# Exploring the methods and goals of students who DDoS educational facilities

Author: Dolph Sandkühler
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands

**ABSTRACT,**
***DDoS attacks on educational facilities have increased in recent years. Research suggests that students are the cause of this problem. This thesis investigates, why students DDoS their educational facilities and which methods they use to do so. Criminology theories such as Routine Activity Theory were used to develop a questionnaire which was then filled out by attackers of the past. Content analysis was used to identify typical themes and patterns across the participants. The results indicate that apart from preventing examinations, many DDoS offenders attack their educational facilities out of pure curiosity and experimentation. In most cases, offenders seem to regret their actions as they did not consider the consequences of such an attack. This can be referred to the fact that the use of DDoS attacks has become easier to execute as people can buy publically available DDoS-for-hire services online for low prices. Results from this study can be used to look for intervention points. Future studies should be conducted on a larger scale to validate findings made in this thesis.***

**Graduation Committee members:**
Prof. Dr. Junger
Dr. Abhishta

**Keywords**
DDoS attacks, Methods, Goals, Schools, educational facilities

# 1. INTRODUCTION

## 1.1 Background

In today's digital age, most businesses heavily rely on their functioning internet services. The importance of cybersecurity for business continuity should therefore not be overlooked, as such attacks can not only have major financial consequences, but also bring important safety concerns with them. The constant advancement of technology leaves room for potential attacks. Security gaps need to be closed as quickly as possible in order to minimize damage. A commonly used method of cybercrime are Distributed-Denial-of-Service attacks (DDoS). The main goal of these attacks is to cause unavailability of services provided by computer platforms for legitimate users (Riza' et al., 2019). This is done by stressing and overwhelming the servers with huge amounts of data and requests, making the server unable to respond to legitimate requests.

Nowadays, there are DDoS-for-hire services that allow you to buy DDoS attacks as a service for a monthly fee starting at 1$. Such attacks are commonly used by young people such as gamers in order to gain an advantage over their competitors (Karami & McCoy, 2013). Unfortunately, also educational facilities such as schools and universities frequently experience DDoS attacks, preventing users to access important educational materials and services (Rice, 2017). In the case of students like me, we now submit the majority of our assignments digitally through platforms such as 'Canvas'. Due to the COVID-19 outbreak and the subsequent lockdown, we are forced to even take our exams remotely from home. The potential consequences of a DDoS attack can therefore be as impactful as never before.

Research by Abhishta on Distributed Denial-of-Service (DDoS) attacks against educational facilities in the Netherlands concluded, that there is a clear correlation between the academic schedules and the DDoS attack trends (Abhishta, 2019). Most attacks were conducted during working periods and working hours instead of holiday and vacation periods. Such attacks are therefore targeted to achieve the disruption of educational activities. Accordingly, this suggests that students are the most likely offenders, this is not sure though, as no systematic research has been conducted on this topic yet. Also, the exact benefits behind why students attack their own educational facilities are still unclear. This paper aims to fill this gap in research by taking an exploratory approach. Students that have used DDoS attacks against their educational facilities in the past have been asked to report about their goals and the methods that were used.

## 1.2 Research Question

The aim of the present study is to find out how students approach the decision for the DDoS attack and what the reasons for their behaviour are. The main research question therefore is:

What are the underlying principles and motivations of students to use DDoS attacks against their own educational facilities?

Accordingly, I will investigate two separate questions:

1) What are the goals of students when they DDoS their own educational facility?

2) How did they do this: how exactly did they conduct these attacks?

## 1.3 Structure of the thesis

Chapter 2 will focus on analyzing, connecting and evaluating the existing literature and research on DDoS attacks in order to address the current research gap in literature as well as provide a foundation for this research. In chapter 3 I take a look at existing theory that is relevant to this specific research problem. By defining the key concepts in the theoretical framework, I aim to narrow down the scope of this project and justify the theoretical approach for my research design. During chapter 4, I justify the methodological approach and explain how I collected and analyzed the data to ensure the reliability and validity of this research. Chapter 5 will present the results that have been collected and discusses them in an analytical manner. The study will then be summarized in chapter 6. Here I also broaden the scope again and look at the practical and theoretical implications as well as limitations to the validity of this research.

# 2. LITERATURE REVIEW

## 2.1 Defining DDoS Attacks

The primary goal of Denial-of-Service attacks is to disrupt the availability of web applications (Radware, n.d.). They are a malicious form of cybercrime that prevents the use of internet services for legitimate users (Mirkovic & Reiher, 2004). Attackers achieve this by occupying a network with huge amounts of data traffic and requests, therefore depleting a network's bandwidth and resources (Douligeris & Mitrokotsa, 2004). An advancement of Denial-of-Service attacks are Distributed-Denial-of-Service attacks (DDoS). Similar to normal DoS attacks, DDoS attacks function by having multiple computer systems performing DoS attacks against a single target at the same time (Keary, 2019). These computer systems have usually been affected by malware, giving the attacker remote control over the system. The group of infected systems that is used to perform such a DDoS attack is called a botnet (Cloudflare, n.d.). The use of Botnets is also sold online via "attack-for-hire" services, which will be further discussed in section 2.2. Due to the increasing development of the Internet of Things, even small electronic devices, which are a lot easier to infect and take control over, can become part of such botnets (CISA, 2019). Attacking the victim through multiple completely different machines is also what makes tracing the origin of the attack so difficult (Keary, 2019).

## 2.2 Methods of DDoSing

There are multiple different methods to flood a server with excessive amounts of traffic. Nowadays, not even a lot of technical knowledge is required to perform a Denial-of-Service attack. One common tool is Low Orbit Ion Cannon (LOIC). It was originally developed as a stresser-tool, so a program to test one's own server for its robustness and see what loads the server can sustain. Ever since it has become open-source, it has mostly become a tool for DoS attacks, or, if multiple offenders use LOIC simultaneously against the same target, for DDoS attacks (Cloudflare, n.d.-c). Its successor High Orbit Ion Cannon (HOIC) works similarly and also provides a user-friendly interface just like LOIC. Both tools are legally available as they only claim to be tools for stress testing, consequently giving easy access to people with malicious intents (Cloudflare, n.d.-b). DDoSing is simpler than ever before, because attacks are now also being offered as a service for a monetary return. They can be found on the internet as e.g. DDoS-for-hire, booter-service, or, to hide the criminal intent, as simple IP stresser tools. These services offer the use of botnets for DDoS attacks, which are being loaned out by owners of botnets. Prices for such services already start at $1 (Noroozian et al., 2016), but can gradually get more expensive, depending on how long and strong the desired attack is supposed

to be. This has therefore become a serious business for botnet-providers.

## 2.3 DDoS on Educational Facilities

According to Santanna et al. (2015), SURFnet, the network provider for all Dutch educational networks has experienced a series of DDoS attacks in recent years. Research by Abhishta has confirmed, that these attacks mostly occurred during working hours of the educational facilities (Abhishta, 2019). This would suggest that students are the most likely offender, because jamming the network during working hours will lead to a disruption of educational activities. Noroozian et al. (2016) stated that a total of 12% of all DDoS attacks were directed at either educational or governmental networks and that there are a wide variety of motives behind these attacks. Yet, there are only very few news articles and blogs that report that DDoS attacks on universities and schools become more common and are mostly conducted by students. Also, all these articles list different motives and none of them rely on scientific research.

Chicago Tribune reported about a DDoS incident in 2014, where 2 students DDoSed their school several times over a month's period (Ward, 2014). They got into DDoSing through a friend from an online gaming community. The article also mentions that setting up technological countermeasures to prevent feature attacks could cost hundreds of thousands of dollars.

A public court case in the Netherlands reports about a student DDoSing his own school out of pure curiosity (Rechtbank Zeeland-West-Brabant, 2013). He owned a website and used DDoS attacks to stress-test his own servers. After hearing about past DDoS incidents at his school, he was interested in finding out if the school was resistant to his DDoS attacks, or if he could disrupt the network himself. He launched attacks a total of 3 times and as soon as he saw that the school's network was malfunctioning, he stopped the DDoS attack again, which validates pure curiosity as a reason for his actions. Contrarily to other articles, this does not suggest a malicious intent from the offender but instead the curiosity of the attacker in the ability to disrupt someone else's network.

# 3. THEORETICAL FRAMEWORK

In order to better understand the goals of students when attacking their own educational facilities, first general theories that aim to explain the tendency towards criminal behaviour need to be discussed and shall form the basis of my research. I will use 'crime science' theories that focus on the context of crime, which fits with the present approach of the topic. Accordingly, I will describe the Routine Activity Theory, Rational Choice Theory and give an introduction into crime scripts in the following section.

## 3.1 Routine Activity Theory

The Routine Activity Theory was first developed by Felson and Cohen in 1979 (Miro, 2014). It proposes that there are three major factors that encourage crime which are the existence of a motivated offender, a suitable target, as well as the absence of a capable guardian for this target (see Figure 1). The theory states that if these three factors are aligned with each other in space and time, a crime is likely to occur.

According to Miro (2014), a likely offender can be anyone who has a motive to commit a crime and the required capacity to do so. So, the potential offender does not only need the motivation to commit a crime, but also the physical capabilities to successfully execute the crime. As identified in section 2.2, executing DDoS attacks has become easier than ever before due to the possibility to buy DDoS-for-hire services for a cheap price.

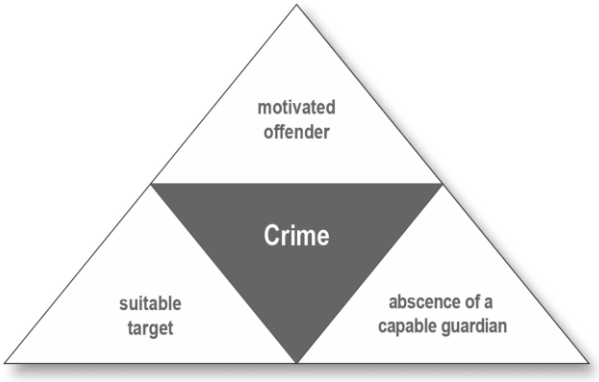


**Figure 1. Routine Activity Theory (Wickert, 2019)**

A suitable target is characterized by the four attributes of the acronym **VIVA**, which stands for **value**, **inertia**, **visibility** and **access** (Miro, 2014). With these four attributes, a potential offender defines the level of attractiveness a target has and its level of risk connected to it. The value of a target refers to the real or symbolic value of a target from the offender's perspective. Inertia describes to what extent the target can be seen as an obstacle in terms of size, weight and shape. Smaller targets are usually more prone to crime as they are easier to execute. Visibility refers to the degree to which the offender is exposed to the target and how well he knows it. Lastly, access refers to the architecture around the target and how easy it is to reach said target. The higher the scores are on each of these attributes, the more attractive a target is to an offender. As most students have or had compulsory school attendance, the visibility attribute is naturally high in the scenario of students DDoSing their educational facilities.

Often connected to the attractiveness of a target is the absence of a capable guardian. The capable guardian is someone or something that is supposed to prevent attacks from being successfully executed, such as a patrol, a firewall, or a whole cybersecurity system (Miro, 2014). If these guardians are absent, or have exploitable loopholes which make the offender believe to unlikely be caught, then a crime is more likely to occur.

## 3.2 Rational Choice Theory

Next up is the Rational Choice Theory. According to Cornish & Clarke (2017), criminal behaviour is conceived as rational, meaning that offenders try to achieve their benefits with the best available means possible. Criminal behaviour is usually purposive, meaning that offenders see a real purpose, a benefit in committing the crime which outweighs the connected risks. Such benefits can be monetary, as well as desires for revenge, material goods, sexual pleasure etc. Criminal behaviour is also being seen as rational, meaning that offenders try to achieve their benefits with the best available means possible. Due to the risky and uncertain nature of crime and the incompleteness of information, a rational decision usually leads to a short-term satisfying rather than optimal outcome for the offender.

In sum, criminals have specific aims in mind, which means that offenders do not commit a crime for the sake of it, but that they act goal oriented and that there lies a personal motive/benefit behind every crime. Criminals are responsive to the opportunities

and risks that occur in different situations. The benefits and the risks for crime depend on opportunities and situations. As these opportunities differ a lot for different types of crime, this makes comparisons and generalizations between crimes difficult. For instance, the opportunities and risks for burglary differ from the opportunities of car theft or fraud. Criminal involvement also needs to be distinguished from crime event decisions. While Event decisions only concern the choices "when preparing for, carrying out and concluding the commission of a particular type of crime", involvement decisions extend over longer time scales, as they consider the offender's criminal career. They are concerned with a larger set of variables. Cornish & Clarke (2017) also identify three broad stages for the involvement in crime. These are initiation, habituation and desistance. At each stage, different variables influence the decision making of the offender. Such variables can be success rates, the impact on their lifestyle as well as extraneous factors.

The Rational Choice Theory serves as a model to show the goal-oriented intentions of likely offenders. It explains how every potential offender has its own specific beliefs and motivations and based on that decides on the crimes he would like to undertake.

## 3.3 Crime Scripts

In 1994, Cornish introduced the concept of the script-theoretic approach which helps to generate, organize and systematize knowledge about procedural aspects of a crime. It serves as "a useful tool for looking at behavioural routines in the service of rational, purposive, goal-oriented action" (Cornish, 1994). Linked to the rational choice perspective, the theory about scripting crimes explains that human behaviour follows predictable patterns which can be analysed and traced. Scripts could therefore be divided into smaller units, with each of these units being a potential intervention point. Understanding the full script of a crime is therefore essential to prevent crime in the future as they help to understand behavioural processes and procedural aspects of crime scenes and consequently support the implementation of innovative control measures (Borrion, 2013). Cornish's research on crime scripting is still relevant to this day, as the use of crime scripts has grown exponentially ever since he released his article (Dehghanniri & Borrion, 2019).

# 4. RESEARCH DESIGN

## 4.1 Methodological Approach

The central purpose of this research is to explore the methods and goals of students that DDoS their educational facilities. As discovered in the literature review, this field is not researched thoroughly yet. In order to answer my research question and better understand the reasoning of students performing DDoS attacks against educational facilities, I conducted qualitative research that collected original data to gain in-depth insights into the background of these attacks.

I took an exploratory approach on research design, meaning that I took a yet to be defined problem and explored potential causes in order to better understand the problem that needs to be solved and gain new insights. Exploratory research is being conducted when prior literature and studies are limited and the subject not yet well understood (Van Wyk, 2012). This paper therefore does not aim to draw final conclusions to the research problem, but instead describe and identify common patterns to develop a foundation for future research to come.

## 4.2 Units of Analysis

As this study aims to understand the behavior of students that DDoSed their educational facility in the past, these students were the unit of analysis. I collected data directly from these individuals, therefore they also embody the unit of observation. The important factor is that they performed such a DDoS attack when they were still students themselves. Whether they are still students today or not is not relevant to this study. Additionally, we reached out and got in contact with the IT Security manager of the University of Twente, Peter Peters, who is also part of the Computer Emergency Response Team (CERT) at SURFnet. His job is to keep the IT systems of Dutch educational institutions safe and secure. Part of that involves raising awareness and investigating incidents of DDoS attacks. He served as an expert for our study and helped us validate the impressions from the data analysis.

## 4.3 Method of Data Collection

In order to receive responses for my qualitative study, I registered in multiple public hacking forums. This is a common place for all sorts of hackers and cybercriminals to exchange about a wide variety of IT and hacking knowledge. On these forums, I made a public post to explain my request and ask people that DDoSed their educational facility in the past to reach out to me either via a private message or per mail. Additionally, I used the search function to look back into the archives of the forums and find people that have discussed the DDoSing of schools. Here, multiple users have admitted to DDoSing their school in the past. Via a private message I reached out to these people and asked them to fill out my questionnaire.

The data collection method that was used was a web-based, semi-structured questionnaire. The tool used to collect answers from respondents was Qualtrics. Qualtrics is a software-tool to create online surveys and it is freely available to all students of the faculty of Behavioural, Management and Social Sciences (BMS). A questionnaire was used due to the sensitive nature of the topic addressed. It would provide enough anonymity so that the DDoS offenders could open up about their past criminal activity without revealing any personally identifiable information. An audio or video call would have most likely led to less participants and respondents.

The questionnaire asked a total of 16 questions regarding the respondents' experience with DDoS attacks and took about 20 minutes to complete. Themes and topics addressed include how the individual got into DDoSing, which service they used, why they launched the DDoS, the consequences and their thought-process and mindset before and after they DDoSed their educational facility.

The questions were mostly developed by linking them to the theories that are explained in section 3. For example, Routine Activity Theory (section 3.1) was used to form questions about the offender's motivation when DDoSing his educational facility. Participants were also asked about the methods and resources that were used to perform the DDoS attack. So, whether they got any external help when DDoSing and at what time they performed the attack. Routine Activity Theory also refers to the absence of a capable guardian as a reason for criminal behavior. Therefore, participants were asked what made them believe that they would not be caught.

The Rational Choice Theory was used to develop questions regarding the offender's thought process and whether risks and rewards were evaluated prior to the attack. Based on this model, participants were asked what their goal and motive was when DDoSing their educational facility and why they believed the risks of such an attack did not stop them from doing it.

Lastly, some questions were developed without a specific theory in mind but in hope to gain additional information from the participants. Such questions include reflective questions such as how they assess their actions nowadays and how their relationship was within school.

Accordingly, three types of questions were developed. Questions based around the Routine Activity Theory, Rational Choice Theory as well as some additional ones. The full questionnaire can be found in the appendix.

The questionnaire received a total of 10 responses, of which 9 have been filled out by students that DDoSed their educational facility in the past. 1 respondent reported about his experience with DDoSing in general and was therefore excluded from the data analysis as he does not comply with the requirements for our units of analysis as mentioned in 4.2. Relevant to my study are therefore only the responses of the other 9 participants.

Additionally, P. Peters, who is the IT security manager at the University of Twente and part of the Computer Emergency Response Team (CERT) at SURFnet, served as an expert and was interviewed in a video call using Skype. The interview took place on the 2nd of June 2020. In a 20-minute open-question conversation I asked him about his experiences regarding DDoS attacks on educational facilities. The topics addressed were similar to the ones that have been asked in the questionnaire. His answers were used to validate the impressions from the data analysis of the questionnaire and thus aimed to make the conclusions more reliable.

## 4.4 Method of Data Analysis

In order to analyze the raw data from the questionnaire, a qualitative content analysis was conducted. Krippendorff (1989) describes content analysis as potentially one of the most important research techniques in social sciences and that it is increasingly applied to data such as answers from open-ended interview questions. Carley (1993, p. 81) states that "content analysis focuses on the frequency with which words or concepts occur in texts or across texts". These words or concepts need to be coded in order to detect common patterns and make them comparable.

There are two typical approaches to coding data. One is the deductive approach, where codes are developed a priori, so before data was collected. This is possible when certain themes or patterns are expected to occur due to prior research or theory development on the phenomenon (Ryan & Bernard, 2003). For example, if literature has shown that some DDoS offenders attacked their educational facility to prevent an exam, then in the questionnaire "prevent an exam" can be offered as a potential answer to a multiple-choice question which asks about the goal of the offender to attack his educational facility. This approach was therefore being conducted during the process of developing the questionnaire.

The other approach is the inductive approach to coding. Here, codes are assigned as the raw data is being reviewed. In the form of open questions, answers need to be reviewed line-by-line to identify the respondent's perspective on the topic (White & Marsh, 2006). As each answer is being reviewed and summarized, they can be put into response categories. In the end, all answers will land in at least one response category. If similar answers occur between respondents, then those response categories will stand out for being mentioned more frequently.

As the questionnaire includes both closed as well as open questions, both approaches were used in this study.

Because the sample size of this research is relatively low with a total of 9 valid respondents, the coding could be done manually. First, all questions were added into separate Excel sheets. For each question, the recorded answers were added underneath. In the case of closed, multiple-choice questions, the answers given were also used as codes and counted each time they were used. For the open-ended questions, each response was read carefully and the main keywords of the answers were written down. Once the main keywords of all 9 responses were written down, they were put into response categories. Those answers that had the same content, but maybe were worded slightly differently were counted together and put into the same response category. It is possible that respondents answered with more than one response category per question. In that case, each answer was counted separately, so some questions have more than a total of 9 responses.

In the end, a table was created for each question (see Results). In these tables, each response category that was developed is shown along with how many times this particular response occurred across all respondents, thus making the qualitative answers of the questionnaire quantifiable to give them slightly more meaning.

## 4.5 Ethical Concerns

All studies at the University of Twente that involve the collection of new primary data on humans require an approval by the ethical committee. As I was dealing with the analysis of individuals that have performed cybercriminal activity in the past, confidentiality was of highest importance. All data has been treated in accordance to the EU General Data Protection Regulation. In addition to that, at no time was personally identifiable information collected or asked for. The questionnaire does not request any personal information and the link to the questionnaire has also been anonymized, meaning that no IP could have been tracked. This was an important step to gain trust of the individuals that were willing to participate in the study. Additionally, respondents were allowed to use a nickname to make answers differentiable without giving away their identity. Before participants could enter the questionnaire, they were required to acknowledge and accept a letter of consent and approve that they were at least 16 years of age, so that no parental consent had to be given. The letter of consent made them aware that the participation in the study was entirely voluntary, confidential and that results of the study may be used for future research.

# 5. RESULTS

In this section, the answers and results of the questionnaire will be presented and discussed. For each question in the questionnaire a descriptive table has been created. The most relevant tables in regard to the research question will be presented in this text with additional tables for further insights attached in the appendix. The left column of the tables describes the codes/keywords that were identified from the answers of the respondents. The center column describes the frequency these keywords occurred across all answers. The column furthest to the right describes the percentage of a code/keyword being mentioned out of all responses for that particular question. Results are presented in the order the questions were asked during the questionnaire in order to create a coherent story.

Table 1 showcases the answers to the question how the DDoS offenders got introduced to DDoSing. Four people responded that they found out about DDoSing through their activity in an online forum. Three respondents answered that they were exposed to DDoS attacks through playing video games. The video games that were mentioned are the open-world sandbox game Minecraft, which was released in 2009 and the 2012 released strategic shooter Counter Strike: Global Offensive. Two respondents said they were actively searching how to perform a cyberattack via an internet search.

**Table 1. How respondents discovered DDoSing**

| | | |
|---|---|---|
| *Online forum* | 4 | *44%* |
| *Gaming* | 3 | *33%* |
| *Internet search* | 2 | *22%* |
| *Total* | *9* | *100%* |

The second question asked the respondents about the program or service that was used to perform the DDoS attacks. As can be seen in Table 2, the majority of respondents said they rented a botnet via a DDoS-for-hire service so that an external party performed the DDoS attack for them. Two respondents have reported that they used the stresser-tool Low-Orbit-Ion-Cannon, which was explained in section 2.2. The remaining two respondents owned their own botnet which they used to execute the DDoS attacks.

**Table 2. How respondents executed DDoS attacks**

| | | |
|---|---|---|
| *DDoS-for-hire* | 5 | *56%* |
| *LOIC* | 2 | *22%* |
| *Using own botnet* | 2 | *22%* |
| *Total* | *9* | *100%* |

The third part of the questionnaire was a descriptive question which asked the DDoS offenders about how many times they targeted a DDoS attack against their educational facility (Table 3). A total of three people only performed a single DDoS attack against their educational facility. Three other respondents DDoSed their educational facility a total of three times while one respondent launched two attacks. Standing out the most is one respondent who DDoSed his educational facility more than 10 times.

**Table 3. How many times they DDoSed their educational facility**

| | | |
|---|---|---|
| *1 time* | 3 | *33%* |
| *3 times* | 3 | *33%* |
| *2 times* | 1 | *11%* |
| *10+ times* | 1 | *11%* |
| *No response* | 1 | *11%* |
| *Total* | *9* | *100%* |

Table 4 adds on to research conducted by Abhishta (2019), which pointed out that DDoS attacks against educational facilities usually occur during working periods. In this sample, four respondents launched their DDoS attack in the morning between 8AM and 9AM. Two respondents conducted their DDoS attacks around midnight while one did so in the afternoon. The remaining two participants did not respond to this particular question.

**Table 4. Time of day the DDoS attacks were launched**

| | | |
|---|---|---|
| *Morning* | 4 | *44%* |
| *Night* | 2 | *22%* |
| *Afternoon* | 1 | *11%* |
| *No response* | 2 | *22%* |
| *Total* | *9* | *100%* |

To continue on Abhishta's research (2019), which suggests that DDoS attacks are conducted during working periods in order to disrupt educational activities such as exams, the questionnaire asked the participants what their goal was when DDoSing their educational facility. This is also one of the two sub questions to the research question, as stated in section 1.2.

Table 5 shows that a total of four respondents reported, that their goal was to prevent an exam or delay an assignment. This corresponds to and backs the claim of Abhishta, that DDoS attacks during working periods are conducted to disrupt educational activities (Abhishta, 2019). Also shown in Table 5 is that two respondents used DDoS attacks as a form of protest to signalize their dissatisfaction with their schools.

Two respondents made 2 very similar statements in regard to the motivation behind their DDoS attack. They both stated that they were curious of and experimenting with the power they had. Two separated themes were identified from this. One is the experimentation aspect, where the offenders were curious to find out if they were able to disrupt the network of their educational facility. This motive has also been discovered in section 2.3, where a court case reported about a student being curious to find out whether he could disrupt his school's network. The second motivation that the two respondents gave was that they all enjoyed the thrill and feeling of having the power to disable someone's network.

The last participant reported that the motivation behind his DDoS attack was purely out of fun. In the expert interview, P. Peters also listed this as a motivation of students that DDoS their schools. Apparently, many young students DDoS their school for fun. They like to talk and brag about it in front of their friends group in order to earn so called "street credits" (personal communications, June 2, 2020).

The successful execution of a DDoS attack on educational facilities will also have consequences, so the participants were asked what the impact was on the educational facility they attacked. As can be seen in Table 6, in five cases an exam or a homework assignment was postponed. Two attacks led to the IT classes being compromised as computer equipment reliant on the network were made unavailable. One attack was only focused on the website of the respondent's school, which was successfully put offline. The last reported attack went unnoticed without an impact.

As already mentioned in section 3.1 when explaining the Routine Activity Theory, someone becomes a likely offender once he has a motive to commit a crime and the capabilities to do so. The main motives that were identified from Table 5 and Table 6 are the opportunity to delay examination, the curiosity in having the power to disable someone's network, the dealing with discontent at school, as well as the fun aspect of disabling someone's network.

**Table 5. The motivation behind DDoSing the educational facility**

| | | |
|---|---|---|
| *Prevent/delay examination* | 4 | *36%* |
| *Experimentation/curiosity* | 2 | *18%* |
| *Feeling of power* | 2 | *18%* |
| *Dissatisfaction with school* | 2 | *18%* |
| *For fun* | 1 | *9%* |
| *Total* | *11* | *100%* |

**Table 6. The impact of the DDoS attacks**

| | | |
|---|---|---|
| *Exam/homework postponed* | 5 | *56%* |
| *IT classes compromised* | 2 | *22%* |
| *School website offline* | 1 | *11%* |
| *None* | 1 | *11%* |
| *Total* | *9* | *100%* |

A motive alone is usually not enough for an offender to participate in cybercriminal activity. Referring back to section 3.1 and the Routine Activity Theory, an important factor is also the absence of a capable guardian (Miro, 2014). Therefore, participants were asked about what made them believe at the time that they were not going to be caught (Table 7). Four respondents said, they thought buying an external booter was enough to not be caught. Three people mentioned the use of a VPN as convincing enough to bypass the presence of a guardian. Three other respondents reported, that they were actually not even considering the thought of being caught and described their actions at the time as careless. By modifying their IP-addresses, two participants thought they could not be caught, while the final two respondents mentioned the inexperienced IT-staff of their school as enough reason to believe that they would not be caught. Related to this, these two respondents also reported the small size of their school as a reason. This refers back to the Routine Activity Theory (section 3.1), which describes a suitable target as one with low inertia. The students perceived that the school's size was small enough to make not make it an intimidating obstacle.

During the expert interview with P. Peters this was further confirmed. Schools usually have to ask the network providers for measures to be put into place first. He also mentioned as a problem, that most schools do not have the manpower and experience to investigate the incoming DDoS attacks (personal communications, June 2, 2020). The schools could ask the network provider to investigate the roots of the attack, but this would come at a great financial expense.

The Rational Choice Model, which was explained in section 3.2, states, that criminal behavior is purposeful, meaning that there are motives and benefits for performing said criminal behavior. It also explains criminal behavior as being rational, so that offenders perform a cost-benefit analysis and weigh up the risks against the rewards that can be gained. In this sample, three people simply did not consider the risks, while the other 6 people believed that the methods shown in Table 7 were enough to make the benefits outweigh the naturally uncertain risks of criminal behavior.

**Table 7. What made the respondents believe to not be caught**

| | | |
|---|---|---|
| *Use of DDoS-for-hire* | 4 | *25%* |
| *Use of VPN* | 3 | *19%* |
| *Carelessness* | 3 | *19%* |
| *Hidden IP-address* | 2 | *12%* |
| *Lack of experienced IT-staff* | 2 | *12%* |
| *Small size of school* | 2 | *12%* |
| *Total* | *16* | *100%* |

I was also curious to find out, whether the participants today still assess the benefits and risks the same way as they did before executing DDoS attacks on their educational facilities. Table 8 shows, that all seven respondents to the question changed their perception on the act of DDoSing educational facilities. Four people answered that they would not recommend anyone to do something similar anymore, as the risk involved is too high for the very small benefit that someone would gain from DDoSing his educational facility. For example, one participant questioned whether this effort and the subsequent act of messing with institutions that belong to the government is worth it, just to delay an exam by a week. Three respondents perceived their actions in hindsight as reckless and shortsighted. They think they should have taken a lot more precautions when DDoSing their educational facility. One respondent even mentioned that he regrets the act and that he should not have done it in the first place. The remaining two participants did not give an answer to this particular question.

Answers to this question correspond to statements made by the expert P. Peters. When asked why DDoS attacks occur more and more often recently, he stated that it is much easier to order an attack nowadays but that the students involved sometimes do it for fun without realizing what damage can be done from this (personal communications, June 2, 2020).

**Table 8. How respondents view their actions nowadays**

| | | |
|---|---|---|
| *Would not recommend* | 4 | *40%* |
| *Reckless* | 3 | *30%* |
| *Regret* | 1 | *10%* |
| *No response* | 2 | *20%* |
| *Total* | *10* | *100%* |

Following the question, which methods were used to perform the DDoS attacks, all participants were asked whether they used help from someone else to execute the attack. The results of this question are shown below in Table 9. Seven respondents said that they performed the attack all on their own, while the other two respondents reported that they needed help by others as they were using Low Orbit Ion Cannon to perform a DDoS attack. As mentioned in section 2.2, a Low Orbit Ion Cannon attack only becomes a DDoS attack once multiple people use the program simultaneously. As this method requires a fair bit of communication and coordination, it was perceived as more difficult by the respondents. Those participants that rented a botnet online via a DDoS-for-hire service did not get any external help apart from the people that managed the DDoS-for-hire service.

**Table 9. Involvement of others in the DDoS attack**

| | | |
|---|---|---|
| *No* | 7 | *78%* |
| *Yes* | 2 | *22%* |
| *Total* | *9* | *100%* |

Participants were also asked about who knew that they performed the DDoS attack (see Table 10). In four cases, friends were aware of who launched the DDoS attack. Four other people managed to keep the attack all to themselves. In two cases the school was aware and informed of who attacked them. Family and police were involved in only one case of this sample.

**Table 10. People that knew who performed the attack**

| | | |
|---|---|---|
| *Friends* | 4 | *33%* |
| *No one* | 4 | *33%* |
| *School* | 2 | *17%* |
| *Family* | 1 | *8%* |
| *Police* | 1 | *8%* |
| *Total* | *12* | *100%* |

As a reflective follow up question, participants were asked whether the act of DDoSing their educational facility was difficult to execute (see Table 11). Seven respondents reported that it was not difficult to execute, while the other two respondents perceived the attack as difficult to execute. These two respondents were using Low Orbit Ion Cannon, which suggests that coordinating the attack simultaneously with multiple people is what made the DDoS attack more difficult to execute. Referring to Routine Activity Theory (section 3.1), someone is more likely to become an offender if he has the required capacity to perform the crime. In this case, seven participants perceived this capacity to not be a burden, either due to simply hiring a DDoS attack, or due to already owning a botnet to DDoS targets (see Table 2).

**Table 11. DDoS attack perceived as difficult to execute**

| | | |
|---|---|---|
| *No* | 7 | *78%* |
| *Yes* | 2 | *22%* |
| *Total* | *9* | *100%* |

The last question of the questionnaire was trying to investigate whether the intention to DDoS their educational facility was amplified by the relationship to their school or the school's teachers (see Table 12). Three participants reported that they disliked going to school in general and performed badly there. Three other participants said they only disliked particular teachers, with two of them saying the DDoS attack was initiated due to the relationship to these teachers. The remaining three participants did not have any bad or unordinary experiences at school and described their life at school as normal or even good.

**Table 12. Respondent's relationship with school / teachers**

| | | |
|---|---|---|
| *Disliked school* | 3 | *33%* |
| *Disliked particular teacher* | 3 | *33%* |
| *Normal relationship* | 2 | *22%* |
| *Good relationship* | 1 | *11%* |
| *Total* | *9* | *100%* |

# 6. CONCLUSION

This study aimed to give an insight into how and why DDoS attacks occur at educational facilities. Prior research suggested that students are the ones conducting these DDoS attacks. In an exploratory approach, qualitative interviews were conducted with students that admitted to DDoS their educational facilities in the past. The aim was to discover the goals of students who DDoSed their educational facility and understand typical methods with which these were conducted. On the basis of a questionnaire and its respective answers, a content analysis was carried out in order to make qualitative answers measureable. The results of the content analysis showed that people often learn about DDoSing through online communities such as forums and video game communities. As it is the easiest method for amateurs, DDoS-for-hire services seem to be the most common method to execute these attacks, while Low Orbit Ion Cannon and the use of an owned botnet were also mentioned as possible methods. Results from this research also matched with conclusions of other research which stated that most DDoS attacks on educational facilities occur during working periods. Routine Activity Theory was used to analyze whether the intention of these offenders was to disrupt educational activities. It was identified that disrupting examinations and assignments are indeed common motives of offenders. Additionally, curiosity, thrill and the feeling of power were found to be reasons for these attacks. By applying the Rational Choice Theory, it was understood that the use of DDoS-for-hire services and VPN usage are popular methods to make the benefits outweigh the risks connected to the criminal activity. In addition to that, it was found that a proportion of the participants were not considering the risks of a DDoS attack at the time. The expert P. Peters confirmed, that students often do not realize what damage can be done from DDoSing educational facilities. Results also showed that all participants changed their view on DDoSing educational facilities and now perceive it as something that should not be done and that they discourage others from doing it.

## 6.1 Contribution to Theory

This study served as an introduction to exploring the phenomenon of students DDoSing their educational facilities. Future research can conduct this research on a larger scale in order to validate assumptions made in this paper and better understand the foundation of the underlying problem.

## 6.2 Contribution to Practice

This thesis can be used as an access point to investigate the causes of DDoS attacks on educational facilities. By analyzing the common themes and patterns of DDoS offenders, a basis of the script of this crime was given. Understanding the methods and motives is the first step to find possible intervention points. Schools can take these results into consideration in order to mitigate the impact of incoming DDoS attacks and proactively reduce the chances of them occurring in the future.

## 6.3 Limitations

This research does have some limitations that need to be considered. An exploratory research design is not meant to draw any conclusions or solutions to the problem. Instead, it aims to gain new insights by providing an interpretation of qualitative data and is therefore subject to bias. The problem that is addressed in this study is also not a phenomenon that can be explained with one definite answer. There exist multiple different causes for people DDoSing their educational facilities and the goal of this study is to detect the themes that appear to be the most common. In addition to that, a total sample size of 9 participants is not big enough to prove a statistically significant representation of the total population. Therefore, results of this research cannot be generalized or considered as exclusive answers. Either way, the privacy of the participants had to be respected due to the nature of the topic that was addressed. As data collection was done completely anonymously, the validity and reliability of the results cannot be verified.

# 7. ACKNOWLEDGEMENT

First of all, I would like to thank all people that participated in the questionnaire. Due to the sensitive nature of the topic this could not be taken for granted and without their contribution this thesis would not have been made possible. I would also like to express my gratitude towards my supervisors, Prof. Dr. Junger

and Dr. Abhishta. Thanks to their continuous guidance and feedback, the process of writing this thesis was significantly supported by them. Furthermore, I would like to thank P. Peters for his contribution to the study as an expert role. Lastly, I would like to thank my family and friends for proofreading and supporting me throughout the process of writing this thesis.

## 8. REFERENCES


1. Abhishta, A., Junger, M., Joosten, R., & Nieuwenhuis, L. (2019). *Victim Routine Influences the Number of DDoS Attacks: Evidence from Dutch Educational Network*. Retrieved from https://www.researchgate.net/profile/Abhishta_Abhishta/publication/335945402_Victim_Routine_Influences_the_Number_of_DDoS_Attacks_Evidence_from_Dutch_Educational_Network/links/5d89daeea6fdcc8fd61b39ce/Victim-Routine-Influences-the-Number-of-DDoS-Attacks-Evidence-from-Dutch-Educational-Network.pdf
2. Borrion, H. (2013). Quality assurance in crime scripting. *Crime Science*, *2*(1). https://doi.org/10.1186/2193-7680-2-6
3. Carley, K. (1993). Coding Choices for Textual Analysis: A Comparison of Content Analysis and Map Analysis. *Sociological Methodology*, *23*, 75. https://doi.org/10.2307/271007
4. CISA. (2019, November 20). Understanding Denial-of-Service Attacks | CISA. Retrieved May 20, 2020, from https://www.us-cert.gov/ncas/tips/ST04-015
5. Cloudflare. (n.d.-b). What Is The High Orbit Ion Cannon (HOIF)? Retrieved May 20, 2020, from https://www.cloudflare.com/learning/ddos/ddos-attack-tools/high-orbit-ion-cannon-hoic/
6. Cloudflare. (n.d.-c). What Is The Low Orbit Ion Cannon (LOIC)? Retrieved May 20, 2020, from https://www.cloudflare.com/learning/ddos/ddos-attack-tools/low-orbit-ion-cannon-loic/
7. Cloudflare. (n.d.). What is a DDoS Attack? Retrieved May 20, 2020, from https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
8. Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime prevention studies*, *3*, 151-196.
9. Cornish, D., Clarke, R. (2017) "The reasoning criminal: Rational choice perspectives on offending". In: *Environmental criminology and crime analysis*, pp. 29–38. Dehghanniri, H., & Borrion, H. (2019). Crime scripting: A systematic review. *European Journal of Criminology*. https://doi.org/10.1177/1477370819850943
10. Dehghanniri, H., & Borrion, H. (2019). Crime scripting: A systematic review. *European Journal of Criminology*, 147737081985094. https://doi.org/10.1177/1477370819850943
11. Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*, *44*(5), 643–666. https://doi.org/10.1016/j.comnet.2003.10.003
12. Karami, M., & McCoy, D. (2013). *Understanding the Emerging Threat of DDoS-As-a-Service*. Retrieved from https://www.usenix.org/system/files/conference/leet13/leet13-paper_karami.pdf
13. Keary, T. (2019, July 30). DOS vs DDOS attacks: The Differences and How To Prevent Them. Retrieved May 20, 2020, from https://www.comparitech.com/net-admin/dos-vs-ddos-attacks-differences-prevention/
14. Khandkar, S. H. (2009). Open coding. *University of Calgary*, *23*, 2009.
15. Krippendorff, K. (1989). *Content analysis: An introduction to its methodology*. Sage publications.
16. Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39–53. https://doi.org/10.1145/997150.997156
17. Miró-Llinares, Fernando. (2014). Routine Activity Theory. 10.1002/9781118517390/wbetc198.
18. Noroozian, A., Korczyński, M., Gañan, C. H., Makita, D., Yoshioka, K., & van Eeten, M. (2016). Who Gets the Boot? Analyzing Victimization by DDoS-as-a-Service. *Research in Attacks, Intrusions, and Defenses*, 368–389. https://doi.org/10.1007/978-3-319-45719-2_17
19. Radware. (n.d.). DoS Attack: What is a Denial-of-Service Attack? | DDoSPedia. Retrieved May 20, 2020, from https://security.radware.com/ddos-knowledge-center/ddospedia/dos-attack/
20. Rechtbank Zeeland-West-Brabant. (2013, December 20). ECLI:NL:RBZWB:2013:9954, Rechtbank Zeeland-West-Brabant, C/02/273719 / KG ZA 13-759. Retrieved June 1, 2020, from https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBZWB:2013:9954&showbutton=true&keyword=ddos+school
21. Research Methodology. (n.d.). Exploratory Research. Retrieved June 2, 2020, from https://research-methodology.net/research-methodology/research-design/exploratory-research/
22. Rice, D. (2017, August 21). DDoS Attacks on Schools – Why Schools are an Easy Target for Cyber Crime. Retrieved March 16, 2020, from https://diamondit.pro/cybercrimes/ddos-attacks-schools-schools-easy-target-cyber-crime/
23. Riza', A., Yusof, R., Udzir, N. I., & Selamat, A. (2019). Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), 292. https://doi.org/10.1504/ijdet.2019.097849
24. Ryan, G. W., & Bernard, H. R. (2003). Techniques to Identify Themes. *Field Methods*, *15*(1), 85–109. https://doi.org/10.1177/1525822x02239569
25. Santanna, J. J., van Rijswijk-Deij, R., Hofstede, R., Sperotto, A., Wierbosch, M., Granville, L. Z., & Pras, A. (2015). Booters - An analysis of DDoS-as-a-service attacks. *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 243–251. https://doi.org/10.1109/inm.2015.7140298
26. Van Wyk, B. (2012). Research design and methods Part I. *University of Western Cape*.
27. Ward, B. (2014, December 19). Students expelled, face charges in St. Charles school computer hacking. Retrieved June 3, 2020, from https://www.chicagotribune.com/suburbs/ct-students-expelled-st-charles-tl-20141219-story.html
28. White, M.D., & Marsh, E.E. (2006). Content Analysis: A Flexible Methodology. Library Trends 55(1), 22-45. doi:10.1353/lib.2006.0053
29. Wickert, C. (2019, June 4). Routine Activity Theory (RAT). Retrieved June 7, 2020, from https://soztheo.de/theories-of-crime/rational-choice/routine-activity-theory-rat/?lang=en

# 9. APPENDIX

## Appendix A: Additional results from Data Analysis

| Table 13. Whether respondents were pleased with the outcome of their attack | | |
|---|---|---|
| *Yes* | 7 | *78%* |
| *No response* | 2 | *22%* |
| *Total* | *9* | *100%* |

| Table 14. Whether classmates were pleased with the DDoS attack | | |
|---|---|---|
| *Divided opinions* | 4 | *44%* |
| *Yes* | 3 | *33%* |
| *No one noticed* | 2 | *22%* |
| *Total* | *9* | *100%* |

## Appendix B: Questionnaire protocol:

1) How did you first hear about the possibility of DDoSing?
2) What service did you use to execute the DDoS attack?
   a) Low Orbit Ion Cannon
   b) DDoS-for-hire
   c) High Orbit Ion Cannon
   d) Other: please specify below
3) How many times did you DDoS your educational facility?
4) Do you remember at what time of day you launched the (biggest) DDoS attack?
5) What was your goal when DDoSing? What did you try to achieve?
   a) Prevent an exam
   b) For fun
   c) Delay an assignment
   d) Revenge
   e) Other: please specify below
6) Did you achieve what you wanted? What was the impact of your (biggest) DDoS attack?
7) What was the volume / intensity of your (biggest) attack in terms of gigabits per second?
8) At the time, what made you believe you were not going to be caught?
9) Do you think the same today?
10) Were others involved in executing the DDoS attack?
11) If yes, where did you know these others from?
12) Were you pleased with the outcome?
13) Do you think other students were pleased as well?
14) Did anyone know it was you?
    a) School
    b) Family
    c) Police
    d) Friends

15) Looking back at your (biggest) DDoS attack, was it difficult to execute?
16) What do you think about your educational facility / school / university? What is your relationship with the teachers?