A financial evaluation of DDOS defences dynamics from an organisational perspective: how long will these defences hold?

Summary / abstract

This paper reports on the financial evaluation of DDOS reference architecture and associated policies settings using system dynamics. DDOS peak attack capacity and cyber security costs have been growing exponentially over time. This raises the question which structure explains investment behaviour in this area. We believe system dynamics modelling is appropriate due to cyber security due to its dynamic complexity in this field. This complexity follows from attacker-defender interaction and the response of the resilient organisation.

We identified relevant security metrics, their (delayed) interrelations and resulting feedback loops. By capturing this structure in an investment model we were able to cope with the often observed difficulty in the field of cyber security of estimating financial impact of policy settings. We were able to align DDOS defence measures effectiveness with vulnerabilities and (potential) impacts of DDOS attacks in the model. Our model reveals tipping points in long term financial performance which indicate important changes in policy effectiveness. We believe a rat race between attacker and defender by increasing defence capacity over time is not sustainable. Based on our initial model simulation we analyse six alternative solutions.

DDos, Attacker – Defender Dynamics, Security Economics

Introduction and reference mode

A Denial of Service (DOS) attack has the purpose of preventing legitimate users from using a specific network resource. A Distributed Denial of Service (DDOS) attack is a coordinated attack on the availability of services of a given target system or network that has been launched indirectly through compromised computer systems (Specht and Lee 2004). In 2016 a massive DDOS attack of 600 Gbps (Gigabit per second. GBPS is a metrics for measuring the size of a DDOS attack) has been claimed (Khandelwal 2016). However, most attacks involve less bandwidth. Ungureanu (2016) indicated that 50% of all attacks are topped at 50 Gbps and some at 100 Gbps. In the scientific literature no papers are been found on DDOS attack behaviour. Most scientific literature on DDOS covers areas such as taxonomy of attackers, taxonomy of defences, technicalities, specific counter measures. Nonetheless, commercial reports, like Imperva Incapsula (2016), showed similar behaviour as identified by Edwards et al. (2016) in the area of data breaches: a heavy-tailed distribution. In the case of DDOS this distribution applies to both magnitude and duration. Depending on the magnitude and duration of the DDOS attack, economic consequences can be huge to organizations. These economic consequences are caused by unavailability of services resulting from a successful DDOS attack. Unavailable services evoke a delay of revenue generation or even a revenue loss. In addition customers might contact these targeted organisations with questions about service performance and availability. Addressing this questions will take additional effort and evoke additional costs for customer service and communication departments. Furthermore alternative service delivery to these customers requires additional resourcing. If large (business) customers are involved organisations might even face legal claims for not delivering services as stated in underlying agreements.

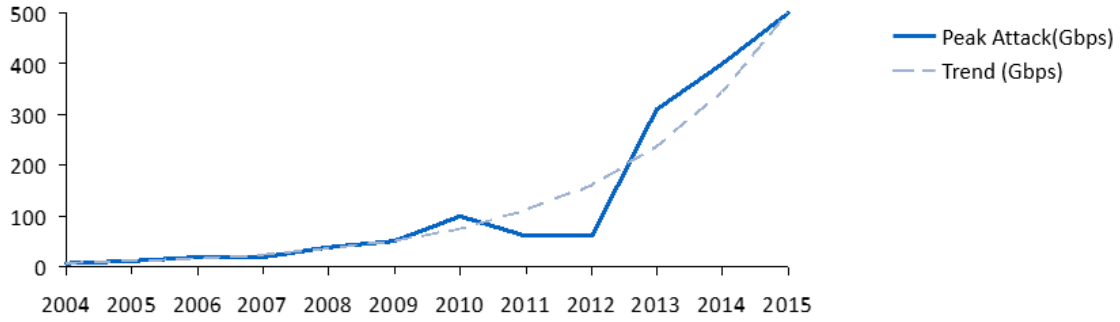

Fig 1. DDOS Survey peak attack size year over year (derived from Arbor Networks 2016) enhanced by non-linear increase

During the last decade we observed a non-linear increase in the DDOS peak attack size. Figure 1 (Arbor Networks 2016) indicates a three percent month on month increase of attack size. In more or less the same time period we also see a similar increase in the cyber security spending. Although Figure 2 (Atlantic Council 2015) is related to spending in the US it might considered an industry wide trend. This figure also demonstrates a non-linear increase of approximately nine percent year on year. This trend is mainly explained by the impact of cyber security incidents (Atlantic Council 2015).

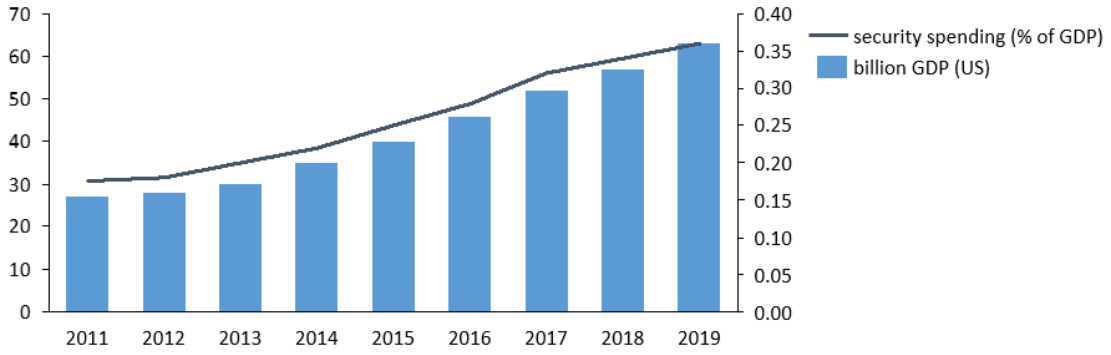

Fig 2. Cybersecurity spending in US in relation to GDP . (derived from Atlantic Council 2015)

These trends might seem logical since they point to an increase on both the attacker and the defender side. Yet, Martinez-Moyano et al. (2011) indicated that defenders are subject to the detection trap. This means defenders are only inclined to invest in security if the attack is detected / visible. As a consequence security investments will be made directly after a successful attack. In those situations it is likely that suppliers are in a much stronger position to increase their prices. Hence, the increased spending in cyber security can be explained by both attack behaviour and decision making behaviour of parties involved.

In business sectors with declining margins a structural increase of cyber security cost will present a challenge in the long run. For instance, the financial sector has to cope with declining margins. Figure 3 (statistica 2016) indicate that US financial institutions have a four percent year on year declining interest margin.

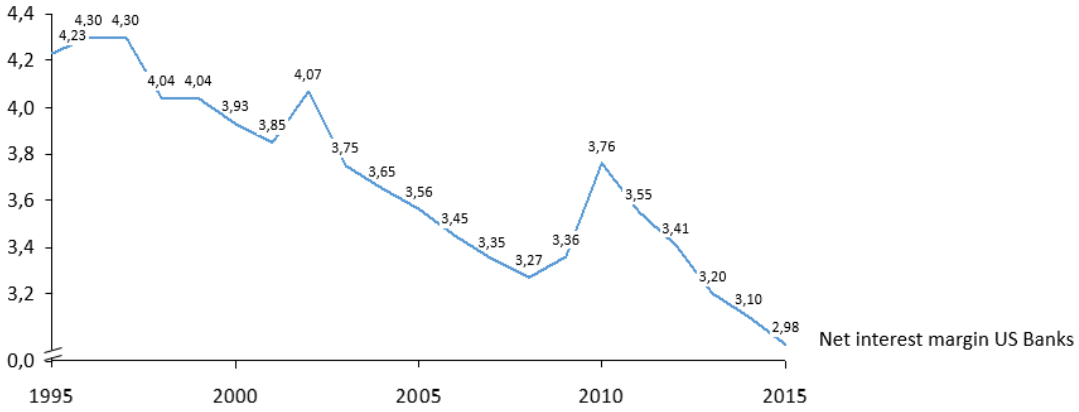

Fig 3. Average interest margins banks US 1995 – 2015 (derived from statista.com 2016)

In conclusion, an increasing DDOS attack peak requires investments in higher DDOS protection, while decreasing margins yield less available investment budget. In such a situation it is difficult to keep an investments in line with observed attack behaviour. However, if a part of this increasing security cost trend can be explained by decision making behaviour, how can this trend be influenced by the DDOS defence policy setting?

According to Warren (2016a) system dynamics modelling is complementary to enterprise architecture and can be used for business case design for financial decision making (Warren's 2016b). This research in the field of DDOS defences in a financial organisation is an example of the operationalization of his thoughts. This paper is about evaluating DDOS policy settings by testing these in a system dynamics model. This paper explains why system dynamics model building is appropriate, addresses basic literature on DDOS attack and defences, explains the different components of the system dynamics model on DDOS and provides insights into policy evaluation.

Why system dynamic modelling?

The heavy-tailed distribution of DDOS attack behaviour might raise uncertainty about the probability of being attacked, the duration and the impact of the attack. As a consequence making investment decisions regarding DDOS policy becomes a difficult process, because potential benefits are related to the prevention of these attacks. Difficult elements to estimate have been, among others, damage, benefits and value (Rue et al 2007, Su 2006) which can significantly impact security decision making (Graves et al 2016). Tversky and Kahneman (1973)) showed that decision makers employ simple mental processes or heuristics in case of such uncertainty. So, in the absence of clear indicators on which to base decisions, other means for investment evaluation will be used, like Fear, Uncertainty and Doubt (FUD) (Tongia and Kanika 2003) or willingness to pay (Anderson 2013), or delayed decision making may occur (Böhme and Moore 2016).

When defenders' perceived uncertainty about implementing the right counter measures is too high, the defender will use reactive security management (Böhme and Moore 2016) and therefore might be susceptible to the detection trap. Falling for the detection trap can be seen as counterintuitive behaviour of a complex system that arises from the interactions of the system's agents over time. Sterman (2006) and Forrester (1971) call this dynamic complexity. A complex system, like DDOS defences, has the following characteristics: constantly changing, tightly coupled, governed by feedback, non-linear, history dependent, self-organizing, characterized by trade-offs, counterintuitive and policy resistant (Sterman 2006, 2000). Zeijlemaker (2016a, 2016b) argues that these characteristics can be found in the attacker – defender interactions and response of the organisation. The attacker – defender interaction is an ongoing dynamic between attacker and defender both searching for the weakest link. This link will be used for attacking and defending respectively and both agents will anticipate and learn from each other's actions (Clayton et al 2015, Libicki et al 2015, Su 2006, Böhme and Moore 2016, Barth et al 2012, Martinez-Moyano et al 2015). A successful attack will result into a defender to mitigate the associated impact. A resilient organization will maintain positive adjustment under challenging conditions and emerges under these conditions more powerful through a sophisticated band of learning (Vogus and Sutcliffe 2007, Reinmoeller and Baardwijk 2005, Martinez-Moyano et al. 2015). The resilient organization might be negatively affected by efficiency improvements through the capability trap (Repenning and Sterman 2002) and adaptability trap (Rahmandad and Repenning 2015). Zeijlemaker (2016a, 2016b) also argues that system dynamic modelling helps to understand this complex system, address the dynamic complexity and therefore provide a deeper insight in financial consequences of DDOS policy setting. System dynamics provide insights in feedback loops and time delays (Sterman 2006)

The DDOS model structure

Two main forms of DDOS attacks can be recognized: bandwidth depletion attacks and resource depletion attacks (Naykude et al 2015, Maheshwari and Krishna 2013, Mittal et al 2011, Zhang and Parashar 2006, Specht and Lee 2004). In a bandwidth depletion attack large volumes of IP traffic are sent to a target's network to congest it. This network experience packet loss and slows down, crashes or suffers from network bandwidth saturation preventing access by legitimate users (Specht and Lee 2004). In a resource depletion attack the attacker sends malformed packets that tie up system resources so that none are left for legitimate users (Maheshwari and Krishna, 2013). Examples of these resources are sockets, CPU, memory, disk/database bandwidth and I/O bandwidth (Zargar 2013). Compared to bandwidth depletion attacks less volume is needed for these resource depletion attacks.

Moreover Zargar (2013) also recognized that DDOS attacks exploit vulnerabilities and implementation bugs in the software implementation of services. According to Maheshwari and Krishna (2013) DDOS attacks can be performed at three levels: the network level, the operating system level and the application level. For this paper we distinguish bandwidth depletion attacks and targeted resource attacks. As a consequence in this paper targeted resource attacks include resource depletion attacks and DDOS attacks exploiting vulnerabilities in implementation bugs. The paper does not distinguish different layers like network, operating system and application level.

All of these DDOS attacks have the following three characteristics;

- Especially DDOS bandwidth attacks generate large volume flow that overwhelms a target. In order to make the response and detect time as low as possible detection and defence of DDOS should be as close to the attacker as possible (Zhang and Parashar 2006, Khajuria and Srivastava 2013). Therefore a DDOS defence policy may include the internet service provider (ISP) and defence capabilities that are able to handle large volumes like a cloud solution or a content delivery network.
- The need for volume and no content provides the attacker the means to make packets identical to legitimate traffic (Zhang and Parashar 2006, Khajuria and Srivastava 2013). This makes low volume DDOS attacks harder to detect. Especially the targeted resources attack can be made by closely mimicking normal traffic.
- Given the bursty nature of internet traffic DDOS detection is difficult (Zhang and Parashar 2006).

These DDOS characteristics give rise to the following. There is a need to have insights in how to defend against these attacks. The literature on DDOS attack and DDOS defence taxonomies provides a deeper understanding on the challenges of the denial of service field (Douligeris and Mitrokotsa 2004, Mirkovic et al 2004, Specht and Lee 2004). These studies have recognized some preventive, detective and responsive mechanisms. Apart from these Douligeris and Mitrokotsa (2004) emphasized 'intrusion tolerance and mitigation' while Specht and Lee (2004) recognized post attacks forensics. This model has been built based on various subject matter expert (SME) interviews, DDOS reference architecture and policies in line with the process described by Sterman

(2000) and Pruyt (2013). In the following the appropriate data to this system has been included. During construction of the system dynamics model it became clear that DDOS defence policies include a mixture of the above mentioned mechanisms. It also became evident that the system dynamic model goes beyond the scope of processes, technology and also include the behaviour of different agents like, government, law enforcement, attacker, internet service provider, cloud provider. These agents have a role in this complex system. Consequently, the DDOS model contains the following sub-models (for a detailed explanation of sub models see Appendix 1 of the supportive material) as shown in Figure 4:

- Sub model 1: attackers perspective: DDOS attack.
- Sub model 2: defenders perspective: Bandwidth attack.
- Sub model 3: defenders perspective: targeted resource attack.
- Sub model 4: the resilient organisation: threat intelligence.
- Sub model 5: the resilient organisation: major incident response.
- Output model 6: customer impact.
- Output model 7: financial impact.
- Output model 8: financial evaluation.

Sub model 1 on attackers behaviour is about the probability that an attacker will attack and the type of attack the attacker will use. In this paper the word hacker has been used, however it should be noted that a hacker is a skilled person in the field of cyber security that may use his skill for the purpose of good (white hat) or bad (black hat) oboth (grey hat). In this paper we focus on black hat hacking . In our model the attacker can use a bandwidth attack or targeted resource attack. The probability of being attacked depends on the successfulness of an attack. In this paper a successful DDOS attack is defined as an DDOS attack that results in a negative customer service impact. *A successful attack will increase the probability of further attacks due to word-of-mouth effect that alerts other hackers to a perceived vulnerable organisation*[1]. On the other hand, the probability of being attacked will decline if national governments intervene by arresting the hacker and/ or destroying the botnet used for DDOS attacks. *An unsuccessful attack might result in a second stronger attempt. Hereafter the probability of attacks will decrease because hackers are going to look for another target*. Attacker innovation is also triggered by unsuccessful attacks, because the attackers are going to search for new ways of attacking. Thus the future probability of an attack might increase due to an unsuccessful DDOS attack.

[1] These are various dominant loop in the model (word-of-mouth effect jacker, perceived vulnerable organization, hacker works harder and hacker looks for other target.

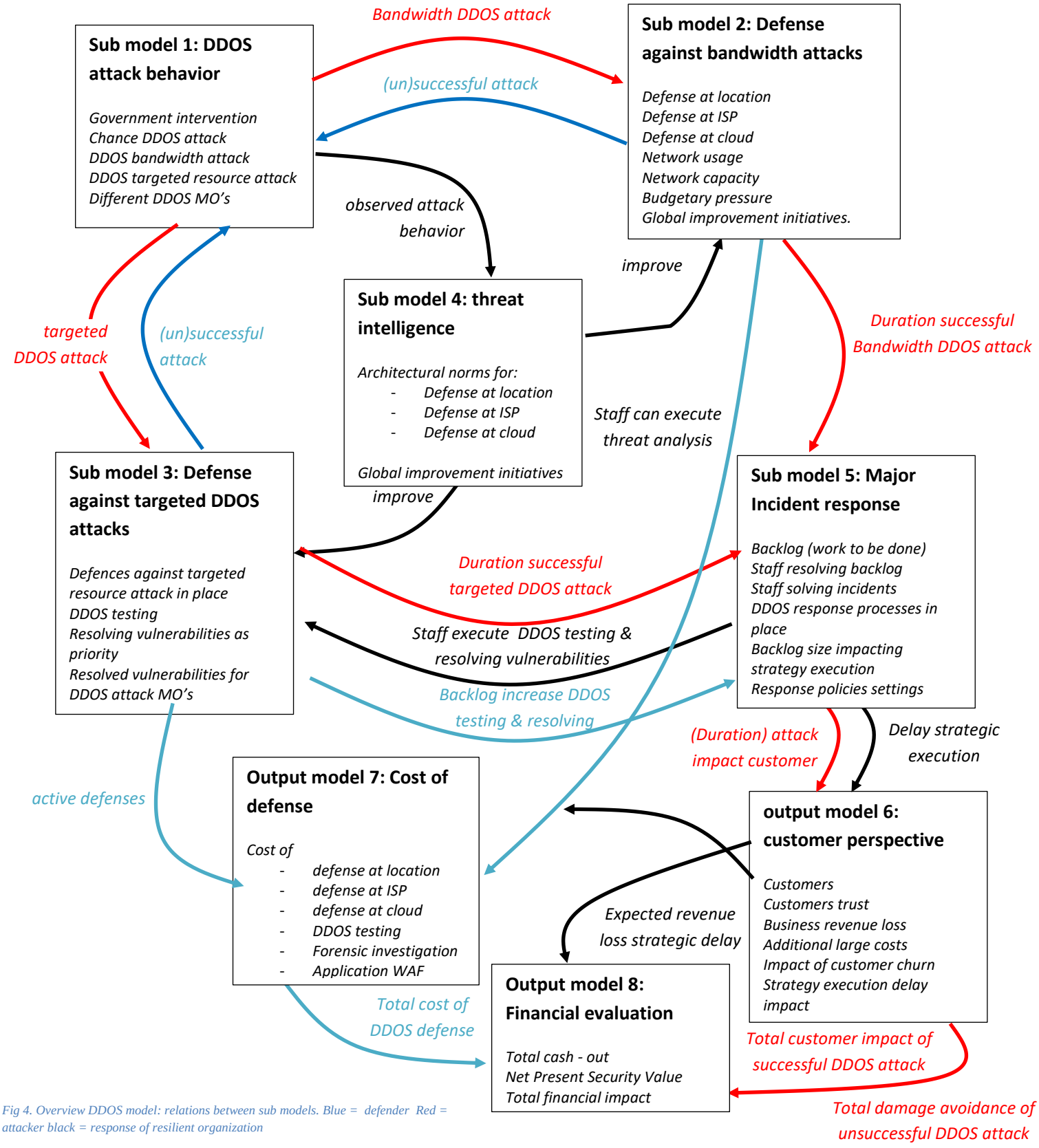

Fig 4. Overview DDOS model: relations between sub models. Blue = defender Red = attacker black = response of resilient organization

The defender will receive information about hackers' behaviour through other organisations and their own organisation. This is called threat intelligence. *Based on the analysis of this information the defender can decide to upgrade the defences (sub model 4 threat intelligence) during regular life cycle management*[2]. Threat intelligence can only be used if sufficient staff is available to analyse this information and this staff is not occupied with other activities. The defender has defences in place for bandwidth attacks (sub model 2 defence against bandwidth attacks) and targeted DDOS attacks (sub model 3 defence against targeted DDOS attacks). For bandwidth attacks these defences can be at the location of the defender, at the internet service provider(s) or in the cloud (the cloud can be seen as a shared defence capability that can absorb a very large amount of an DDOS attack with a large magnitude). *Depending on the successfulness of the hacker's actions the defender might decide to directly upgrade or over time downgrade his defences*[2]. Downgrading is likely to be realised due to budgetary pressure and a lack of observed attacks.

Another part of the model focuses on a different form of DDOS attacks, the targeted DDOS attacks. On one hand the defender has specific measures in place and on the other hand *the defender will search for vulnerabilities by specific DDOS testing and then resolve them*[2]. A successful targeted DDOS attack will evoke temporary higher effort on solving vulnerabilities. All these defence related activities will cost the organisation money (output model 7 cost of defences).

If an attack is successful the defender needs to respond to this attack for mitigating the effects of the attack on the organisation (sub model 5 major incident response). In this study this is called major incident response in line with the jargon of the investigated organisation. During this response selected senior staff will stop their regular day to day activities and resolve this major incident. *If an organisation has to mitigate too many successful attacks its staff can be fully occupied with resolving these incidents. In such a case the organisation suffers from the capability trap and activities such as threat intelligence analysis or even strategic project implementation, are slowed down or temporary stopped*[3]. The effect of a successful attack on the organisation might be threefold. Customers cannot perform intended transactions, the organisation has additional costs for maintaining its service levels and in worst case scenario customers go elsewhere (output model 6 customers perspective). Customer churn is increased by declining trust evoked by multiple successful attacks in a certain time period.

In the final submodel all financial aspects of this system are aggregated and evaluated (output model 8 financial evaluation). For evaluation the total effects on cash-flow (Dorsman 2003) and the total benefits of the investment compared to the cost of security investment (Anderson et al. 2013, Brecht and Norway 2013) are considered. The first is called in this research "total money spent" and the latter "net present security value[4]". The net present security value will also consider the time impact of money.

[2] Upgrade defenses based on threat intel is a goal seeking dominant loop in the model, adjusting defenses bases on successfulness of the attacker are dominant loops as well as resolving vulnerabilities

[3] Strategic project delay might be potential dominant loop but depends on the upgrade or downgrade of defenses.

[4] Net present security value can be explained as Total financial impact for security investment decisions taking into account the time value of money. Total financial impact for security investment decisions can be explained as the total cost of the damage of avoided successful DDOS attacks minus the total cost of the DDOS defence and the total

Model validation and testing

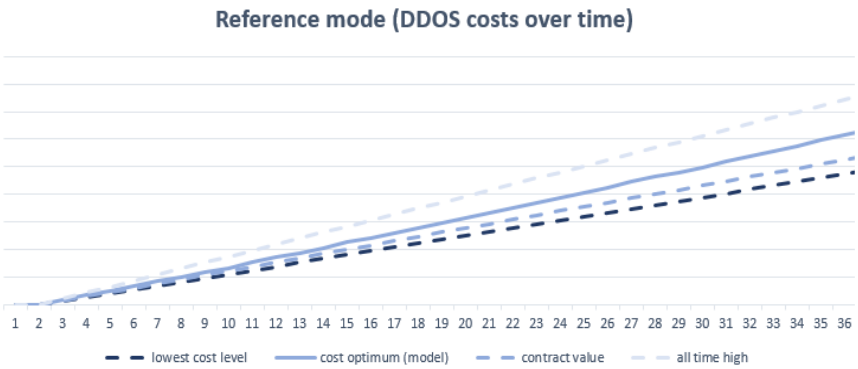

Fig 5. Reference mode (DDOS cost over time) 36 months of model behavior has been compared with the lowest possible contract – cost, the maximum contract cos and the average

Following Forrester and Senge (1979), Barlas (1996) and Sterman (2000) we have tested and validated the structure and the behavior of our model. Amongst others, we validated the structure by interview, model walk through and comparison with DDOS papers, DDOS policies and DDOS reference architecture. In addition model behavior has been compared with actual behavior with regards to various variables. More detailed information on testing and validation can be found in Appendix 2 of the supportive material. Initial values underlying sources are explained in Appendix 3 of the supportive material.

The evaluation of the reference mode is based on the net present value and total money spent over the first 36 months. During this period there were no successful DDOS attacks observed. Therefore the only possible cash impact is related to contract cost, as there is no temporary service loss. Figure 5 indicates that the behavior of the model is in line with the contract costs. Since the various contracts have variable and fixed price elements comparison has been made with the minimum cost, maximum cost and the contracted value.

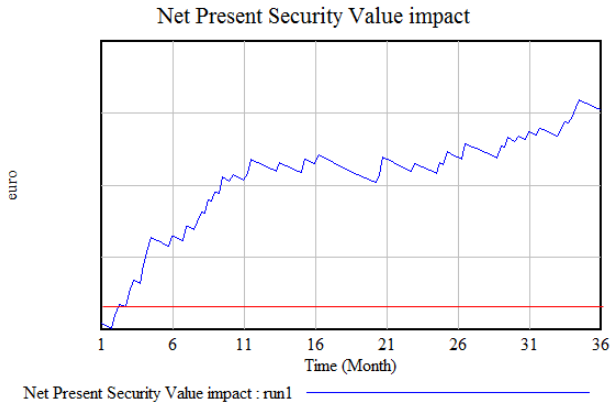

Fig 6. Net present security value. Red line indicate 0 euro

The net present security value should be positive during this period because DDOS defense contributes towards organizational defense. This behavior is visible in Figure 6.

cost of damage of successful DDOS attacks. The avoided damage will be partially considered in line with Gordon and Loeb (2003)

Policy evaluation

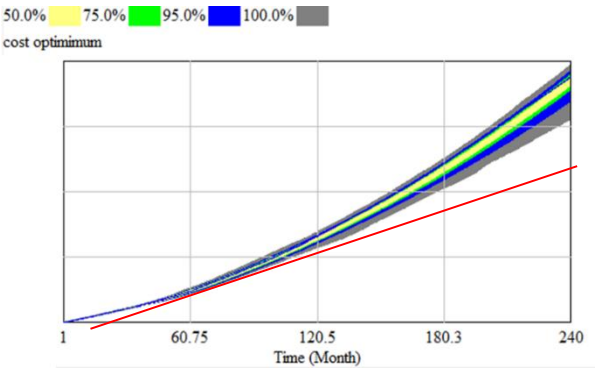

Fig 8. Total consequences in cash

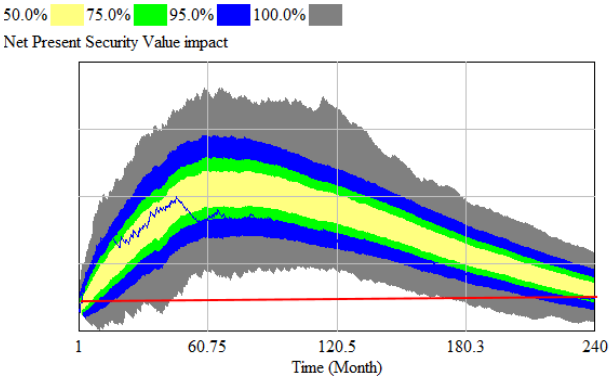

Fig 7. Net present security value over 240 months. Redline is 0

The validated model can now be run for a very long time period based on current policy settings and behaviour of agents in this complex systems., This is called the initial simulation. In this simulation we ran 5.000 different runs and presented the figures in the form of a sensitivity analysis in this paper. Figure 7 shows a more or less table pattern between month 60 and month 120 and here-after a strong decline. Figure 8 indicate that the cash impact of successful attacks and DDOS cost increase after month 120**.** This behaviour can be explained by the following three developments. First, the shared defences at the level of ISP and in the cloud have to mitigate more and heavier DDOS attacks over time. Since these defences are shared it might more often happen

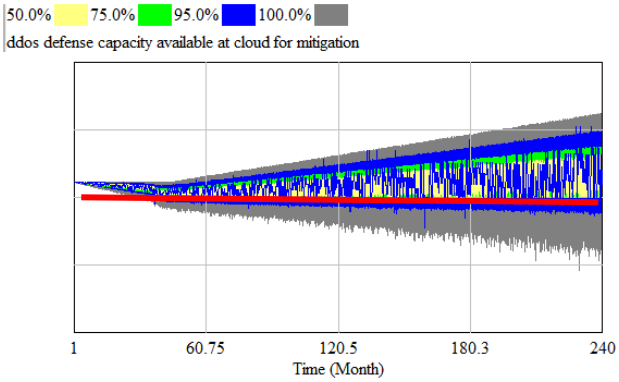

Fig 9. Sensitivity analysis DDOS defense available in the cloud. Below the red line no defense capacity is available. The probability of non-available develops from 5% to 25% as from month 40

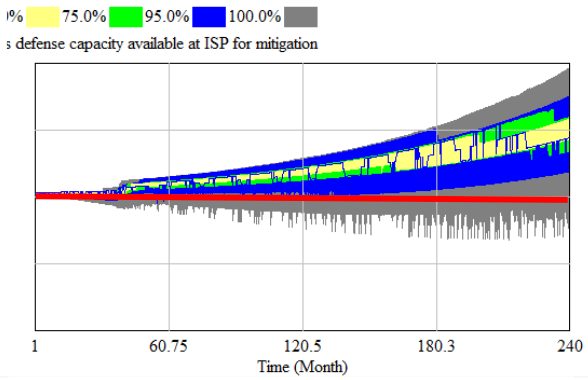

Fig 10. Sensitivity analysis on defense capacity available at the ISP. Below the red line no defense capacity is available. The probability of non-available is approx. 5% as from month 30

that (a part of) the defence is used for mitigating attacks on others, resulting into more defence capacity needed at the own location. This is visible in Figures 9 and 10. Second, the defences against targeted DDOS attack will improve over time and maintain an equilibrium compared with the attackers' innovation pace from month 120 onwards as shown in Figures 11 ad 12. Third, Figure 13 shows that the cost of DDOS defence will increase strongly while the benefits of successful DDOS protection shows a stable increase. This increase of DDOS defence

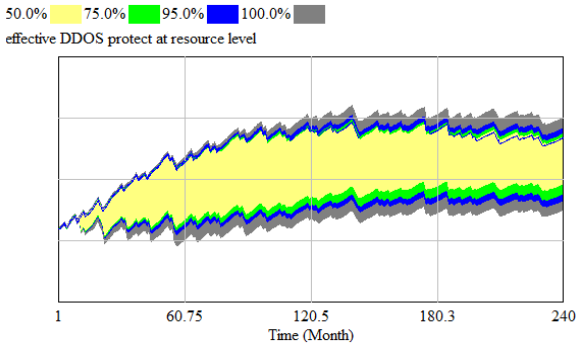

Fig 11. Effective DDOS protection at resource level. Maximum defense effectiveness has been reached at month 120.

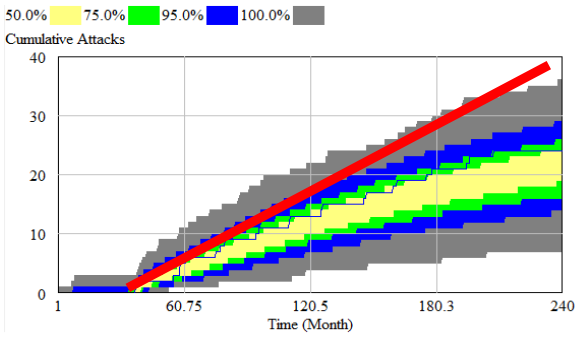

Fig 12. Cumulative (not mitigated) attacks. After month 120 the increase in successful DDOS attacks declines

cost is caused by inflation and more capacity needed, while the price lowering effect caused by innovation is expected to have a limited impact on this increase.

The financial evaluation indicates that the effectiveness of DDOS policy settings will deteriorate after month 120, indicating that money spent on DDOS will contribute less and less to the financial business performance. From a security perspective this financial trends implies that current DDOS defence

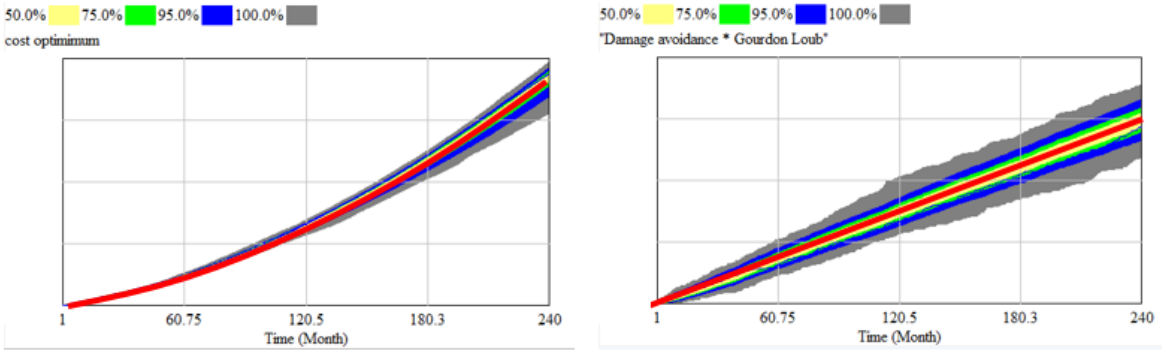

Fig 13. Sensitivity analysis of the cost optimum (= all negative cash impacts of DDOS defences and successful DDOS attacks) with red line indicating exponential growth versus fraction of (in line with Gordon Loub) sensitivity analysis of damage avoidance (= benefits of not having a successful DDOS attack) with redline indicating linear growth

policy settings seems to lose their effectiveness over time. Böhme (2010) lists the following options for decision making: risk mitigation, risk avoidance, risk transfer and risk retention[5] We believe risk avoidance is no suitable strategy because it implies moving from online activities to off-line activities which will result into significant increase of search and transaction cost. Therefore we simulate the following policy settings:

- Increase investment pace (risk mitigation)
- Increase footprint of business activities (risk mitigation)
- Engage in a trusted network initiative (risk transfer)
- Lobby for stronger government and law enforcement intervention (risk transfer)
- Accept these cost for doing business (risk acceptance)
- Accept lower service levels (risk acceptance)

[5] In this paper we used the following definitions:

- Risk retention is a decision to have a monetary reserve at the organization itself to cope with unexpected financial claims or losses, comparable with self-insurance.
- Risk mitigation involves taking measures that reduces the probability that a specific risk will occur and/or the associated impact of that risk when its occurs.
- Risk transfer implies that another organization is willing to take the financial burden of a specific risk when it occurs (insurance).
- Risk acceptance is taking the decision to accept a specific risk without taking additional measures. Usually risk acceptance takes place when the cost of additional measures are higher compared to the consequences of this risk .

In Appendix 4 of the supportive material the model parameters for each scenario are included.

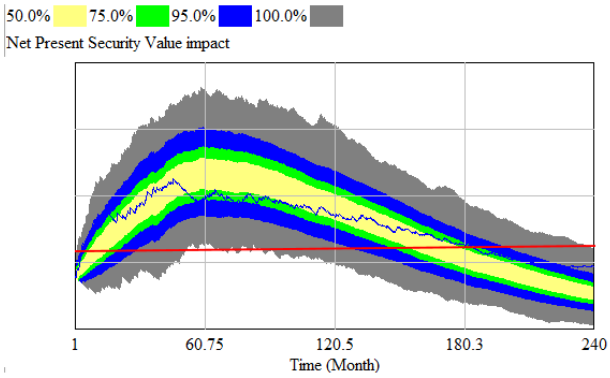

Fig 14. Net Present Security Value for simulation "increase investment pace". The redline indicate 0

The risk mitigation strategy of increasing the investment pace implies increasing all organisational defence capabilities more frequently during regular life cycle management if threat intelligence information indicates increased attacker capabilities. Compared to Figure 7, Figure 14 shows a stronger decline in net present security value which means this is not a financial solid policy adjustment. The additional investment in security defences does not lead to benefits in the sense of preventing the attacks.

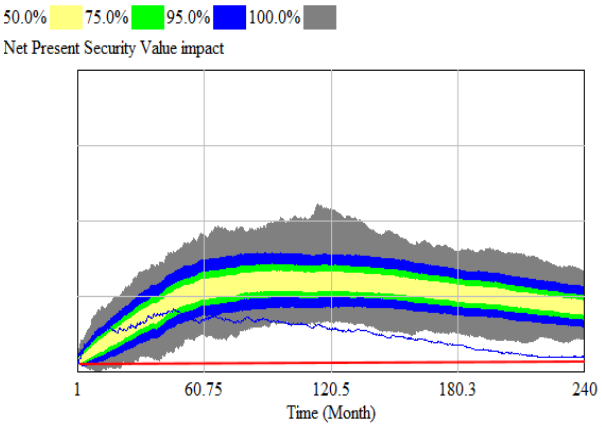

Fig 15. Net Present Security Value for simulation "increase footprint of business activities". The redline indicate 0

The risk mitigation strategy of increasing the footprint of business activities implies a concentration of assets and customers into one customer service platform over time. This means also more means can be allocated to this platform for protecting it from DDOS attacks. Therefore Figure 15 shows an overall higher and stable net present security value. This higher stable value also provides the opportunity to absorb more investment if needed.

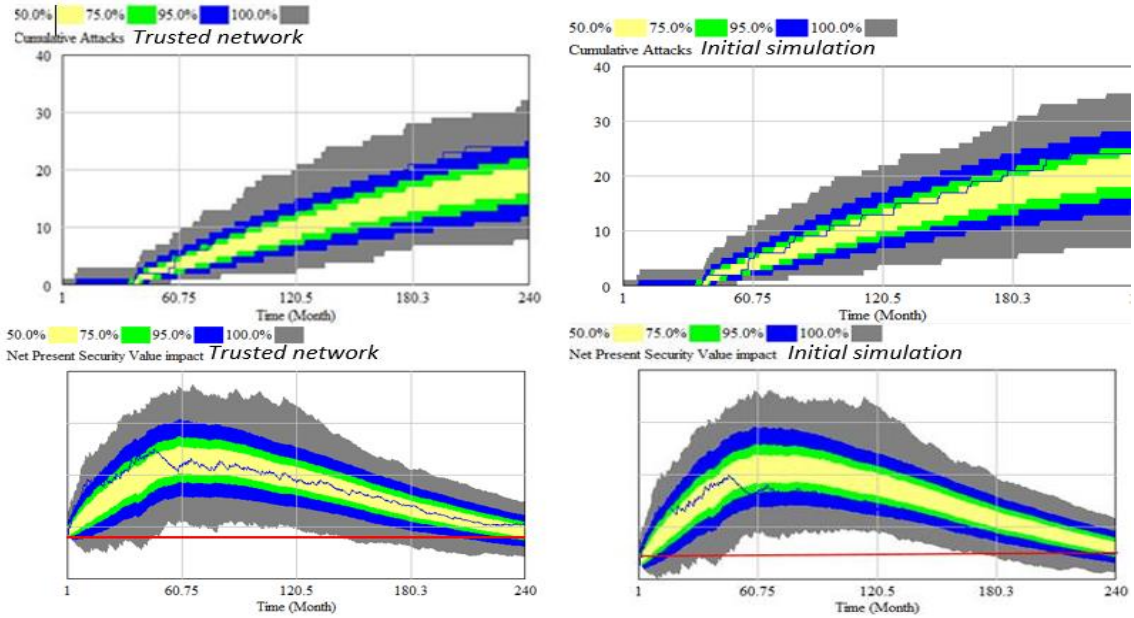

Fig 16. The trusted network imitative a comparison with the initial simulation on Net Present Security Value and number of successful DDOS attacks. The red line indicate 0

The risk transfer strategy of engaging in a trusted network initiative. This initiative implies that after the detection of a very large DDOS attack the trusted network will temporarily be disconnected from the internet and only local communication within this network remains active. International internet traffic will be blocked for the duration of the DDOS attack. Costs will be incurred outside the boundaries of the organisations and each participant in such an initiative should bear a part of these costs. In the simulation we allocated some "assumed cost" of such initiative. This strategy shows a slightly less declining net present value and slightly less increase of the number of successful DDOS attacks over time as seen in Figure 16.

The risk transfer strategy for lobbying for more government and law enforcement intervention will have an cost impact on the government. Despite the fact that DDOS attack capacity growth might be impacted (Figure 17), the number of mitigated attacks is more or less the same compared to the initial simulation. This might be explained by either the DDOS botnet resilience, or intervention impact through DDOS botnet destruction or hackers prosecution needs to be improved significantly. Another option might be lowering the possible foothold for DDOS botnets, especially internet of things. Internet of things are relatively poor protected and easily misused. Legislation about ownership for internet of things should improve its security and therefore the possibilities for exploitation (Schneier 2016). The strategies of accepting the cost for doing business or accept the lower service

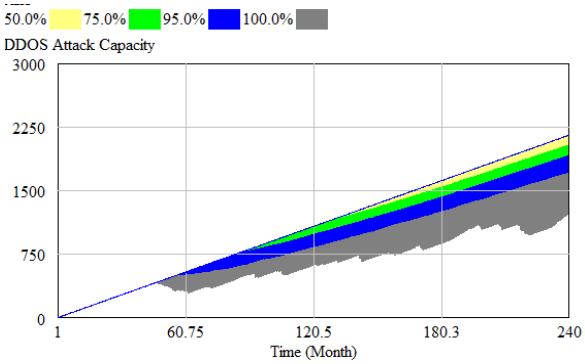

Fig 17. DDOS capacity development under the assumption of stronger government and law enforcement intervention.

levels implies that the decline in financial performance due to DDOS attacks or lower availability of services will be accepted. For these no additional simulation is needed.

Summary of findings and discussion

According to Warren (2016a) system dynamics modelling is complementary to enterprise architecture and can be used for business case design for financial decision making (Warren's 2016b). This research in the field of DDOS defences in a financial organisation is an example of the operationalization of his thoughts. The model we have built relates DDOS defence capabilities to DDOS defence vulnerabilities and the impact of DDOS attacks. By following Böhme (2010) we were able to merge various security metrics with relevant feedback loops and time delay effects into an investment model. We believe our modelling technique addresses some of the difficulties in estimating financial variables. Our model is based on 36 months of historical performance of an organisation and 204 months of future simulation and provides tipping points in long term financial performance as indicators of a change in policy effectiveness. Based on our initial simulation we identified the need for policy change and defined six different alternatives. Our model indicates that keeping increasing the defences in line with the attackers' strength will cost more and more time and might not even considered sustainable. We showed that increasing the footprint of business activities provides a better base for future investment. In addition other forms of DDOS defence cooperation should be investigated further, like trusted network imitative or far stronger and faster means of government intervention against botnet or hackers. This investigation is needed because it will have a cost impact on agents outside the boundaries of this model. Another option is to accept the higher cost for doing business or lower service performance.

Due to the lack of data we have used dimensionless multipliers as described by Fischer (2005) to capture certain variables and modelled attack "events" instead of using the attack-unit of megabit per second (Mbps). We also used a monthly time unit and time steps of 0.25 to cope with the different time period between decision making and DDOS attack duration. In addition we hope to improve this model by making it a multi-country model so the model can be used for group wide policy evaluation as well.

In addition future research should indicate to what extent and under what circumstances this way of modelling can improve financial decision making in the field of cyber security by comparing this method with others.

Literature (for paper and supportive material)

Akamai, 2015, state of the internet, case study: summary of operation DD4BC, DDOS extortionist actor group, issue date 9-9-15

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M.J.G., Levi, M., Moore, T., Savage, S., 2013, Measuring the Cost of Cybercrime, The Economics of Information Security and Privacy, P265-300, Springer, New York

Arbor Networks, 2016, Worldwide infrastructure security report, volume XI, Arbor Networks, the security division of netscout

Atlantic Counsil, 2015, overcome by cyber risks? Economic benefits and costs of alternative cyber futures, Zurich Insurance Company Ltd, Zurich

Barth, A., Rubinstein, B.,I.,P., Surandararajan, M., Mitchell, J.,C., Song, D., Bartlett, P.,L., 2012, A learning-Based Approach to Reactive Security, IEEE transactions on dependable and secure computing, **Vol.9** no.4.,

Brecht, M., Norway, T., 2013, A closer look at information security costs, the economics of information security and privacy, Spinger

Barlas, Y, 1996, Formal Aspects of Model validity and validation in system dynamics, System Dynamics Review **Vol.12**, no 3, 183-210

Bitner J.,M., Booms, B., H., Tetreault, M.,S., 1990, The Service Encounter: Diagnosing Favourable and Unfavourable Incidents, Journal of Marketing, **Vol. 54**, 71-84

Böhme, R., Moore, T., 2016, The Iterated Weakest Link, a Model of Adaptive Security Investment, Journal of Information Science, **Vol 7**, No 2,

Böhme, R., 2010, Security Metrics and Security Investment Models, 5th International Workshop on Security, IWSEC 2010, Kobe, Japan, November 22-24, Proceeding pp 10-24

Chismon, D., Ruks M., 2015, Threat Intelligence: collecting, Analysing, Evaluating, MWR security, CCERt-UK and CPNI, 2015IEE

Clayton, R., Moore, T., Christin, N., 2015, Concentrating Correctly on Cybercrime Concentration, Workshop on Economics in Information Security 2015 conference paper

Dittrich, D., 2012, So you want To Take Over a Botnet, 5th USENIX Workshop on Large-scale Exploits and Emergent Threats, April 24th 2012 San José

Dorsman, A., B., 2003, Vlottend Financieel Management, analyse en planning, 8e druk, Reed Business Information, Doetinchem, Nederland

Douligeris, C., Mitrokotsa, A., 2004, DDOS attacks and defence mechanisms: classification and state-of-the-art, Computer Networks, **nr 44**, page 643-666

Edwards, B., Hofmeyr, S., Forrest, S., 2016, Hype and Heavy Tails: A closer Look at Data Breaches, Journal of Cyber Security, **Volume 2**, Issue 1

Fisher, D., M., 2005, Modelling dynamic systems lessons for a first course, ISSE systems 2005, Lebanon

Forrester, J.W., Senge, P.M., 1979, Tests for building confidence in system dynamics, models, system dynamics group, Sloan School of Management, MIT, Cambridge, Massaschusetts, June 8

Gordon, L.,A., Loeb, M., P., 2002, The Economics o Information Security Investments, ACM Transactions on Information System Security, **vol. 5**, No 4, November, pages 438-457

Imperva Incapsula (2016), Imperva Incapsula Survey: What DDOS Attack Really Cost Business, downloaded May 9th 2016, http://lp.incapsula.com/rs/804-TEY-921/images/eBook%20-%20What%20DDoS%20Attacks%20Really%20Cost%20Businesses%20%28new%29.pdf

Imperva Incapsula (2015), Imperva Incapsula Global DDOS threat landscape: understanding the latest DDOS attack trends, methods and capabilities, downloaded May 9th 2016, https://lp.incapsula.com/ddos-report-2015.html?_ga=1.15816822.1579975859.1483105873

Imperva Incapsula (2014), Imperva Incapsula Global DDOS threat landscape report 2013-2014, downloaded May 9th 2016, https://www.incapsula.com/blog/wp-content/uploads/2015/08/2013-14_ddos_threat_landscape.pdf

Imprerva Incapsula (2015), Global DDOS threat landscape Q2 2015 Understanding the latest DDos Attack trends, methods and capabilities

Khajuria, A., Srivastava, R., 2013, Analysis of the DDOS Defense Strategies in Cloud Computing, International Journal of Enhanced Research in Management & Computer Applicatios, **Volume 2**, Issue 2,

Kim, C., Tao, W., Shin, N., Kim, K., S., 2009, An empirical study of customers' perception of security and trust in e-payment systems, electronic commerce research and applications

Kwon, J., Johnson, E.,M., 2015, The market effect of healthcare security: Do patients care about data breaches?, Workshop on Economics in Information Security 2015

Lee, M., J., Lee, J., 2010, The impact of information security on customer behaviour: a study on large-scale hacking incident on the internet, Springer, published online,

Libicki M.,C., Ablon, L., Webb, T., 2015, The Defender's Dilema, Charting a Course Towards Cybersecurity, Rand Corporation, Santa Monica, California

Maheshwari, R., Krishna, R., 2013, Mitigation of DDOS attacks using probability based distributed hop count filtering and round trip time, International Journal of Engineering Research and Technology, **Vol 2**, Issue 7, July

Martinez-Moyano, I.J., Conrad, S.H., Anderson D.F., 2011, Modeling behavioural considerations related to information security, computers & security **30**, 397-409

Martinez-Moyano, I.J., Morrison, D., Sallach, D., 2015, Modeling Adversarial Dynamics, Proceedings of the 2015 Winter Simulation Conference

Mirkovic, J., Martin, J., Reiher, P., 2004, A Taxonomy of DDOS Attacks and DDOS Defense Merchanisms, ACMCIGCOMM Computer Communication Review, **Vol 34**, issue 2,

Mittal, A., Shirvastava, A.K., Manoria M., 2011, A Review of DDOS Attack and its Countermeasures in TCP Based Networks, International Journal of Computer Science & Engineering Survey (IJCSES) **Vol.2**. No. 4.

Naykude A.B., Jadhav, S.S., Kudale, K.D., Sheikh, S., Patil, Y, 2015, TDDA: Traceback-based Defence Against DDOS Attack, International Journal on Recent and Innnovation Trends in Computing and Communication, **Volume: 3**, Issue: 9

NetDilligence 2014, cyber claim study 2014, NetDilligence

NetDilligence 2013, cyber claim study 2013, NetDilligence

Pencavel J., 2014, The productivity of Working Hours, discussion paper series, IZA DP **No 8129**

Ponemon 2012, 2012: cost of data breach study: global analysis, Ponemon institute LLC

Ponemon 2013, 2013: cost of data breach study: global analysis, Ponemon institute LLC

Ponemon 2014, 2014: cost of data breach study: global analysis, Ponemon institute LLC

Ponemon 2015, 2015: cost of data breach study: global analysis, Ponemon institute LLC

Pruyt, E., 2013, Small system Dynamics Models for Big Issues: Triple Jump towards Real World complexity. Delft: TU Delft Library. 324p.

Rahmandad, H., Repenning, N., 2015, Capability Erosion Dynamics, Strategic Management Journal

Repenning, N., P., Sterman, J.,D., 2002, Capability Traps and Self Confirming Attribution Errors in the dynamics of Process improvement, Administrative Science Quaterly, **47**, 265-295

Reinmoeller, P., Baardwijk, N., 2005, The Link between Diversity and Resilience, MitSloan Management Review,

Rue, R., Pfleeger, S., L., Ortiz, D.,2007, A framework for Classifying and Comparing Models for Cyber Security Investments to Support Policy and Decission Making, Workshop on Economics in Information Security 2007

Specht, M.L., Lee, R.B, 2004, Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures, Distributed systems, pp 543-550,

Schweitzer, M.,E., Hersley, J.C., Bradlow E.,T., 2006, Promises and lies: restoring violated trust, Organizational Behavior and Human Decision Processes, **101**, 1-19

Sterman, J., 2000, Business Dynamics: system thinking and modelling for a complex world, Irwin MC Graw-Hill

Sterman, J.,2006, Learning from Evidence in a complex world, public health matters, **vol 96**. No 3.

Su, X., 2006, An overview of Economic Approaches to Information Security Management, University of Twente, Information System Group, Enschede, The Netherlands

Tongia, R., Kanika, J. 2003, Investing In Security – Do not rely on FUD, ISACA

Traverski, A., Kahneman, D., 1973, Judgement under uncertainty: heuristic and biases, Oregon Institute Research bulletin, Volume **13**, no 1.

Vlaanderen, K., Jansen, S., Brinkkemper, S., Jaspers, E., 2011, The agile requirements refinery: Applying SCRUM principles to software product management, Information and Software Technology **53,** 58-70

Verizon DBIR 2015, 2015 data breach investigations report, Verizon

Vennix, J.A.M., 1996, Group Model Building, facilitating team learning using system dynamics, John Wiley & Sons, West Sussex, England

Vogus, J., T., Sutcliffe, K., M., 2007, Organizational resilience: Towards a theory and research agenda, conference paper

Warren, K, 2016a, Entreprice Architectures: Easier, Faster, Better with System Dynamics models, www.linkedin.com viewed on 2016-11-8 and supportive video on www.sdl.re/OGEASD

Warren, K., 2016b, main stream system dynamics, international conference system dynamics, Delft, Netherlands

Warren, K, 2016b, *Main-stream System Dynamics*, presentation on international system dynamics conference 2016, Delft, https://www.youtube.com/watch?v=JGPj3hxYwPU

Zargar, S.T., 2013, A survey of Defense Mechanisms Against Distributed Denial of Service (DDOS) Flooding Attacks, IEEE: Communications & Tutorials

Zhang, G., Parashar, 2006, Cooperative Defense against DDOS Attacks, Journal of Research and Practice in Information Technology, **Vol 38**. No. 1

Zeijlemaker, S (2016a), Exploring the dynamic complexity of the cyber security economic equilibrium, PhD colloquium of the 34th International Conference of the System Dynamics Society, Delft, Netherlands, july 17 - july 21

Zeijlemaker, S (2016b), Exploring the dynamic complexity of the cyber security: does a deeper understanding support financial policy evaluation?, PhD Research Proposal, March 2017, Radboud University

Websites

Agile Manifesto, 2001, agile manifesto, 2001, (various writers), available at: http://agilemanifesto.org/

Atlas, 2014 – 2015, are variaous reports based on the atlas data sets which are available at https://www.arbornetworks.com/atlas-portal

IEEE 1471, 2000, defining architecture [online], ISO/IEC/IEEE 42010 Website, available at http://www.iso-architecture.org/ieee-1471/defining-architecture.html

Kessem, L., 2015, The return of Ramnit: life after a law enforcement takedown [online], December 22 2015, Security Intelligence.com, available athttps://securityintelligence.com/the-return-of-ramnit-life-after-a-law-enforcement-takedown/

Khandelwal, S., 2016, 602 Gbps! This may have been the largest DDOS attack in history, January 8 2016, the hackers news, available at: http://thehackernews.com/2016/01/biggest-ddos-attack.html

Kirk, J., 2015, Pushdo spamming botnet gains strength again [online], April 20 2015, PCWorld.com. available at http://www.pcworld.com/article/2912532/pushdo-spamming-botnet-gains-strength-again.html

Kitten, T., 2014, Botnet Takedown: A lasting impact?, June 3 2014, BankInfoSecurity.com, available at http://www.bankinfosecurity.com/malware-takedown-lasting-impact-a-6903

Kovacs, E., 2012, The longest DDOS attacks in H2 of 2011 lasted 80 days, February 29 2012, Softpedia.com, available at http://news.softpedia.com/news/The-Longest-DDOS-Attack-in-H2-of-2011-Lasted-80-Days -255688.shtml

Krebs, B., 2016, KrebsOnSecurity Hit by Record DDOS, September 2016, KrebsOnSecurity.com, available at https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

Newman, L. H., What we know about Friday's massive east coast internet outage, October 21 2016, wired.com, available at https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

Schneier, B., 2007, CYA security, Schneider on security, downloaded on 08-30-2015, available at https://www.schneier.com/blog/archives/2007/02/cya_security_1.html

Scheiner, B, 2016, Security Economics of the Internet of Things, downloaded on 15-02-2017, available at https://www.schneier.com/blog/archives/2016/10/security_econom_1.html

Statistica, viewed in 2016, Average net interest margin of banks in the United States from 1995 to 2015 [online] (no date), statistica.com, available at https://www.statista.com/statistics/210869/net-interest-margin-for-all-us-banks/

Ungureanu, H., 2016, World's largest DDOS attack breaks records, clocks at massive 500 Gbps, 27 January 2016, techtimes.com, available at http://www.techtimes.com/articles/128260/20160127/worlds-largest-ddos-attack-

breaks-records-clocks-at-massive-500-Gbps-worldwide-infrastructure-security-report.htm

Quora.com, viewed in 2016, How long does a distributed denial-of-service (DDOS) last? (various dates and various writers) available at: https://www.quora.com/How-long-does-a-distributed-denial-of-service-DDoS-last