Cyber Security Risk Assessment of a DDoS Attack

Gaute Wangen[1], Andrii Shalaginov[1], and Christoffer Hallstensen[2]

[1]NISlab, Norwegian Information Security Laboratory,
Center for Cyber and Information Security,
[2]IT Services,
NTNU
{firstname.lastname}@NTNU.no

Abstract. This paper proposes a risk assessment process based on distinct classes and estimators, which we apply to a case study of a common communications security risk; a distributed denial of service attack (DDoS) attack. The risk assessment's novelty lies in the combination both the quantitative (statistics) and qualitative (subjective knowledge-based) aspects to model the attack and estimate the risk. The approach centers on estimations of assets, vulnerabilities, threats, controls, and associated outcomes in the event of a DDoS, together with a statistical analysis of the risk. Our main contribution is the process to combine the qualitative and quantitative estimation methods for cyber security risks, together with an insight into which technical details and variables to consider when risk assessing the DDoS amplification attack.

1 Introduction to InfoSec Risk Assessment

To conduct an information security (InfoSec) risk analysis (ISRA) is *to comprehend the nature of risk and to determine the level of risk* [2]. InfoSec risk comes from applying technology to information [6], where the risks revolve around securing the confidentiality, integrity, and availability of information. InfoSec risk management (ISRM) is the process of managing these risk while maximizing long-term profit in the presence of faults, conflicting incentives, and active adversaries [19]. Risks for information systems are mainly analyzed using a probabilistic risk analysis [3, 17], where risk is defined by estimations of consequence for the organization (e.g. financial loss if an incident occurred) and the probability of the risk occurring within a time interval. ISRA is mostly conducted using previous cases and historical data. Depending on statistical data (quantitative) alone for risk assessments will be too naive as the data quickly become obsolete [18] and is limited to only previously observed events [16]. While the subjective (qualitative) risk assessment is prone to several biases [11] (Part II) [16]. ISRM methods claim to be mainly quantitative [6, 8] or qualitative [7], but the quantitative versus qualitative risk situation is not strictly either-or. There are degrees of subjectivity and human-made assumptions in any risk assessment, and the intersection of these two approaches remains largely unexplored. The goal of

this paper is to explore this intersection and discuss the benefits and drawbacks from each approach, and how they can complement each other. Moreover, we will discuss alternative ways of expressing uncertainty in risk assessment.

The remainder of the paper is structured as follows: The two following subsections introduces the reader to Distributed Denial of Service attacks and discusses the related work in ISRA. The Section 2 provides a brief description of the DDoS attack and development trend. Also, we present the method applied for ISRA and statistical analysis of the DDoS attack. Later in the Section 3 we give an insight into the qualitative ISRM approach together with results and the quantitative risk assessment in the Section 4 based on statistical methods. Lastly, we discuss and conclude the results, the relationship between this work and previous ISRA work, limitations and propose future work in the Section 5.

1.1 Distributed Denial of Service Attacks

A denial of service (DoS) occurs when an ICT (Information and Communication Technology) resource becomes unavailable to its intended users. The attack scenario is to generate enough traffic to consume either all of the available bandwidth or to produce enough traffic on the server itself to prevent it from handling legitimate requests (resource exhaustion). The attacker needs to either exploit a vulnerable service protocol or to exploit network device(s) to generate traffic, or to amplify his requests via a server to consume all of the bandwidth. The DoS attack is distributed (DDoS) when the attacker manages to send traffic from multiple vulnerable devices. The attacker can achieve amplification through the exploitation of vulnerable protocols or through using botnets.

The increase of Internet throughput capacity has also facilitated the growth in traffic volume for DDoS-attacks. According to Arbor Networks, the largest observed attack in 2002 was less 1 Gbps (Gigabit per second). While the biggest observed attack until now targeted a British television channel and reportedly generated $\approx$ 600 Gbps of traffic. That is an approximate 60x development in capacity for DDoS attacks over the course of about 14 years, see Fig. 1.

1.2 Related work in ISRA

The ISRA approach presented in this paper primarily builds on two previous studies; firstly, Wangen et.al.'s [17] Core Unified Risk Framework (CURF), which is a bottom-up classification of nine ISRA methods. The motivation behind CURF, was that there are several ISRA methods which conduct similar tasks, but there is no common way to conduct an ISRA. The approach ranked as most complete in CURF was ISO27005 [3] (from this moment referred to as ISO27005), while ISO27005 has many strengths, such as the process descriptions and taxonomies, one of the primary deficits of the ISO27005 is the lack of variables to consider and risk estimation techniques. The proposed approach in this paper builds on ISO27005 and addresses the outlined issues by defining classes and estimations for each step. Second, the probabilistic model presented in this paper builds on the feasibility study conducted by Wangen and Shalaginov [18], which

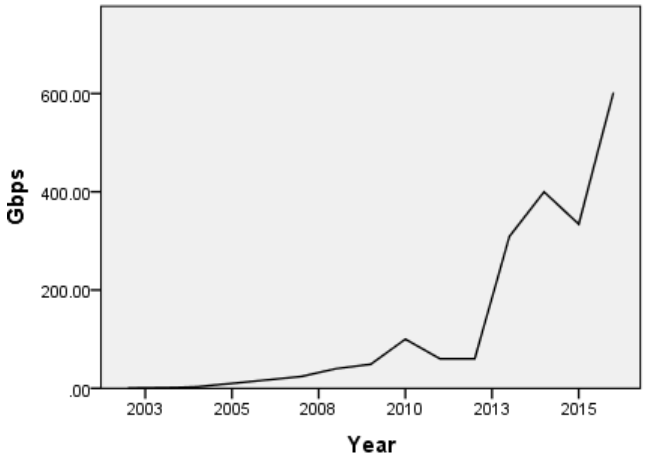


Fig. 1. The development of bandwidth consumption (Gbps) of DDoS-attacks during the last 15 years. *Data source: Arbor Networks and media reports*

discusses statistics and *Black Swan* (see Taleb [16]) issues in ISRA. The Authors [18] found that there are Black Swan related aspects of the ICT domain that may render past observations (Statistics) inappropriate for probability, such as for novel and unique attacks, and the fast development of ICT, for example, Fig. 1. However, the authors also found that quantifying and modeling InfoSec risks have utility as long as the risk assessor is aware of the properties of the risk and the domain we are modeling. The Single and Annual Loss Expectancy (SLE/ALE) represent the most developed area of statistics in ISRA, where risk is described as the probability of a loss occurring [6]. Yet, risk must be considered as more than an expected loss [5]. Knowledge-based probabilities represent the main approach in ISRA [17], as previously discussed, there is utility in statistical data. The combination of these two approaches to probability has remained relatively unexplored in ISRA. So, this study proposes to combine a statistical and a qualitative ISRA to address the research gap.

Thus, this paper proposes a step-by-step process model for an ISRA of a distributed denial of service (DDoS) attack, and we apply the model to a real-world case as a proof of concept and feasibility study. The proposed ISRA approach is compliant with ISO27005.

2 Choice of Methods

This section outlines the core risk assessment concepts applied in this paper. First, we present the fundamentals of our risk analysis approach, then the qualitative ISRA method, and, lastly, discuss the statistical methods employed for quantitative analysis. Our overarching approach to validation is case study.
The proposed approach is based on the two ISO27005 steps (i) *Risk Identification*

-process of finding, recognizing and describing risks [2], and (ii)*Risk Estimation - process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable* [2]. We go further proposing classes and estimations for qualitative asset evaluation, and vulnerability, threat, and control assessment, together with both quantitative and qualitative risk estimations.

2.1 Fundamentals of risk analysis

Our proposed ISRA approach builds on the *set of triplets* as defined by Kaplan and Garrick [12], *Scenario, Likelihood*, and *Consequences*. In which we define the scenario as a combination of assets, vulnerability, threat, controls, and outcome. Each step in the approach generates useful knowledge in on its own, for example, a thorough threat assessment will provide information regarding opponents that are also useful in other risk-related activities and decision-making.
We combine the two approaches to risk and probability proposed by Aven [5]: (i) the frequentist (*"the fraction of times the event A occurs when considering an infinite population of similar situations or scenarios to the one analyzed"*), and (ii) the subjective knowledge-based probability (*"assessor's uncertainty (degree of belief) of the occurrence of an event"*). In terms of risk analysis, the key components of a risk (R) related to an activity for discussion and calculation are as follows [4] (p.229): R is described as a function of events (A), consequences (C), associated uncertainties (U), and probabilities (P). U and P calculations rely on background knowledge (K) which captures the qualitative aspect of the risk, for example, low K about a risk equals more U. Model sensitivities (S) display the underlying dependencies on the variation of the assumptions and conditions. Thus, $R = f(A, C, U, P, S, K)$ allows for a comprehensive output and incorporates the most common components of risk.
In the following section, we define the classes and estimators for each of the key elements of InfoSec risk as subjective knowledge, where the classes describe and categorize the risk components, and the estimators represent qualitative estimations based on expert knowledge and collected data. We do not define the scales for each estimator in this paper as this is individual for each organization.

2.2 Proposed Methodology for Qualitative Risk Analysis

The proposed qualitative methodology is based on descriptions, classes, and estimators. Based on ISO27005 we defined these for Assets evaluation, Vulnerability assessment, Threat assessment, and Control Assessment.

Asset identification and Evaluation.
To start, the Institution needs to identify and know its assets. We define *Asset Identification* as the process of identifying assets, while asset *Evaluation* assess their value, importance, and criticality. According to ISO27005[3] Annex B, there are two primary assets, (i) Business Processes & activities and (ii) Information. While *Asset Container* identifies where assets are stored, transported, and processed [7].

As a part of the process, we map the organizational goals and objectives for risk assessment, as these are important in deriving security goals for the InfoSec program. Also, we consider these when determining the risk event outcome.

- Assets - Something of value to the organization, person, or entity in question.
- Asset type - Description of the asset class, E.g. sensitive information.
- Asset Container - refers to where and how the asset is stored [7].
- Asset value - Estimated, either monetary or some intangible measurement of value
- Importance in Business Process is an estimation of the criticality of the asset in daily operations
- Asset criticality is the comprehensive assessment of the asset value and role in business process estimations.

Vulnerability Assessment
Vulnerability Identification is the process of identifying vulnerabilities of an asset or a control that can be exploited by a threat [2]. Vulnerability *Assessment* is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. Vulnerabilities can be discovered through many activities, such as automated vulnerability scanning tools, security tests, security baselining, code reviews, and penetration testing. In the case of network penetration from a resourceful attacker, the analyst should also consider the *attacker graph*: how compromising one node in the network and establishing a foothold in the network can be exploited to move laterally inside the network and compromising additional nodes.

- Vulnerability type - A classification and description of vulnerability, *weakness of an asset or control that can be exploited by one or more threats* [2].
- Attack description - description of the attack for single attacks such as DDoS, or *attacker graph* where the adversary obtains access to an asset or asset group. The attacker graph is a visual representation of how the attacker traverses the network and gains access to an asset or a group of assets.
- Attack difficulty - Estimation, how difficult is it to launch the attack?
- Vulnerability severity - Estimation of the seriousness of the vulnerability
- System Resilience - How well will the system function under and after an assault, especially important for availability related risk
- Robustness - is the measure of how strong an attack will the system absorb.
- Exposure assessment - Determines exposure of entity's assets through the vulnerability and attack

Threat Identification and Assessment.
Threat identification is the process of identifying relevant threats for the organization. A Threat is a potential cause of an unwanted incident, which may result in harm to a system or organization [2]. Besides mother nature, the threat is always considered as a human. For example, the threat is not the computer worm, but the worm's author. While the threat *Assessment* comprises of methods and approaches to determine the credibility and seriousness of a potential threat. The

assessment process relies on the quality of threat intelligence and understanding of the adversary. For each threat, we propose to consider the following classes and estimators:

- Threat actor - Describes the human origin of the threat. There are several classes of threat agents in InfoSec, for example, malware authors, Cyberspies, and hackers.
- Intention - Defines what the threat actor's objectives with the attack, for example, unauthorized access, misuse, modify, deny access, sabotage, or disclosure.
- Motivation - Defines the primary motivation for launching the attack, previous work on malicious motivations [13] suggests Military or Intelligence, Political, Financial, Business, Grudge, Amusement, Self-assertion, Fun, and Carelessness.
- Breach type - which type of security breach is the threat actor looking to make; either confidentiality, integrity, availability, non-repudiation, or accountability.
- Capacity - Estimation of the resources he/she has at their disposal to launch the attack. For example, if an attack requires a lengthy campaign against your systems to succeed, the threat actor must have the resources available to launch such an attack.
- Capability - Estimation the threat's *know how and ability* for launching the attack.
- Willingness to attack - Estimation of how strong the motivation is to attack. For example, historical observations of the threat actor's frequency attacking the system is a good indicator.
- Threat severity is the comprehensive assessment of the above variables and the main output of the process.

Control Efficiency Estimation

Existing controls are measures already in place in the organization to modify risk [2]. *Control identification* is the activity of identifying existing controls for asset protection. *Control (efficiency) Assessment* are methods and approaches to determine how effectively the existing controls are at mitigating an identified risk.

The important issue to consider here is if the control sufficiently mitigates the risk in question. If the control is considered adequate, the risk can be documented for later review.

- Control Objectives - a written description or classification of what the control is in place to achieve.
- Control domain - Addresses in what domain the identified control is, either in the physical, technical, or administrative [9] (P.166-167).
- Control class - Addresses what the control is supposed to achieve; either prevent, detect, deter, correct, compensate or recovery [9] (P.166-167).
- Risk Event components - Consists of the *Asset Criticality*, *Exposure Assessment*, and *Threat Severity* for the identified risk event.

– Control efficiency - Estimation, addresses how efficient the control is at modifying the identified threat event and how well it achieves the control objectives.

2.3 Methodology for statistical risk analysis

The main statistical approaches considered in this paper are for theoretical analysis of the supplied historical data to run calculations. The motivation is to use conventional statistical methods to extract particular characteristics that are suitable for Quantitative ISRA. Additionally, we make hypotheses about an applicability of each particular method concerning available data. The calculations in this article are based on DDoS attacks data from the Akamai Technology's *State of the Internet* Reports (duration and magnitude) [1] and data gathered from the assessed case study institution on occurrence. These data are considered as quantitative observation of metrics of selected events, for example, some DDoS attacks over time. We utilize several community-accepted methods to deal with the historical data when it is necessary to make predictions in numbers. In particular, these are *Conditional Probability* and *Bayes Theorem*. First, the probabilistic model $p(x)$ is suggested and the corresponding set of parameters are estimated from the data to fit suggested distribution. In sequence, we apply statistical testing, which is an important part of our work since further for the DDoS case study we will justify the usage of a specific statistical method and make a hypothesis about their applicability. By testing, we can make a quantitative analysis of different statistical models quality. However, this is based only on pure analysis of the case's data and deducing the most applicable model that can describe the data and fit the purposes. The testing is suitable for determining whether the data follow a particular distribution model with some degree of defined beforehand confidence interval measured in %. The tests evaluate the actual observed data O with the expected data E from the hypothesized distribution. This is done with a help of QQ-PLOT or Quantile-Quantile plot representing a probability plot by depicting expected theoretical quantiles E and observed practical quantiles O against each other. The quality of hypothesized data distribution can be evaluated using linearity in this plot. It means that if the expectations match observations, even with some minor outliers, then the null hypothesis can be rejected, and data fit selected distribution. Second, the probabilistic model can be used to estimate the probability of similar events in this very period or later on. We observe the following well-known shortcomings of the probabilistic modeling. First, very few data points from history may cause a wrong decision. Second, very rare events have negligibly small probabilities which might cause trouble in predicting corresponding outcomes. The authors have applied the statistical analysis software IBM *SPSS*, GNU *PSPP* and *RapidMiner*. Later on, we also discuss the application of this methodology and possible ways of its improvement.

3 Case Study: Qualitative Risk Assessment of a DDoS attack

The case data together with relevant available statistics was collected from an institution whose IT-operations delivers services to about 3,000 users. The Case study Institution (hence referred to as "The Institution") is a high-availability organization delivering a range of services to the employees and users, mainly within research and development. The objectives of the IT-operations is to deliver reliable services with minimal downtime. The target of this study has a 10 Gbps main fiber optics connection link, which is the threshold of a successful DDoS attack. Fig. 2 displays the institution's network capacity and average traffic during regular weekdays, this case study considers attacks on the main link. During the five previous years, the Institution has had an average annual occurrence of two DDoS attempts, whereas none has been successful thus far. The goal of this assessment is to derive the qualitative risk of the Institution experiencing a successful attack by applying the proposed method.
The case study starts with asset identification and evaluation, further, considering vulnerabilities, threat assessment, control efficiency, and outcomes. Our contribution in this section is the application of the classes and qualitative estimators for each step of the risk assessment process.

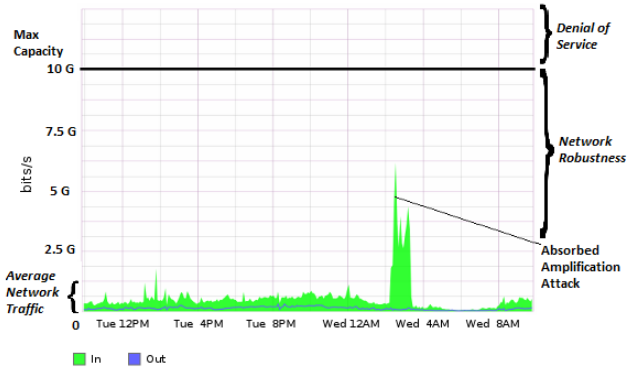


Fig. 2. Illustration of Network robustness with an absorbed amplification attack. Network capacity at 10 Gbps, everything above constitutes a DoS.

Case Asset Evaluation. A DDoS attack is primarily an attack on the availability of the organization's Internet connection. We compare the Internet connection capacity with a pipeline; it's capacity limits the pipe's throughput. Once the capacity is filled, no additional traffic can travel through the pipe. The attacker's goal is to fill the pipeline with traffic and effectively block all legitimate traffic from traveling through the pipe.
In the considered case, a successful DDoS attack will lock the users out of the

network and prevent them from conducting their connectivity-dependent tasks. Most of the organization's value chain is dependent on some level of connectivity, which makes the availability of services and assets the top priority when considering DDoS attacks. For simplicity, we consider "Service" as the main asset. As the institution is high availability and has up-time as one of the top priorities, service delivery is seen as crucial for production. Table 1 shows the classification and estimation considered for protection in the case study.

Table 1. Asset considerations for the DDoS attack

Asset type	**Container**	**Protection Attribute**	**Importance in Business Process**	**Asset value**	**Asset Criticality**
Service delivery	Infrastructure - Internet Pipeline	Availability	Essential (70-100)	Very high (50-85)	Essential (70-100)

Case Vulnerability Assessment Results. The Institution is exposed to several attack vectors for achieving DoS; for example resource starvation, application layer-based, and volumetric/flood. We provide a technical description of one attack, together with a vulnerability assessment. These estimations assume a 10 Gbps connection and the current security level in the Institution.
We measure the robustness in the DDoS-case in the gap between maximum network capacity and average traffic, illustrated in Fig. 2. A narrow gap between average load and maximum capacity is an indicator of fragility towards traffic generating attacks. To describe the network robustness we look at the maximum load versus the average load and measure the gap. The average load on the network is ≈ 1 Gbps; the system can absorb DDoS attacks up to ≈ 9 Gbps before the users experience denial of service, Fig. 2.
On resilience, the network will continue to function within acceptable service delivery up to traffic of about approximately 6-9 Gbps, depending on several variables such as weekday and hours, before users start to experience a degradation in service. Although attacks in this vicinity do not entirely cause a DoS, they reduce the latency in the network and efficiency of the workforce.
Based on our assessment of the network, we define four events (A) for further assessment:

1. Attacks less than 6 Gbps which will be absorbed by the network robustness and will go by unnoticed by the users. (A1)
2. Attacks ranging 6-9 Gbps can cause reduction of service in the network. (A2)
3. Attacks ranging above 9 Gbps will cause DoS together with day-to-day use. (A3)
4. Attacks ranging from approximately 50 Gbps carry the potential for causing damage at the Internet Service Provider (ISP) level but carry the same consequences for the institution. (A4)

Attacks need to be able to generate a traffic within the ranges of scenarios A2 - A4 to be considered a threat potential threat in the case study, for illustration purposes, we only considered volumetric and flood-based attacks. The Institution's vulnerability is then the generic network capacity; we assume that no vulnerable services are running on the Institution's internal network. *Volumetric and flood based* attacks aims to saturate the amount of connections to the Link, through UDP (User Datagram Protocol) amplification generating a small amount of data from the attacker resulting in a lot of data traffic to the victim. UDP DDoS attacks exploit the fact that the UDP does not require a handshake to transmit data, and requires the service to return more bytes than the attacker sent with spoofed source IP. Hilden [10] provides the following example, *services running a vulnerable CharGen (Character generator protocol) can be exploited to generate traffic: the attacker sends a 1-byte sized packet with a spoofed IP (the target's IP) to the vulnerable servers. Due to no handshake, the servers immediately responds with a 1024 byte large packet to the target IP. The attacker can amplify his traffic (bytes sent) with 1024x (bytes received by the target) by exploiting one vulnerable server.* The Table 2 represents the attacker's bandwidth limits the attack.
The UDP amplification attack requires access to either a botnet or vulnerable service, both of which are readily available on the Internet, the former for hire and the latter for exploitation. The technical expertise required to launch an attack is low, where the trick is to locate vulnerable services through scans. The attacker can create traffic volumes in the ranges A2-A4, whereas attacks within ranges A2 and A3 are easily achieved with a low number of vulnerable services, Table 2. The A4 scenario requires more resources regarding bandwidth and services, but is still easily achieved for the technically skilled.
With a 10 Gbps connection, the Institution is inherently vulnerable to DDoS attacks, and since this is an attack on availability, the duration of the attack is also important to consider. We have defined the following downtime scenarios according to the Institution's risk tolerance:

1. Attack ranging between 0-10 min are considered negligible. (B1)
2. 11-30 min will produce a slight loss in production. (B2)
3. 31 - 120 min will produce a moderate loss in production, it is also likely that employees will seek out the helpdesk and cause extra overhead. (B3)
4. 2 - 24 hours will produce a critical loss in production, at this point everyone will have exhausted their tasks that can be solved without connectivity. (B4)
5. >24 hours will qualify as a catastrophe. (B5)

The Institution is exposed to volumetric and flood-based attacks due to ease of exploitation and effective amplification. Attacks ranging within A2-A3 are easily achievable with an initial technical insight, while ability to maintain the attack up to scenarios B3-B4 depend on a number of externalities that have a high level of uncertainty related to them, such as internal reaction time, threat capacity, and ISP capabilities. We address uncertainty related to the threat actor in the next section.

Table 2. Examples of approximate amplifications by exploiting vulnerable UDP, including possible amplification of the 100 Mbps connection. *Data source: Hilden[10], Norwegian Security Authority (NSM)*

Protocol	**Amplification Ratio**	**100 Mbit/s ⇒**
NTP	1:556	55.6 Gbit/s
CharGen	1:358	35.8 Gbit/s
QOTD	1:140	14 Gbit/s
Quake (servers)	1:63	6.3 Gbit/s
DNS (open resolver)	1:28-54	2.8 - 5.4 Gbit/s
SSDP	1:30	3 Gbit/s
SNMP	1:6	600 Mbit/s
Steam (Servers)	1:6	600 Mbit/s

Case Threat Assessment Results. Based on the exposure assessment, we identify and assess one threat actor in the position to trigger the attacks. For the threat actor, we consider the motivation, intention, willingness, capacity, and capability, to determine threat severity. The amplification attacks in question are easy to implement as long as vulnerable services are running, so, the analyst should consider less able attackers. However, for the case study we consider only one threat actor based on the estimated properties regarding the specifically analyzed DDoS attack:
Actor 1 is the politically motivated hacktivist whose weapon of choice is commonly the DDoS attack. Due to some of the research conducted in the Institution being controversial, they are the a potential target of Actor 1. We estimate the capacity for maintaining a lengthy attack (B3-B4) as *Moderate* and the capability for launching the attacks A2-A5 as *Very high*. It is uncertain whether this actor has been observed attacking their networks in the past, Table 3.

Table 3. Threat assessment for DDoS attack, K represents confidence in the estimates

Threat Actor	**Motivation**	**Intention**	**Capacity**	**Capability**	**Willingness**	K	**Threat Severity**
Actor 1	Political	Disruption	Moderate	Very high	Moderate	Low	High
Actor 2	Military or Intelligence	Access	Very high	Very high	Very low	Medium	Medium
Actor 3	Self-assertion	Deny Access	Low	Medium	Very high	High	Medium

Control Assessment Case Results. We provide a description of countermeasures for the considered attack, together with an estimation of efficiency which, for reactive controls, can be measured in time until the attack is mitigated.
In the case organization, the first and primary control strategy is to filter vulnerable UDP protocols on ingress network traffic. This control limits the attack surface of the organization's network and limits the effectiveness of exploiting vulnerable UDP based protocols. This control does not completely mitigate the possibility of attack because there is still network nodes that need to respond to UDP like Network Time Protocol and Domain Name System, but these are

configured to provide low possibility for amplification values so that threat actors cannot effectively use them for attacking other systems on the Internet.
The second available mitigation strategy is to have a close cooperation with the Internet service provider's CSIRT. This control is vital because of the ISP's capabilities to blackhole (null-routing), rate-limit or even block network traffic that originates outside of their own network, or the country itself. For large DDoS attacks, the ISP is the only one capable of filtering away this traffic efficiently. On a day-to-day basis and within normal work hours, to involve the ISP CSIRT to start shaping or blocking traffic is highly effective and possible to implement within 1 to 2 hours. After working hours, 2 to 5 hours is estimated.

Table 4. Control efficiency estimation. K represents confidence in the estimates

Control Objectives	**Control Domain**	**Control class**	K	**Control Efficiency**
1. Filter UDP traffic	Logical	Preventive	Medium	*Medium*
2. Agreement with upstream ISP	Organizational	Reactive	High	*High*

3.1 Events and Results

The *Event outcomes* describes the range of outcomes of the event, consisting of asset, vulnerability, threat, and control, and how it affects the stakeholders and the organization. The process consists of identifying and describing the likely outcome(s) of the event regarding breaches of confidentiality, integrity, and availability, which does not entail calculations of consequence, as this is performed in the risk analysis. For example, an event outcome can have a financial impact or an impact on reputation.
The qualitative risk assessment shows that the most severe risk facing the organization is a DDoS campaign in the ranges A3-A4 ($>$ 9 Gbps) and lasting longer than 2 hours (B4-B5). The Institution is currently vulnerable to such attacks due to the dependency on connectivity for running business processes. There is currently one politically motivated threat actor with a high capability of launching such an attack, but a moderate capacity for maintaining a lengthy campaign. We estimate the existing controls to be quite efficient to mitigate UDP amplification attacks, although the upstream ISP option includes third party dependencies which the institution does not control and introduces another layer of uncertainty. We continue the ISRA with the quantitative assessment of available real-case data from Akamai in the next section.

4 Quantitative Risk Analysis

The Risk analysis phase consists of estimating risk concerning $R = f(A, C, U, P, S, K)$. We assign the identified adverse outcomes, section 3.1, probability according to

previous observations and subjective knowledge. A (event) is the result of the risk identification process and in the analysis described as a range of adverse outcomes based on the consequence calculations. There are primarily two approaches to probability, frequentist or subjective knowledge-based assessments (quantitative and qualitative). This section starts with the quantitative risk approach, before combining it with the qualitative results to obtain the risk.

4.1 Risk Calculations

The goal of the risk estimation is to reduce U related to risk occurring. For $P\&C$ calculations, we suggest merging the objective data gathered through observations and statistics with the subjective knowledge-based probabilities. We define the following:

- *Quantitative Assessment (Objective data)* - prior frequencies of occurrence, including past observations of the risk and generic risk data used to derive objective measurements of probability. Together with the gathering of relevant metadata through observations made by others.
- *Qualitative Assessment (Knowledge-based data)* - a combination of knowledge that is specific to the organization and the threat it is facing. Primarily derived from the *risk event components*, section 3.
- *Risk Estimate* - The final estimate of the probability for the risk, derived from quantitative and qualitative data.

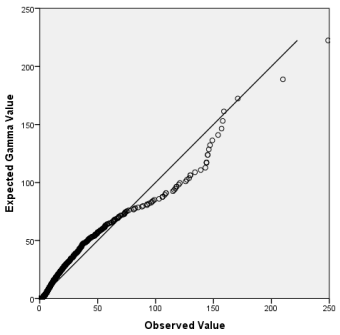
The consequence estimation is derived primarily from two factors, monetary loss and intangible losses such as loss of reputation. Besides, the consequence estimation should consider the organizational objectives and goals [3]. The loss calculation is challenging as complex systems may fail in unpredictable ways. Possible data sources and input for consequence/impact considerations: prior loss data, monetary losses, consequences for organizational goals and objectives, and risk specific factors such as response time and attack duration.

Observed Frequencies of DDoS Attacks. By monitoring activity, we can obtain reliable numbers on how large the average DDoS attack and generate corresponding reports. The data applied in this article was provided by Akamai [1], and is based on 4,768 valid observations from 2014-2015, shown in the Tab. 5. There was no observed attack magnitudes over 255 Gbps in the data set. The observed frequencies of attacks towards the case study institution averaged two annual attacks during the last five years, $P_{occ} = \frac{1}{6} \approx 17\%$ of monthly occurrence, none of which have succeeded in attaining the necessary magnitude to achieve DoS. One of which managed to cause instability in the wireless network, thus, classifying as an A2 scenario.

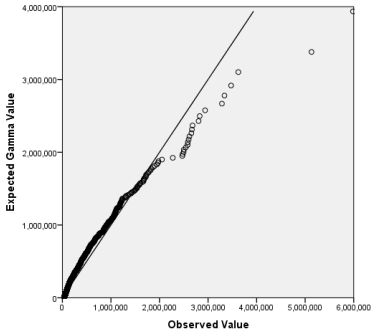
Further, to test our hypothesis about the distribution of the data we used Q-Q plot, depicted in the Fig. 3. The plot shows the dependency between the observed data and expected data according to **Gamma distribution** prediction. Also, one can see two outliers at the high bandwidth interval indicating either unusual events or possible error in logging the characteristics of the events.

Table 5. Frequencies of DDoS Magnitude observations from Akamai Dataset [1].

Characteristic	Valid	Missing	Mean	Median	Std. Dev.	Minimum	Maximum
Duration	4768	0	154,931.00	48,180.00	622,073.00	600	29,965,740.00
Gbps	4768	0	6.09	1.50	15.63	10^{-5}	249.00



(a) γ-distribution for DDoS Gbps



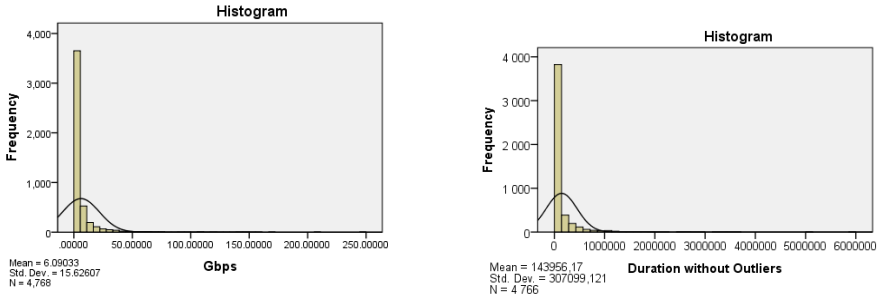
(b) γ-distribution for DDoS Duration

Fig. 3. Fitting DDoS Magnitude and Duration data set by means of Q-Q Plot using γ-distribution. Two outliers are evident at the high end of the range for both distributions.

Observed values for Impact Estimation. By monitoring activity, we can also obtain reliable numbers on the duration of DDoS attacks and generate distributions. Our data provides us with Table 5, the data shows that the documented DDoS durations observed in this period were in the range from 600 up to $29 \cdot 10^6$ seconds, the longest lasting attack lasting approximately 347 days with magnitudes reaching about 4 Gbps. Removing two outliers from the data set gives a new mean value equal to $1.4 \cdot 10^5$ seconds. The Figure 4 displays the data clustering in the area around the mode and median. The majority of the data are distributed in this particular interval. In the case of probabilistic estimation, it means that the data located far from this region are going to have a negligible level of occurrence.

Our tests showed that there is no correlation between the variables "attack duration" and " attack magnitude". There is a small difference between the mean attack durations in the considered outcomes, but it is not statistically significant, Table 6. The A3 attacks seem to have shorter durations than the other; the one-way ANOVA (Analysis of variance model) shows that these two groups of observations are similar only to significance P=85%. Yet, if we combine the A3 and A4 attacks this mean duration rises, and there is no significance.

Fig. 5 depicts the correlation between duration and magnitude, where the attacks from the *A1* and *A2* scenarios are distributed nearly uniformly across the duration scale. It means that the nature of such attacks is more random and non-deterministic, which was also confirmed by our correlation tests. Going



(a) Histogram for DDoS Gbps (b) Histogram for DDoS duration

Fig. 4. Histogram of DDoS magnitudes and durations with normal curve, without two largest outliers. *Data Source: Akamai [1]*

Table 6. Frequencies for the defined events, *A.Data Source: Akamai [1]*

Scenario	Magnitude Gbps	Mean	Median	N	Std. Dev	% of attacks	$P(P_{occ} \wedge A)$
A1	<6	159,956.64	48,900	3,713	682,039.967	77.9	13.2%
A2	6 - 8.9	162,124.35	44,700	331	450,382.579	6.9	2.6%
A3	9 - 49.4	117,437.50	46,080	624	259,646.272	13.1	1.8%
A4	>49.5	178,485.20	52,380	100	284,012.424	2.1	0.4%

further, one can see that the majority of the attacks from the range of *A3* are located in the duration range around $10^3 \cdots 10^6$ seconds. Finally, same stands for the scenario *A4*, where the dispersion of possible magnitudes is large in comparison to *A3*. However, much higher frequency in case of probabilist model suppresses less frequent cases, while fuzzy logic describes data independently from the frequency of its appearance, only taking into consideration its possibility as described before by Shalaginov et.al. [14].

4.2 Probabilistic modeling for Risk Estimation

Unplanned downtime is an adverse event for which most ICT-dependent organizations need to have contingencies. The Institution considered in this paper have defined the severity metrics in Table 7, ranging from "Negligible" to "Catastrophe", together with the distribution of duration within the defined intervals. Losses are considered to be moderate up to two hours downtime, as most employees will be able to conduct tasks that do not require connectivity for a short period. Losses are estimated to start to accumulate after 2 hours of downtime. The analysis shows that the defined events *B3-B5* are over 99% likely to last more than 2 hours, which falls well outside of the Institutions risk tolerance. The conditional probability that the institution will suffer DDoS events in a given month is described in Table 6, right column. The risk estimation is modeled as an *Event tree*, Fig. 6, based on conditional probabilities $P(P_{occ} \wedge A \wedge B)$.

Sensitivity. The most sensitive numbers for the risk calculation is the P_{occ}, which is based on approximately ten observations from the last five years. The

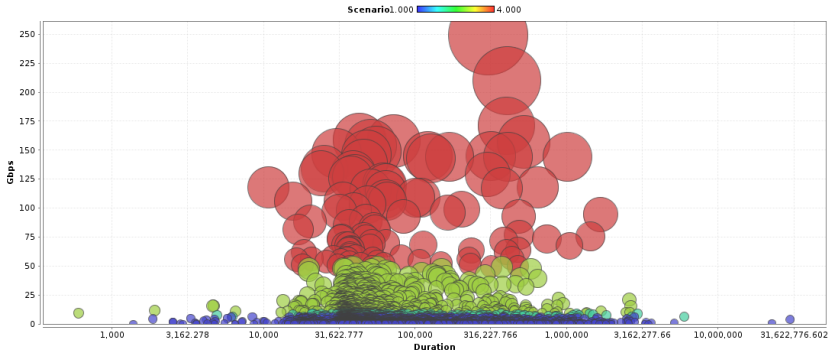


Fig. 5. Bubble plot of the attack bandwidth depending on the duration for each scenario. Size of the bubble also denote magnitude of the attack. Scenarios are depicted with different colours.

Table 7. Overview attack severity for the case study and duration frequencies. *Data Source: Akamai [1]*

Outcome	Interval (min)	Seconds	Severity	Frequency	% of Attacks
B1	0-10 min	0 - 600	Negligible	1	0.0
B2	11-30 min	601 - 1,800	Slight	1	0.0
B3	31 - 120 min	1,800 - 7,200	Moderate	28	0.6
B4	2 - 24 hours	7,201 - 86,400	Critical	3,346	70.2
B5	>24 hours	> 86400	Catastrophe	1,392	29.2

low amount of observations makes the mean sensitive to changes and one can capture this aspect in the analysis by assigning ranges to P_{occ} instead of concrete numbers. A probability range will help to make the assessment more robust, by for example adjusting for a range of 1-6 (or more) occurrences of DDoS attacks every year.

5 Discussion & Conclusion

In this section, we discuss the possibility of adjusting the risk model with additional qualitative input and propose an expanded model. We then discuss the limitations of the work and the potential future directions for the work.

5.1 Adjusting for Knowledge-based probability estimations

The primary objective of the ISRA process is to provide the decision-maker with as good a decision basis as possible. The benefit of the quantitative analysis is that the results are grounded in reality and defensible in a risk communication process. From the other side, the advantage of the qualitative risk assessment is that it allows more dynamic risk assessments. The main fragility of quantitative

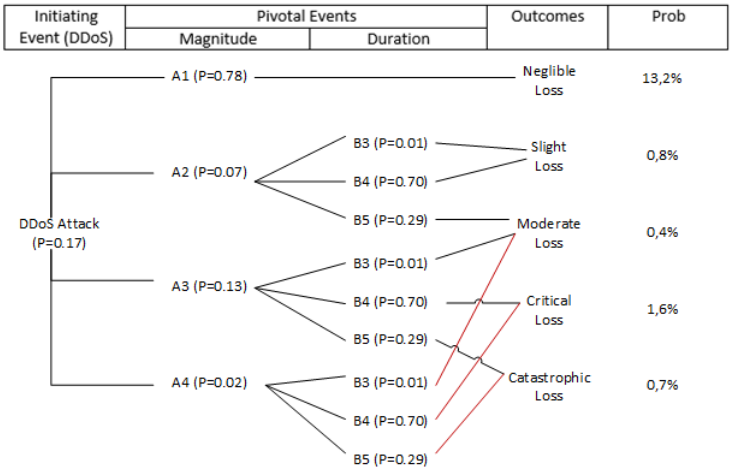


Fig. 6. Event Tree displaying probability of monthly DDoS occurrence for the Case study.

approaches is the dependence on the data quality and quantity of observations. We know about the fast-paced developments in ICT, for example, Fig. 1, showed the progress in capacity for DDoS attacks, and that attack trends may vary which have implications for the annual occurrence (discussed in [18]). The duration and magnitude of γ distributions should be more stable although the observed values are likely to increase according to the trend. However, the limitation of quantitative risk assessments is that attacks may not be present in the dataset, which makes the probabilistic approach less flexible as conducted in Section 4.2. It means that there is a need to have a control or introduce an additional factor that may indicate the possibility of the attacks.

One specific finding is the *Control efficiency*, Table 4, in which we have identified one proactive and one reactive control in place to mitigate an attack. For this discussion, we disregard the proactive control *Filter UDP traffic* as attacks have been occurring at a regular rate even with this control in place. We consider the reactive control, *Agreement with upstream ISP*, as a part of the risk assessment, where, during the workday we can expect an attack to be mitigated within 1-2 hours, and after working hours the handling time is between 2-5 hours. Although our quantitative analysis, Fig. 6, shows the combined risk of a monthly DDoS attack ranging from critical to a catastrophic loss at $\approx 2,3\%$. Further, if we include the control efficiency assessment we can adjust down the risk estimate for DDoS attacks lasting longer than two hours. A caveat here is that we must consider the event of control failure, in this case, we have a high degree of knowledge about the control efficiency and can put more trust in its functionality. However, third party dependency always comes with uncertainties due to information asymmetry problems between the service provider and the institution.

We also have the opportunity to adjust P_{occ} estimates based on the threat assessment, which applies to cases where the attacker attributes changes, for example, willingness to attack in the case of controversial political events. A thorough threat assessment is likely the best data source for more technical and rarer attacks than the DDoS. An understanding of the threat's intention and motivation will also provide a better understanding of possible consequences. The qualitative risk assessment shows that the Institution is facing one serious threat actor who both has the capacity, capability, and moderately willing to launch an attack. At the current time, the UDP-based amplification attack vector is easily exploitable and can generate traffic far beyond system limits to achieve all adverse scenarios between A2-A4. Which means that threat actors with less capacity and capability will be able to produce more powerful attacks. For a more technical and resource intensive attack, it would make sense to consider the threat assessment where the more resourceful threats are linked to the more advanced attacks, for example, Threat *Actor 2* (Table 3) is more likely to be behind attacks in the critical to catastrophic loss events. *Actor 3* will be responsible for most attacks, but due to his limitations in capacity and capability; attacks will primarily be limited to short lasting and small magnitude attacks. While *Actor 2* is rarely observed, but can launch the catastrophic range attacks.

Taking into account both the threat and control assessments, we modify the Event tree to accommodate the qualitative assessment. For the combined assessment, we consider control efficiency concerning subjective ranges for P of a successful attack with Control 2 in place. To operationalize the threat assessment in the model, we have visualized our estimated attack ranges assigned to the identified threat actors in the left column, Fig. 7.

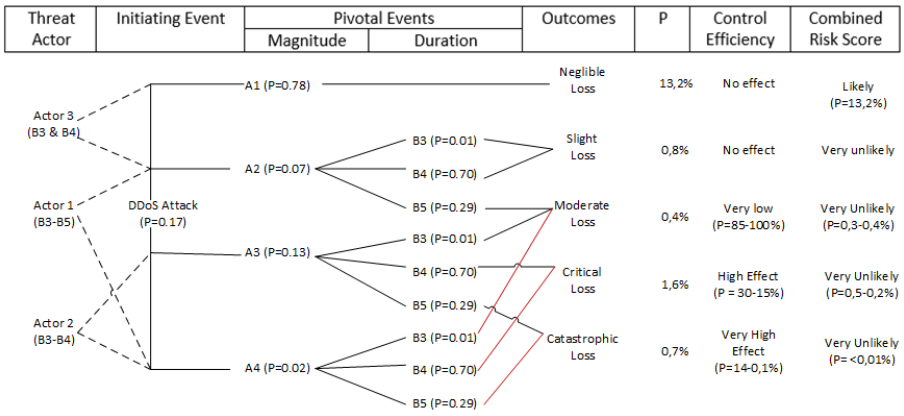


Fig. 7. Expanded Event Tree also including subjective estimates of threat actors and control efficiency.

5.2 Limitations & Future Work

Our work has proposed an approach on how to combine quantitative and qualitative risk estimates. However, there is a limitation in our model due to the combination of the subjective and statistical assessments. We believe that application of possibilistic models such that Fuzzy Logic may help to understand the reasoning of statistical models better when the probabilities of two events are nearly equal and are very small. It means that the difference between two similar events can be below the limit of computing error because the event falls under the category of what Taleb defines as *Extremistan* (see [18, 15]). Therefore, applying a combination of subjective and objective estimators, we will be able to achieve better generalization of the model. Another way to improve the methodology is to use hierarchical models that ensemble inference of human-understandable Fuzzy Rules (also used for decision support) into a comprehensive framework.

We propose to apply our approach to model other cyber risks for further validation. The risk considered in this paper is a very technical communications risk, and the risk model would benefit from testing in areas where historical data is less available. Another limitation is the limited generalization of our case study; the ISRA approach should also be applied to other types of organizations

5.3 Conclusion

In this paper, we have proposed and applied classes and estimators for qualitative ISRA, which should contribute towards making the overall risk assessment process easier and more comprehensive. Our work shows that applying statistical methods for a cyber risk is feasible as long as there is data available. Moreover, with more accurate data there are possibilities for even more accurate and better quality models. Also, we adjusted the quantitative risk estimates with qualitative findings, for example, the definitions of scenario events (A and B) were based on qualitative measures of vulnerability and applied to categorize objective data. This paper also took the merging further by implementing the findings from the qualitative threat and control efficiency assessments into the probabilistic model. The control estimation is crucial to the risk estimation as it directly affects the estimation result, which in our case study made the most severe outcomes very unlikely. Thus, the conclusion is that combination of both the qualitative and quantitative aspects of ISRA is both feasible and beneficial. Defining an ISRM method as either-or in this manner may cause the risk analyst to miss out on valuable information for the assessment.

Acknowledgements

The authors acknowledge Professors Einar Snekkenes, Katrin Franke, and Dr. Roberto Ferreira Lopes from NTNU, Anders Einar Hilden from the Norwegian Security Authority (NSM), Karine Gourdon-Keller, David Fernandez, and Martin McKeay from Akamai. Also, the support from the COINS Research School for InfoSec is highly appreciated. Lastly, we acknowledge the contributions made by the anonymous reviewers.

References

1. 2014-2015 ddos attack duration and magnitude dataset. Technical report, Akamai Technologies, 2015.
2. Information technology, security techniques, isms, overview and vocabulary, ISO/IEC 27000:2014.
3. Information technology, security techniques, information security risk management, ISO/IEC 27005:2011.
4. Terje Aven. *Misconceptions of risk*. John Wiley & Sons, 2011.
5. Terje Aven. The risk concept - historical and recent development trends. *Reliability Engineering & System Safety*, 99:33–44, 2012.
6. Bob Blakley, Ellen McDermott, and Dan Geer. Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms*, pages 97–104. ACM, 2001.
7. Richard A Caralli, James F Stevens, Lisa R Young, and William R Wilson. Introducing octave allegro: Improving the information security risk assessment process. Technical report, DTIC Document, 2007.
8. Jack Freund and Jack Jones. *Measuring and Managing Information Risk: A FAIR Approach*. Butterworth-Heinemann, 2014.
9. Peter H. Gregory. *All in one - CISA - Certified Information Systems Auditor - Exam Guide*. McGraw-Hill Companies, 2012.
10. Anders Einar Hilden. *UDP-Based DDoS Amplification Attacks*. Norwegian Security Authority (NSM), 2015. Lecture held at NTNU (Gjøvik), 07.10.2015.
11. Daniel Kahneman. *Thinking, fast and slow*. Macmillan, 2011.
12. Stanley Kaplan and B John Garrick. On the quantitative definition of risk. *Risk analysis*, 1(1):11–27, 1981.
13. Donald L. Pipkin. *Halting the Hacker: A Practical Guide to Computer Security, Second Edition*. Pearson Education, 2003.
14. Andrii Shalaginov and Katrin Franke. A new method of fuzzy patches construction in neuro-fuzzy for malware detection. In *IFSA-EUSFLAT*. Atlantis Press, 2015.
15. Nassim Nicholas Taleb. Errors, robustness, and the fourth quadrant. *International Journal of Forecasting*, 25(4):744–759, 2009.
16. Nassim Nicholas Taleb. *The Black Swan: The Impact of the Highly Improbable*. Random House LLC, 2nd ed. edition, 2010.
17. Gaute Wangen, Christoffer Hallstensen, and Einar Snekkenes. A framework for estimating information security risk assessment method completeness - core unified risk framework. In *[Submitted for Review]*, 2016.
18. Gaute Wangen and Andrii Shalaginov. *Risks and Security of Internet and Systems: 10th International Conference, CRiSIS 2015, Mytilene, Lesbos Island, Greece, July 20-22, 2015, Revised Selected Papers*, chapter Quantitative Risk, Statistical Methods and the Four Quadrants for Information Security, pages 127–143. Springer International Publishing, Cham, 2016.
19. Gaute Wangen and Einar Arthur Snekkenes. A comparison between business process management and information security management. In M. Paprzycki M. Ganzha, L. Maciaszek, editor, *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems*, volume 2 of *Annals of Computer Science and Information Systems*, pages 901–910. IEEE, 2014.