Quantitative Risk, Statistical methods, and the Four Quadrants for Information Security

Gaute Wangen and Andrii Shalaginov

NISlab, Norwegian Information Security laboratory,
Center for Cyber and Information Security,
Gjøvik University College
{Gaute.Wangen2,Andrii.Shalaginov2}@hig.no

Abstract Achieving the quantitative risk assessment has long been an elusive problem in information security, where the subjective and qualitative assessments dominate. This paper discusses the appropriateness of statistical and quantitative methods for information security risk management. Through case studies, we discuss different types of risks in terms of quantitative risk assessment, grappling with how to obtain distributions of both probability and consequence for the risks. N.N. Taleb's concepts of the Black Swan and the Four Quadrants provides the foundation for our approach and classification. We apply these concepts to determine where it is appropriate to apply quantitative methods, and where we should exert caution in our predictions. Our primary contribution is a treatise on different types of risk calculations, and a classification of information security threats within the Four Quadrants.

Keywords: Risk Assessment, Information Security, Statistical Methods, Probability, Four Quadrants, Black Swan

1 Introduction

Being able to predict events and outcomes provide a great benefit for decision-making in both life and business environments. For information security risk management (ISRM), the aim is to find the appropriate balance in risk-taking relative to the organization's risk appetite and tolerance. Too many security controls will inhibit business functionality, and the opposite will lead to unacceptable exposure. The inherent complexity of information community technology (ICT) makes it challenging to gather enough relevant data on information risks for building statistical models and making quantitative risks calculations [2]. It is therefore generally perceived as being too much work, complex and time-consuming [14]. However, we argue that the cause for the lack of prevalence of statistical methods is just as much lack of maturity in the field as the reasons stated above. Prediction of information security risks has therefore been reliant on the intuition and heuristics of the subject matter experts [2,14]. Although qualitative methods are the predominant approach to forecasting information risks, there is ample evidence from psychological experiments suggesting that qualitative risk predictions are unreliable [13,9,14]. Moreover, the qualitative risk analysis is not suitable when dealing with expected monetary losses such that Annualized Loss Expectancy. Quantitative and statistical methods should provide better results than guesswork and improve decisions in the long run. However, there are many types of information risks, and it is not likely that we can predict all equally well. Information security risks are more often than not products of complex systems and active adversaries. The main topics in Black Swan [13] is risk unpredictability caused by lack of data and knowledge about the complexity and the limitations of statistical methods in predicting risks in such systems. Lack of understanding and overconfidence in models often leads to the costly mistake of underestimating risk. The Four Quadrants [12] is a risk classification system developed primarily for economics for determining where the risk analyst safely can apply statistical methods, where he should show caution, and where to discard traditional statistical approaches. In this article, Taleb's Four Quadrants are adapted to address the feasibility of applying statistical methods to predict information risks. To the extent of our knowledge, there has not been published any previous work on this particular issue.

To provide a clear view on the problem, we did a feasibility study of applying statistical methods to several major information risk case studies that can affect any businesses or even countries. This work addresses the following research questions and finds answers with relevant support from the case studies: (i) *Can we apply statistical methods to deal with Information Security Risks? Sketch the applicability domains and possible failures to predict extreme events* and (ii) *In which information security domains can statistical methods be applied to improve the decision-making process in risk management even if the methods do not seem reliable and accurate?*. The implication from answering these research questions are both theoretical, corresponding knowledge and historical data was collected, simulated and analyzed in this study. For practical implications, a family of various statistical approaches was analyzed with scientifically sound proof for specific methods and applications for ISRM even if the prediction results are not entirely reliable. Furthermore, we discuss factors that contribute to our lack of knowledge about the quantitative ISRM using statistical methods as the most promising approach to numerical characterization of the ICT risks. Additionally, a classification of risks within the Four Quadrants is proposed.

The remainder of this article is as follows: First; we present the state of the art in ISRM in the Section 2, define the terminology and describe the Four Quadrants classification scheme. In the Section 3 we describe the applied method. We present three case studies and their relation to quantitative risk assessment and their relation to the Four Quadrants in Section 4. Section 5 discusses our findings, factors that reduce predictability, and classification of information risks within the Four Quadrants. The conclusion is found in Section 6.

2 Information Security and Risk Assessment

ISO/IEC 27005:2008 defines information or ICT risk in as *the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.* Probabilistic risk analysis (PRA) is the preferred approach to risk in information security. Where impact to the organization (e.g. loss if a risk occurred) and probability calculations of occurrence express risk. There are no standardized statistical approaches to information risks. To calculate risks (R) we, therefore, apply the definitions provided by Aven in [3] (p.229) for discussion and risk calculation. Where risk is described by events (A), consequences (C), associated uncertainties (U) and probabilities (P). U and P calculations rely on background knowledge (K). Also, model sensitivities (S) are included to show how dependencies on the variation of the assumptions and conditions. Thus, *R=f(A, C, U, P, S, K).* A quantitative risk assessment in this sense derives from applying statistical tools and formal methods, mainly based on historical data (e.g. law of large numbers), obtained distributions and simulations. So, based on the definition of risk by Aven, we will consider applications of relevant methods for quantitative risk evaluation in terms of R. A risk assessment is very seldom purely quantitative as there are assumptions K underlying the forecast. Exposure is a crucial concept in risk management that we define as how susceptible an organization is to a particular risk.

2.1 The Black Swan and the Four Quadrants

N.N. Taleb [13] developed Black Swan theory to describe rare, extreme and unpredictable events of enormous consequence. These events, known as Black Swans, are so rare that they are impossible to predict, and they go beyond the realm of reasonable expectations. A Black Swan has three properties; (i) It is an outlier. (ii) It carries an extreme impact. (iii) Moreover, despite its outlier status, human nature makes us formulate explanations for its occurrence after the fact, rendering it explainable and predictable. The Four Quadrants risk classification concept of comes from the core concepts of the Black Swan, which links risk management to decision theory. *The classification system allows us to isolate situations in which forecasting needs to be suspended – or a revision of the decision or exposure may be necessary* [12], and to determine where it is safe to apply statistical risk models. The classification consists of two types of randomness and decisions [12,13]:

Mediocristan randomness is predictable; the Gaussian bell curve applies and applying statistical methods is safe. Examples of Mediocristan are human height, weight and age probability distributions, where no single outcome can dramatically change the mean. We can accurately predict events in Mediocristan with a little uncertainty, e.g. hardware lifetimes are from Mediocristan. Mediocristan randomness represents risks in Quadrants 1 and 3 in the classification.

In *Extremistan* randomness is Black Swan domain where small probabilities and rare extreme events rule. Since samples of events are so rare, the probability models will be sensitive to minor calculations changes and prone to error. In Extremistan, events scale and are subject to *fat-tails*[1], and can appear as power law or Pareto distributions. An example of such an event is the development of the amount of malware in the wild, with a growth trend that follows a Pareto distribution, where the theoretical malware amount is close to infinity. Extremistan randomness represents risks in Quadrants 2 and 4 of the classification.

The two types of payoffs from decision making are; (1) Simple Payoffs and (2) Complex Payoffs. In the former, decisions are binary form, e.g. either true or false, infected or not infected, which is where mainly probabilities play. Decisions are more complex for the latter, where the decision-maker must also consider the impact or a function of the impact, and weight benefits against disadvantages. Type 1 is thin-tailed and non-scalable while type 2 decisions can be fat-tailed.

This accumulates into Taleb's risk classification system of four quadrants; where risks in the First Quadrant has Mediocristan randomness and low exposure to extreme events. The payoffs are simple and statistical models works. Exposure to events in the Second Quadrant comes with Mediocristan randomness with complex payoffs, where it is generally safe to apply statistical models, factoring in awareness of possible incomplete models. Exposure to Third Quadrant risks comes with Extremistan randomness and low exposure to extreme events. The Fourth Quadrant is *"the area in which both the magnitude of forecast errors is large, and the sensitivity to those errors is consequential"*[12].

The Black Swan and Four Quadrants in ICT Risk For explicitly information security risk, the Black Swan concept has been treated by Hole and Netland[8], who treats the subject of risk assessing large-impact and rare events in ICT. Where the authors provide a basic discussion of what black and gray swans are in information systems and discuss events that may qualify as Swans. They define cascading risks and single points of failure as sources for swans, viruses, and other malware are sources for cascading risks. Additionally, Hole[7] addresses how to manage hidden risks, and how to recover quickly from Black Swan ICT incidents. Audestad (P.28-37)[2] discusses the limitations of statistics from an information security perspective. Audestad does not apply the term Black Swans, but he briefly discusses extreme events and limitations of statistics.

3 Methodology for statistical risk analysis and classification of events

The primary approach for the feasibility study in this paper is theoretical and statistical analysis of several types of information risks by considering a set of related cases that accompanied by historical data. The main classification scheme that we follow in the case study is the Four Quadrants as described by Taleb [12,13]. The work to classify risks within the Four Quadrants consisted

[1] In comparison to the Normal distribution a Fat-tailed distribution exhibits large skewness or kurtosis.

of gathering data and analyzing information security risks to determine their properties, and if statistical data is available if it would be appropriate to run calculations. The motivation is to use conventional statistical methods with a hope to extract particular characteristics that are suitable for quantitative risk analysis and further Threat Intelligence and Threat Forecasts. Additionally, we make a hypothesis about the applicability of a particular method. The information risks we have addressed where chosen from ISO/IEC 27005:2011, and we consider risks towards entities and not persons. This work focuses on risks from the compromise of information, technical failures, and unauthorized actions and does not address risks posed by natural events or similar. The calculations in this article are based on acquired data published by others. Furthermore, we perform specific statistical tests of whether such models are applicable for historical data or not, and extract corresponding quantitative measures. Our approach focuses on usefulness and limitations of statistical methods for information security risks analysis and predictability. In particular, we have analyzed risks to determine their properties with respect to the Four Quadrants (randomness and payoff). The following subsection describes the statistical methods and probabilistic models applied in this paper.

3.1 Supplementary statistical methods for historical data analytic

One makes a decision about information security risks mostly based on the previously collected data within the company or based on the publically available historical data about causes and results [10]. We introduce several community-accepted methods to deal with historical data and be able of making quantitative risk assessment possible since qualitative risk assessment has precision limitations when it is necessary to make predictions in numbers.

Probabilistic modeling. This type of analysis is applied when it is a need for probability estimation of a particular event x occurrence in a given historical dataset. Initially, the model $p(x)$ is built, and an estimation of the corresponding set of parameters from the data [6]. Then, this model can be used to estimate the probability of similar events in this very period or later on. We can state that there exist many obstacles related to the probabilistic modeling. First, very few data points from history may cause a wrong decision. Second, very rare events, like in the case of Fourth Quadrant, have negligibly small probabilities. However, this does not mean that this event are not going to happen.

Numerical analysis. Numerical analysis is a broad field of data modeling, in particular, time series. The function $f(x)$ is build using previous period of time $x_0, \cdots, x_t$. To construct a proper model, available historical data have to be decomposed into trends, seasonal components, and noise in order to build a precise prediction model. At this point, the recent data should possess the biggest degree of trust rather than data from a long time before [1]. For the defined earlier research questions that statistical models can be applied to support risk assessment within the four quadrants, yet under some limitations, we consider the following supplementary statistical approaches [1] from the previous Section:

1. **Logistics function** describes the process when the initial impact causes exponential increase until some moment of time. After this moment, the growth will be decreasing until it is saturated to some ceiling value [5].
2. **Conditional Probability** and **Bayes Theorem** are the probability methods used to calculate the likelihood of occurrence of some event when another dependent or independent event already happen.
3. **Gamma distribution** represents a family of continuous probability distributions that can describe data with quite various characteristics. The main parameters are shaped k and scale of the distribution θ.
4. **Exponential growth** characterize an event that does not have an upper boundary, and the observed outcome will grow more during the next period in comparison to previous.
5. **Log-normal probabilistic model** defines the distribution of some historical data under the condition that the logarithm of the data follows the Gaussian distribution.

So, these methods are the most promising from our point of view for estimation of possible event outcomes based on the previously analyzed information.

Statistical hypothesis testing. Further for each case study we will justify the usage of specific statistical methods and make a hypothesis about their applicability in that particular case. At this point, we need to use statistical tests to verify suggested hypothesis[2]. The two following approaches can be applied with probability distributions: QQ-PLOT, a Quantile-Quantile plot represents a probability plot by depicting expected theoretical quantiles E and observed practical quantiles O against each other and STATISTICAL TESTS that estimates the quantitative metrics of how well the data fit hypothesized distributions.

Confidence Intervals or CI relates to the probabilistic estimation of whether a particular data or data sample is being placed within a hypothesized distribution. It also means that the defined in CI % of data will be in the hypothesized distribution. To be precise, the tests evaluates the actual observed data O with the expected data E from the hypothesized distribution.

4 Case Studies

In this Section, we answer RQ 1 and show the application of models for ISRA with corresponding failures and Confidence Intervals (CI). This study is a comprehensive overview since a particular Case may require several methods to give a broader model. Our approach discusses specific types of risk for information security and where risks can be computed using statistical methods. We characterize information risks by the following predicate:

$$Malicious\ Intentions \xrightarrow{Action} \textit{Observable Outcomes} \tag{1}$$

Since the original $Malicious\ Intentions$ may not be known, the quantitative risk analysis relies on the historical data about *Observable Outcomes* that

[2] http://www.ats.ucla.edu/stat/stata/whatstat/whatstat.htm

can be either published by the information security labs or available within an organization. Each risk calculation in the following case studies are made for the purpose of illustrating and discussing the risks properties, and all risks are considered from the viewpoint of an organization. Based on the publicly available sources of information we made tentative calculations to give our answers on the research questions. Although not present in this paper, we have also explicitly treated risks of Insider attacks and phishing for the classification.

4.1 Advanced Persistent Threats (APT) and Cyber Industrial Espionage

APT are professional, resourceful and global actors often supported by Nation-States. These threats conduct targeted attacks over extended periods, aiming to compromise institutions for through cyber espionage and sabotage.

There are several problems when risk assessing APT attacks; tailored malware and techniques, making signature based scanners obsolete, and detection extremely resource intensive. APTs are generally very low probability (few incidents), although some companies daily deal with this threat. Modus operandi for APTs is stealth and extract data unnoticed, and even with a large ongoing compromise, the target's operations will be business as usual, making losses hard to visualize. Observing the severity of an APT breach is only possible after an extended period, which makes consequences both hard to predict and communicate. There are several different potential outcomes ranging from benign to malicious, all associated with a considerable amount of uncertainty. The discovery of an incident will have consequences, the "Initial Shock", where the harm comes from the loss of resources from general incident handling to before returning to normal. From there, the future of the incident has a large amount of variables affecting the outcome, all with their associated uncertainties. For example if the stolen data was production information, we must consider the probability of product replication, and what harm this would bring to the company in the future. Meaning that without extensive knowledge about the attacker and historical data, we cannot assign probabilities to these variables. Thus, there is a significant amount of uncertainty related to APT attacks.
We propose the following answer to the RQ1 for APTs:

- *Data source.* Targeted organizations generally do not reveal much information about APT. Therefore, the statistics for the particular events and actions are not shown to the public, and most data are available in vague numbers after the damage done. Therefore, the only data we can rely on to deduce the exact flow of the attack can be the analysis reports published by the security labs.
- *Discussion of statistical approach.* Since the exact data in most cases are unavailable or not computable, we can rely on the potential outcomes of the APT attacks. At this point as independent variable *Time* comes after the initial shock. The dependent variable, *Consequence*, therefore follow the numerical analysis model (1) Logistic function since at the beginning the range of probable outcomes growth exponentially until it reaches some point, where the attack

approaches maximum damage. Ideally, it will grow as an (2) Exponential function, yet in real life there are logical boundaries unless cascading happens. In Fig. 1 we have modeled an APT incident; after the initial shock, the system returns to normal, and the uncertainty of the damage is growing until the consequences become evident. Therefore, we conclude that the best way to describe this process is to use Logistic Function, where dependent on the type of business the harm (Y-axis) must reach a maximum amount after some time.

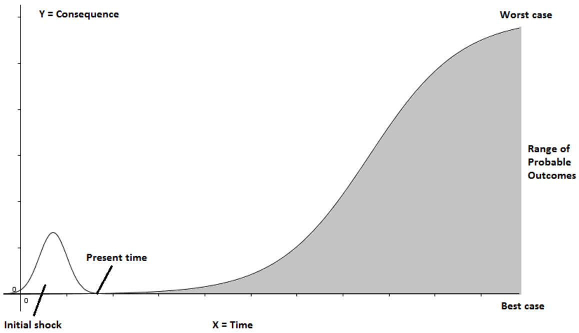


Figure 1: Example of potential outcomes from an APT/Espionage attack, Y=Consequence X=Time. The initial shock comes from detecting and responding to the breach. The long-term C is represented as a Logistic function, where P of all A are bound with a close to unsolvable U.

- *Results - Uncertainty/ Confidence intervals.* The second problem when estimating the risks of APT is the Confidence Interval (CI) estimation of the risk management decision. The uncertainty of the attacks against organization increases after the evidence of the initial attack, which makes the confidence interval of the predicted risk value too low to rely on it:

$$R|_{CI} \approx \frac{1}{uncertainty} \tag{2}$$

  Bigger uncertainty causes less confidence in the predicted outcomes of the damage done. The larger range, the harder to estimate final risk and make an appropriate risk management decisions.
- *Results - Applicability of statistical methods and possible failures for each risk.* Since no data available, it is hard to derive any meaningful decision from the unreliable model that follows Exponential Function. At this point, we do not have any other sources to rely on, so this model helps to understand the way of damage developing. Also, we may derive the qualitative prediction using monotonicity of the process development. This model can be used (1) to show the importance of finding the attack evidences and cause in the initial phase, and (2) impossibility to say the exact cause in the final stage until it is obvious.
- *Classification of Risk* - Without knowledge about attacker intentions and capabilities, a victim of an APT attack, particularly industrial espionage, can only make risk predictions based on knowledge about internal processes and the value

of the stolen information. Even if the Logistic function corresponds to the nature of the APT harm, it is still rather a random prediction than reliable results for risk analysis. No outcomes of an APT attack will be identical, and outcomes are complex in nature, prone to cumulative effects. There is also a lack of both data and knowledge about attacks with corresponding consequences, which makes it a *Fourth Quadrant* risk.

4.2 Malware and Botnet distributions

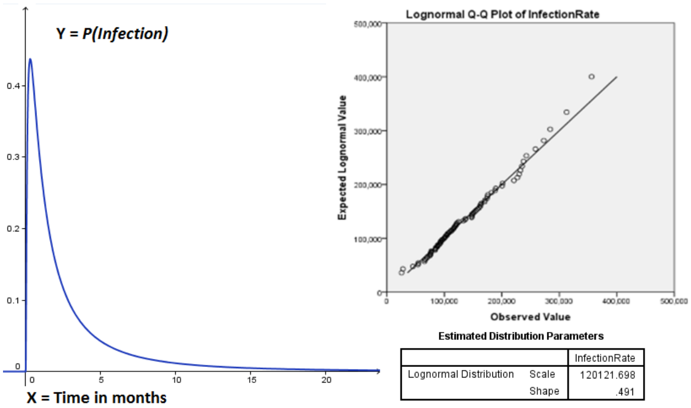
Successful malware distributions such as different versions of botnets, e.g. Zeus, Conficker[3] and others, have shown considerable resilience towards eradication. Epidemic models have proven useful for estimating propagation rates [15,2], however, historical data is more useful for obtaining probability distributions. We propose the following answer to the RQ1 for Malware and Botnet distributions:

- *Data source.* For our calculations, we obtained data from the Shadowserver Foundation [4], which has monitored the infection rates of the Gameover Zeus botnet and Conficker with respect to time. Gameover Zeus is a Peer 2 Peer botnet built by cyber criminals by sending emails with embedded malicious links or attachments, or enticing the victim to visit an infected website where a Trojan infected the victim. In comparison to the APT statistics, the information about botnet distribution relatively easy to gather from publicly available sources like Shadowserver, cause the anti-virus companies construct corresponding signatures shortly after the first discovery of botnet and starts logging occurrences.
- *Discussion of statistical approach.* Based on the available statistics collected over the months by Shadowserver, we ran a fitting test as described in Section 3. The results concluded that the most promising hypothesis about the probabilistic model is that data follow the (1) LogNormal distribution. Therefore, it can be possible to predict the exact percentage of probability of the distribution of the botnet in some period in the future. From the other side, numerical methods for time series analysis can estimate the number of malware species in the wild after a defined period. The value of the last two methods is that the trends of the malware distributions can be predicted with better accuracy that just random guessing, cause human expert may fail to do it accurately.
- *Results - Applicability of statistical methods and possible failures for each risk.* We can state that (1) the available data follows LogNormal distribution, so we can use these methods to say about future conditions. (2) That is not possible to fully rely on these methods since the uncertainty in the predictions is quite significant due to versatility in the data and tail sensitivity in the graph. However, the derived information can be used in qualitative ISRM since it is rather a set of fuzzy metrics.

  We ran the data points for Gameover Zeus in *QQ* plot and got the best fit with a Log-Normal curve with a tendency towards a thick tail, Fig. 2. Our

[3] Conficker was initially a computer worm, but when the payload was uploaded post-infection, it turned out as a Botnet

[4] Gameover Zeus`https://goz.shadowserver.org/stats/`



Estimated Distribution Parameters

		InfectionRate
Lognormal Distribution	Scale	120121.698
	Shape	.491

Figure 2: Gameover Zeus infection probability distribution and timeline. Right shows results of Q-Q plot of LogNormal distribution. Data source: The Shadowserver Foundation.

results show that the Gameover Zeus botnet distribution is left-skewed (positive). The initial propagation speed is high (see Fig.4(b)), until saturation or patch released slows down the propagation, from which point the existing population deteriorates. In addition to adhering to epidemic propagation theory, there are several aspects that will influence the thickness of the tail. For example new versions of the malware being released, either exploiting a new vulnerability for increased propagation or changing behavior/coding to avoid scanners. In addition, we know that Conficker followed similar propagation and deterioration patterns, although Conficker[5] was self-replicating [15]. According to our model: if the entity is vulnerable, the general probability of infection is 30% from the initial dissemination until the first month has passed. With a Mean population = 134,527, Standard Deviation = 64,797, and $\delta = 0.491$. The graph is sensitive to changes in the tails; this is also visible in the Q-Q plot results. The right tail of the graph in Fig. 2 would likely have been thicker if the data came from Conficker A+B, which remains active and deteriorating after six years.

- *Classification of Risk* - Single non-zeroday malware infections are generally detected and removed by antivirus software, and generally pose very little risk. However, dependent on the target infected and type of malware, the payoff can be complex. Self-propagating malware is usually more severe as they pose a threat to larger parts of the infected system. With some computer worms, the payoff can be considered simple, as the computer is infected (meaning non-operational) or not infected. Effectively having only two states of being. It is partially possible to predict exposure from such generic attacks, e.g. amount of vulnerable systems, but there is exposure to multi-vectored and other random effects which puts this risk in the *Third Quadrant*.

[5] See also `http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker`

4.3 Distributed Denial of Service (DDoS) attacks

One of the most feared information attacks is the DDoS attacks, as they have the potential to break servers and deny access to a service to customers over an extended period causing massive revenue losses. By monitoring activity, we can obtain reliable numbers on how large the average DDoS attack is, and generate distributions of attack magnitudes. The answer to the RQ1 for DDoS:

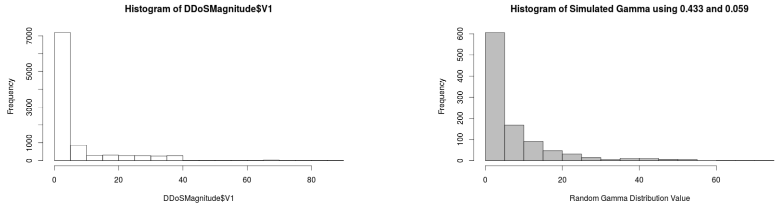
- *Data source.* There is available open access statistics on DDOS attacks. So, we can use available statistics, yet it can not be fully relied on due to misleading detections or hardware malfunctions. Using numbers gathered from open access, we generated an example of possible distribution of DDOS occurrences for different bandwidth, shown in the Figure 3. Available threat intelligence indicated that the commonly observed DDoS magnitude at the time was between 0-90 Gbps, with distributions as seen in Table 1. Our test dataset corresponded to the numbers provided open access sources, having an arithmetic mean = 7.31, and Std. Dev = 13.55. The so-far largest reported DDoS attack was 500 Gbps, we can guesstimate that the generic probability of such an attack occurring annually is large; while the probability of such a large-scale directed attack at a single organization is negligible. There was no observed attack magnitudes over 90 Gbps in the surveys. However, we add such scenario A5 in Table 1.

Table 1: Example of DDoS attack magnitude distributions and probabilities, with conditional probabilities of semi-annual occurrence.

Scenario	Gbps	% of attacks	P(A|B)
A1	<1	55.00 %	27.50%
A2	1-5	15.00 %	7.50%
A3	5-10	10.00 %	5.00%
A4	10-90	20.00 %	10.00%
A5	90+	Not observed (0.1%)	0.05%

- *Discussion of statistical approach.* There are several possible ways of approaching the statistical analysis of DDOS attacks. At first the probability of the DDOS attack can be calculated as simple (1) CONDITIONAL PROBABILITY, which gives an exact risk of being targeted for a DDOS attack out of possible attacks. Table 1 shows the results of calculations made for an organization that expects P(B)=50% annual chance of DDoS attack. At second, we can say something about the number of attacks and maximal used bandwidth by considering the historical information. However, the number of maximum reported DDOS attacks follow the (2) EXPONENTIAL FUNCTION and can not be predicted for the next years: $N = N_0 \cdot e^{t'}$ since some covert parameters are not taken into consideration like breakthrough network controller speed. At third, the particular scenario can be considered when discretion intervals of DDOS bandwidth are considered like $P(DDOS > 90Gbps) = P(DDOS) \cdot P(> 90Gbps|DDOS)$. Also the (3) γ-DISTR. is the most applicable way of modeling such variety in scenarios.
- *Results - Uncertainty/ Confidence intervals.* The data and estimated parameters are valid only for some period until new attack methods emerge. However, it is still possible to form a corresponding γ-distribution to characterize the bandwidth for DDOS as it is depicted in the Figure 3, (a). So, corresponding CI can

be extracted based on the parameters of the distribution to estimate the DDOS [4]. The Lower boundary can be neglected, however, exceeding the upper boundary may indicate that the parameters need to be re-evaluated for quantitative ISRM.



(a) Histogram of DDOS magnitude up to 90GBps

(b) Simulated γ-distribution of DDOS from collected data

Figure 3: Comparison of the original DDOS data and modeled distribution

Though the data distribution can vary and, therefore, change the form depending on newly emerged technologies in network adapters industry, we can still use CI to estimate the boundary of the desired mitigation frame. It can be stated that the company wants to eliminate some % of the DDOS attacks and estimates the threshold of the attacks based on the previously collected information. The Table 2 presents an exact range of the bandwidth at which a particular % of the attacks can be mitigated. Our particular interest is the upper boundary of the CI since the lower boundary can be ignored at this point. For example, to withstand 95% of the DDOS attacks according to modeled γ-DIST. in the Fig. 3, (b) a company has to place a DDOS protection not lower than 62.82 Gpbs.

Table 2: Confidence Intervals for defined % of the DDOS attacks to be eliminated

To eliminate	50%	90%	95%	99%
Limit_lower, Gbps	0.531143	0.012634	0.002547	0.000061
Limit_upper, Gbps	9.411601	29.566104	39.241385	62.822911

– *Results - Applicability of statistical methods and possible failures for each risk.* We can estimate and put a threshold for an intrusion detection system to be capable of handling such attacks. Since it might be significant when guesstimating the risk that the organization takes when ignoring a particularly intensive attacks. For example, the network adapters increase capacity from 100Mbps up to 1Gbps over previous years. Therefore, the statistical models can be used for (1) DDOS bandwidth, and probability prediction and estimation, though constant failures of these models may indicate a need for re-evaluation of the maximal DDOS bandwidth. Furthermore, using the estimated probability, we can built also a qualitative risk estimators as more general linguistic characterization of the risk.

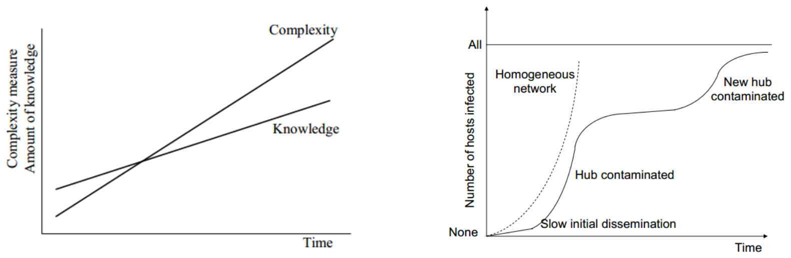
– *Classification of Risk* - As we have shown, it is possible to obtain distributions of DDoS attack magnitudes with associated probabilities. However, our observations can be offset by a single massive attack, such as Russia's DDoS attack on Estonia in 2007. This area is also subject to Moore's law, which means that historical observations of attack magnitudes will quickly become obsolete. We consider the payoff from DDoS attacks as simple; it either succeeds in denying service, or it does not while the duration of the attack determines the consequence. Our analysis, therefore, places risks of DDoS attacks in the *Third Quadrant.*

5 Discussion

Before presenting the Four Quadrant classification, we discuss issues that make information risks less predictable, which we have factored into our classification.

5.1 Factors leading into the Fourth Quadrant

- *The Complexity-Knowledge Gap* - Knowledge about system security quickly diminishes through the increase of *complexity* and *interconnectivity*, and the larger the system, the more uncertainty. Research on complex networks has demonstrated that the number of hosts on a network follows the power law [15], and our knowledge of risks in such systems and environments diminishes quickly. Audestad [2] calls this development the Complexity-Knowledge gap Fig. 4 (a).



(a) The Complexity-Knowledge gap

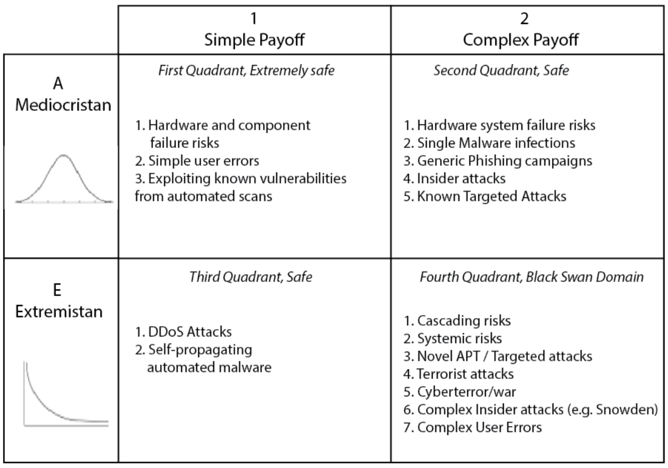
(b) Dissemination of malware, showing Pareto curve distribution in homogenous network towards saturation.

Figure 4: Factors leading into the Fourth Quadrant. *Pictures reprinted with permission, from Audestad, 2009 [2]*

- *Interconnection and Single Points of Failure (SPOF)* – While there is extensive knowledge of SPOF problems in the ICT domain, the risk posed by interconnectivity are easily overlooked and underestimated. For example in a Banking incident from 2001 reported in [8], a human error triggered a SPOF at an operations company delivering ICT services to banks. This mistake caused a DoS for 114 banks and roughly one-fourth of the Norwegian population at the time. Such consequences would not have been possible without a large interconnected operations company representing a SPOF for much of the transactions in Norway. A centralization of operations and processes, which allows for the creation of one large strongly interconnected hub, in which the consequences of failure can become catastrophic for the system as a whole. The society and ICT have never been as interconnected at any period in the past, which quickly outdates most risk predictions based on historical data, as systems will find new ways to fail. The Complexity-Knowledge gap will also come into play, and we are likely to miss or overlook severe risks and potential consequences.

- *The Unpredictable Active Adversary* - In most cases, the activities that lead to a targeted attack are not visible, or they are negligible. The complexity of the extreme events such as cyberwarfare or cyberterrorism in the information security domain is so high that we can hardly notice it unless the damage is done, and the outcomes are obvious [11]. Since these activities are well-planned and rather exceptional cases, there is a need for enormous data analytic and reconsideration of the Internet Crime like in the case with Stuxnet. For rare events, sophisticated classification/regression models have to be applied to conventional statistical methods to understand the nature of the event. It is sometimes necessary to get expert knowledge on the underlying adversary process rather than just rely on numbers for risk analysis. There is also the problem that the past will not reflect the future when it comes to resourceful and adaptable attackers. Advanced attackers will seek novel ways of achieving their objectives, which makes over-reliance on historical data dangerous.
- *Vulnerabilities to Cascading and Systemic risk in ICT* - Cascading and systemic risks are two types of high-level risks that are known to be large impact and low probability events. A cascading risk is when several components of a network fail in a cascade due to a crucial node going down, which subsequently causes an overload on the remaining nodes. Or when one component causes failure in interconnected components [8]. Whereas a systemic risk affects the global system and not just a particular entity. We define cascading risks as having the ability to cause localized harm, and systemic risks as having the capacity to cause global harm to a system. Of the latter, the Morris worm is probably the only known instance to have posed a systemic risk to all systems connected to the internet. The malware forced a segregation of the internet regions to prevent contamination and recontamination.
  The consequences of a cascade can be devastating: In 2009, a Conficker infection within the Norwegian Police ICT systems reportedly caused damage ranging 30-50 million NOK and a downtime of 10 days. The Police computer system was largely homogenous, running older and vulnerable versions of Microsoft Windows, and Conficker was reported to have saturated at about 16 000 infections. Fig. 4 (b) shows general dissemination patterns of self-propagating malware; the stapled line indicates propagation in homogeneous networks. The distribution in the homogenous network follows exponential growth while the propagation in heterogeneous networks produces a model rather close to joint logistic function. Consequences from self-replicating malware and cascading risks are subject to fat tails, which requires caution when dealing with such phenomena.

The Four Quadrants Classification of Information Security Risk Based on the case studies and the factors provided in the previous section, the nonexhaustive classification of information risks is presented in Fig. 5. This classification can help risk analyst in deciding whether to apply quantitative or qualitative risk analysis methods based on risk properties and where he can safely rely on statistical methods. The classification should not be used as an argument to not do risk assessments of Fourth Quadrant risks. However, we recommend avoiding long-term quantitative predictions with these risks due to their uncertain properties caused by a considerable complexity-knowledge gap. It is also possible that with more information and understanding, statistical risk analysis can move several of these risks out of the Fourth Quadrant.



	1 Simple Payoff	2 Complex Payoff
A Mediocristan	*First Quadrant, Extremely safe* 1. Hardware and component failure risks 2. Simple user errors 3. Exploiting known vulnerabilities from automated scans	*Second Quadrant, Safe* 1. Hardware system failure risks 2. Single Malware infections 3. Generic Phishing campaigns 4. Insider attacks 5. Known Targeted Attacks
E Extremistan	*Third Quadrant, Safe* 1. DDoS Attacks 2. Self-propagating automated malware	*Fourth Quadrant, Black Swan Domain* 1. Cascading risks 2. Systemic risks 3. Novel APT / Targeted attacks 4. Terrorist attacks 5. Cyberterror/war 6. Complex Insider attacks (e.g. Snowden) 7. Complex User Errors

Figure 5: The Four Quadrants with Risk Classifications. *Based on Taleb[12]*

6 Conclusion & Future work

In this paper we investigated quantitative risk calculations based on the available data. We provided a classification of where it is safe to apply statistical methods and where to expect a reasonable return on investment in improved decision making within the Four Quadrants. This work studied whether the statistical approaches are feasible to deal with Information Security Risks at all and what are the advantages of using such methods considering fact that they are purely reliable for the prediction. One can state that conventional statistical methods provides reliable accuracy only in case of significant amount of historical data and when the event in question is located within the tolerance interval from the past data. This article has presented several major cases within the Information Security area, with a corresponding applicability study of statistical methods. We can conclude that there is a trade-off between the complexity of supplementary analytic and the risk's harm. It implies that trivial statistical methods are not suitable to deal with threat Intelligence in dangerous risks, yet general knowledge derived from such methods are reliable to make predictions better than random. Moreover, the statistical methods can not only be useful in quantitative analysis, yet also give a basis for qualitative measures. The observable outcomes may not always find a justification from the history since it might be some coincidence of logical triggers and human errors. Also, the implications of the study have discovered severe limitations of quantitative forecasts when it comes to targeted attacks, namely malicious individuals, and sophisticated threat agents. The increase in both complexity and interconnectivity limits our ability to forecast. It means that future advanced models such as Soft Computing should be considered to be able to expand the understanding of the covert malicious actions and make a better quantitative risk assessment.

Acknowledgments The authors acknowledge Professors Jan Arild Audestad, Einar Snekkenes and Katrin Franke, and the data contributions made by the Shadowserver Foundation. The authors also recognize the sponsorship from COINS Research School for information security.

References

1. J.S. Armstrong. *Long-range Forecasting: From Crystal Ball to Computer*. A Wiley interscience publication. John Wiley & Sons Canada, Limited, 1978. 5
2. Jan Audestad. *E-Bombs and E-Grenades: The Vulnerability of the Computerized Society*. Gjovik University College, 2009. 1, 4, 9, 13
3. Terje Aven. *Misconceptions of risk*. John Wiley & Sons, 2011. 3
4. CharlesJ.Geyer. Stat 5102 notes: More on confidence intervals. `http://www.stat.umn.edu/geyer/old03/5102/notes/ci.pdf`, February 2003. accessed: 07.04.2015. 12
5. Arabin Kumar Dey and Debasis Kundu. Discriminating between the log-normal and log-logistic distributions. *Communications in Statistics-Theory and Methods*, 39(2):280–292, 2009. 6
6. Zoubin Ghahramani. Probabilistic modelling, machine learning, and the information revolution. In *presentation at MIT CSAIL*, 2012. 5
7. Kjell J Hole. Management of hidden risks. *Computer*, 46(1):65–70, 2013. 4
8. Kjell J Hole and L-H Netland. Toward risk assessment of large-impact and rare events. *Security & Privacy, IEEE*, 8(3):21–27, 2010. 4, 13, 14
9. Daniel Kahneman. *Thinking, fast and slow*. Macmillan, 2011. 2
10. Max H Bazerman Katherine L Milkman, Dolly Chugh. How can decision making be improved? *Perspectives on Psychological Science*, 4(4):379–383, July 2009. 5
11. James Andrew Lewis. Assessing the risks of cyber terrorism, cyber war and other cyber threats. Technical report, Center for strategic & internation studies, 2002. 14
12. Nassim Nicholas Taleb. Errors, robustness, and the fourth quadrant. *International Journal of Forecasting*, 25(4):744–759, 2009. 2, 3, 4, 15
13. Nassim Nicholas Taleb. *The Black Swan: The Impact of the Highly Improbable*. Random House LLC, 2nd ed. edition, 2010. 2, 3, 4
14. Gaute Wangen and Einar Snekkenes. A taxonomy of challenges in information security risk management. In *Proceeding of Norwegian Information Security Conference / Norsk informasjonssikkerhetskonferanse - NISK 2013 - Stavanger*, volume 2013. Akademika forlag, 2013. 1, 2
15. Shui Yu, Guofei Gu, Ahmed Barnawi, Song Guo, and Ivan Stojmenovic. Malware propagation in large-scale networks. *IEEE Transactions on Knowledge & Data Engineering*, (1):170–179, 2015. 9, 10, 13