of a working day. The ANOVA analysis of $H7_0$ resulted in a F-statistic of 33.475 and p-value of 0.000. Hence, in this case with high confidence we reject the null hypothesis.

The difference between the number of alerts generated during the working and non-working hours of vacation weeks is shown in Figure 2g. We observe negligible difference in the average number of alerts generated in the two periods. Considering the F-statistic of 0.506 and a high p-value of 0.477, we are unable to reject the null hypothesis $H8_0$.

We show the descriptive statistics for comparing the number of alerts generated in the working hour and non working hour of weekends in Figure 2h. The average number of alerts generated in the non-working hours is slightly greater than the average number of alerts generated in the working hours. ANOVA analysis resulted in a F-statistic of 8.739 and a p-value of 0.003. Hence, we reject the null hypothesis $H9_0$.

IV. Discussion

Based on RAT we hypothesized that change in daily routines of the victim will have an impact on the attack pattern. We base our hypotheses on the principle that a motivated attacker looking to disrupt the educational activities of an academic institution would target the network infrastructure during the working weeks period.

With the help of hypotheses H1, H2, H4 and H5, we test if there are more attacks during the days when there are planned educational activities. As discussed in the previous section, using the dataset we were able to reject the null hypothesis in each case. We were also able to show that statistically more attacks happen on the working day of a work week. Hence, we can say that majority of the attacks on the Dutch educational network target working days.

Next with the help of hypotheses H3 and H6, we compare the average number of attacks that happen during different types of holidays. In this case, we were not able to reject any of the null hypothesis. This is an indication that attack patterns are not influenced by type of vacation. This outcome also supports the central theme: *attack patterns change with daily routines*.

Finally, in hypotheses H7, H8 and H9, we compare the number of attacks on SURFnet's infrastructure during different hours of a day. Figure 2i shows the average number of alerts generated during each hour of a day in three different routine periods. The figure clearly shows that educational institutions in the Netherlands get targeted more often during working hour of a working day. With the help of statistical test we also find that more attacks target the network during the non-working hour of weekends. However, the difference in the average number of alerts generated in the two periods is much smaller as compared to the case of hypotheses H1, H2, H4 and H5.

V. Related Work

We divide the papers in this section in two categories: 1) papers that discuss the aims behind DDoS attacks. 2) papers from criminology that have studied the impact of daily routines on crime patterns.

Past studies [12] showed the various incentives that can be there for a hacker to launch DDoS attacks. Nazario [13] in his study analysed the major events in case of political DDoS attacks. Segura & Lahuerta [14] tried to model the economic incentives that can behind DDoS attacks. Sauter [15] in her paper analysed the motivation of activists to use DDoS attacks as a tool to portray civil disobedience. Paulson & Weber [16] discussed the use of DDoS attacks as an effective cyber extortion weapon aginst online gaming companies. In this paper, show that how targeted attacks can be driven by daily routines of the victim.

A few studies in criminology have studied the impact of type of holiday on type of crime. Templer et al. [17] have shown that calls for police service were more frequent on national and local holidays in Fresno. Similarly, Cohn and Rotton[4] concluded that crimes of expressive violence were significantly more prevalent on major holidays, whereas property crimes were less frequent on those days. Maimon et al. [6] have shown that more attacks are likely to target academic institutions based on the data collected at a single university. In this paper, we further generalise these findings by using data from all academic institutions in The Netherlands.

VI. Conclusion

In this paper, we evaluate NetFlow based attack alerts measured by SURFnet on its infrastructure. We analyse these alerts to study the impact of daily routines of academic

institutions on the rate of denial of service attacks. On the basis of RAT we formulate nine hypotheses considering similar and dissimilar daily routines that we test using one-way analysis of variance (ANOVA) method. The analysis showed that routine activity theory can be used to evaluate the influence of victim routines on attack patterns and prove that most of the attacks on academic institutions are not random. Daily routines of academic institutions heavily influence the rate of attack alerts. We also show that attack patterns do not change significantly (statistically) with type of holidays. In view of these results we can draw the following conclusions:

- We should not look at DDoS attacks in isolation, but also consider the societal aspects
- There is a clear correlation between academic schedules and attack trends.
- This can inform decisions for selecting the type mitigation services.

Our results provides proof for the fact that most attacks on academic institutions in the Netherlands are initiated to disrupt educational activities (e.g. lectures, evaluations, etc.). If we speculate on who might benefit from these disruptions, one of the clear contenders are students.

VII. Limitations and Future Work

This study also comes with some limitations. Netherlands is ranked 7th on the ICT development index list [18]. This means that institutions in the Netherlands highly depend on ICT infrastructure for day to day activities. Hence, availability of ICT services is of critical importance for academic institutions. If such a study is repeated in countries with low levels of ICT integration, we might not see similar results.

Due to unavailability of institution specific data, we could not narrow down upon the educational activities that can lead to greater number of attacks (e.g. exams or open days). Modelling the daily routine of academic institutions is more straight forward than modelling the routines for many other business models (eg. e-commerce websites). In the future it would be interesting to study if daily routines of other businesses also influence the rate of attacks targeting them.

Acknowledgement

We would like to thank Dr. Simone Ferlin, Dr. Anna Sperotto, Dr. Roland van Rijswijk-Deij and the anonymous reviewers for their suggestions. This work would not have been possible without the support of Xander Jansen and Bart Bosma from SURFnet and is part of the NWO: D3 project, which is funded by the Netherlands Organization for Scientific Research (628.001.018).

References

[1] Marc J Rosenberg and Rob Foshay. “E-learning: Strategies for delivering knowledge in the digital age”. In: *Performance Improvement* 41.5 (2002), pp. 50–51.

[2] José Jair Santanna et al. “Booters—An analysis of DDoS-as-a-service attacks”. In: *2015 IFIP/IEEE International Symposium on Integrated Network Management*. IEEE. 2015, pp. 243–251.

[3] *University DDoS attack leads to $8.6 million fine, house arrest for New Jersey man*.

[4] Ellen G Cohn and James Rotton. “Even criminals take a holiday: Instrumental and expressive crimes on major and minor holidays”. In: *Journal of Criminal Justice* 31.4 (2003).

[5] Lawrence E Cohen and Marcus Felson. “Social Change and Crime Rate Trends: A Routine Activity Approach (1979)”. In: *Classics in Environmental Criminology*. CRC Press, 2016, pp. 203–232.

[6] David Maimon et al. “Daily Trends and Origin of Computer-Focused Crimes Against a Large University Computer Network: An Application of the Routine-Activities and Lifestyle Perspective”. In: *British Journal of Criminology* 53 (Feb. 2013), pp. 319–343.

[7] Peter Haag. “Watch your Flows with NfSen and NFDUMP”. In: *50th RIPE Meeting*. 2005.

[8] Arbor Peakflow. “IP Traffic Flow Monitoring System”. In: *URI: http://www. arbornetworks. com/index. php* ().

[9] *Netherlands School Holidays*. URL: https : / / www . schoolholidayseurope.eu/school-holidays-holland/.

[10] Clifford Kemp, Chad Calvert and Taghi Khoshgoftaar. “Utilizing Netflow Data to Detect Slow Read Attacks”. In: *2018 IEEE International Conference on Information Reuse and Integration (IRI)*. IEEE. 2018, pp. 108–116.

[11] Eric Jones, Travis Oliphant and Pearu Peterson. “{SciPy}: open source scientific tools for {Python}”. In: (2014).

[12] Saman Taghavi Zargar, James Joshi and David Tipper. “A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks”. In: *IEEE Communications Surveys and Tutorials* (2013).

[13] Jose Nazario. “Politically motivated denial of service attacks”. In: *Cryptology and Information Security Series* (2009).

[14] Vicente Segura and Javier Lahuerta. “Modeling the Economic Incentives of DDoS Attacks: Femtocell Case Study”. In: *Economics of information security and privacy* (2010).

[15] 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.

[16] Richard A. Paulson and James Weber. “Cyberextortion : an Overview of Distributed Denial of Service”. In: (2006).

[17] Donald I Templer, Robert K Brooner and Mark D Corgiat. “Geophysical variables and behavior: XIV. Lunar phase and crime: Fact or artifact”. In: *Perceptual and Motor Skills* 57.3 (1983), pp. 993–994.

[18] *ICT Development Index 2017*. URL: http://www.itu.int/net4/itu-d/idi/2017/index.html.