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

Sander Zeijlemaker, PhD Student Radboud University, Institute for Management Research, Postbus 9108, 6500 HK Nijmegen, +31 6 29 46 84 89, s.zeijlemaker@fm.ru.nl

Etienne Rouwette, Professor system dynamics, group model building, decision support, Radboud University, Institute for Management Research, Postbus 9108, 6500 HK Nijmegen, +31 24 36 11 468, e.rouwette@fm.ru.nl

Appendix 1: explaining the submodels

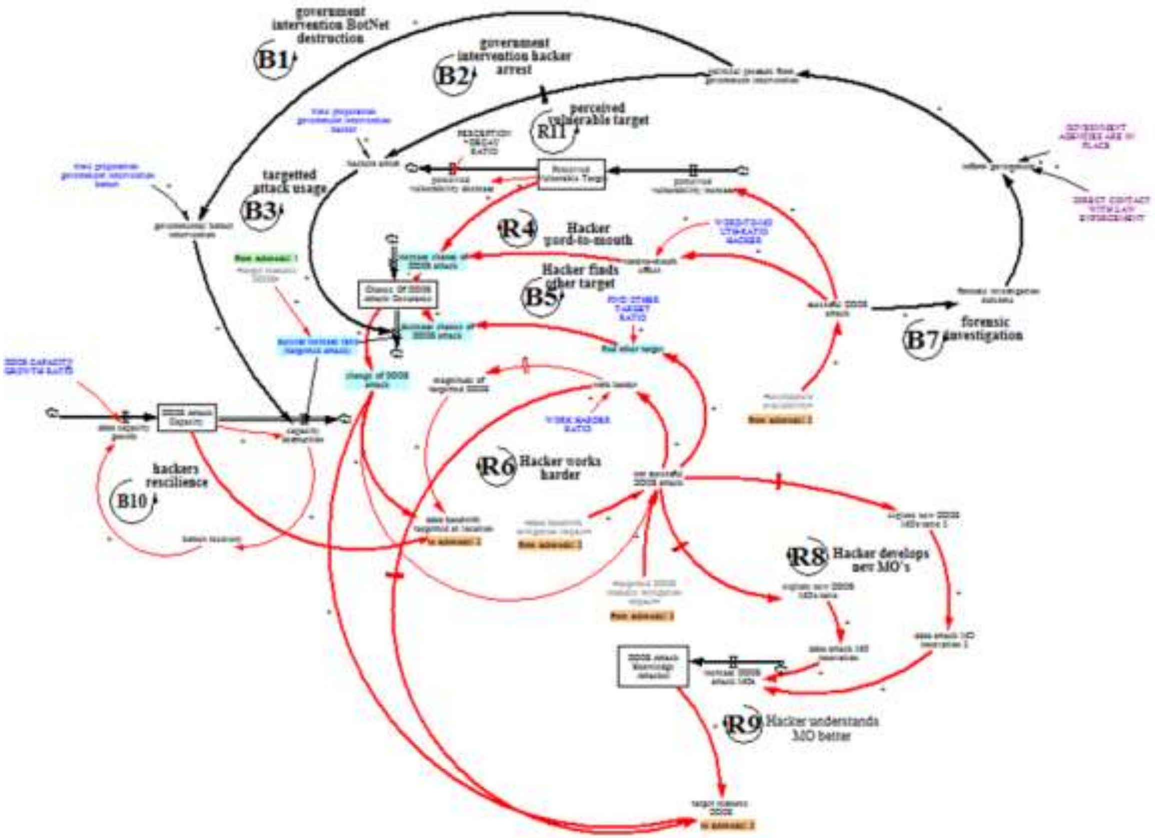

government intervention BotNet destruction
B1
government intervention hacker arrest
B2
perceived vulnerable target
R11
targetted attack usage
B3
R4
Hacker word-to-mouth
Hacker finds other target
B5
B7
forensic investigation
hackers resilience
B10
R6
Hacker works harder
R8
Hacker develops new MO's
R9
Hacker understands MO better

Fig 18. Sub model 1 attacks; perspective DDOS attack

sub model 1: Attackers perspective DDOS attack

Figure 18 shows the sub model about the attackers perspective including attack capacity, government interventions and botnet usage.

Botnets are the dominant mechanism that facilitate DDOS attacks (Zargar et al 2013). The average DDOS bandwidth attack capacity evolves over time (imperva incapsula 2015). Sometimes this capacity is impacted by government intervention on Botnets as described by Ditrich (2012). This is resembled by the **B1 government intervention Botnet Destruction** loop. Sometimes the hacker is also arrested as explained by **the B2 government intervention hacker arrest loop.** Arrested hackers lower the chance for DDOS attacks for a period of time. However most botnets are not fully destroyed by government intervention and will recover over time (Kessem 2015 and Kitten 2014) as indicated by the **B10 hackers resilience loop.**

A hacker has two means for attacking: a bandwidth attack or a target a specific resource. Firstly, the average DDOS bandwidth attack development, magnitude of DDOS bandwidth attacks and the chance of DDOS attack influence the DDOS bandwidth attack at the targeted location. Depending on the defense policy setting (sub model 2) against bandwidth attacks this attack is successful or unsuccessful.

Secondly, the probability of a DDOS attack, the DDOS attacker knowledge and multifactor attack ratio influence if an targeted resource attack will be launched. This form of attack is more sophisticated compared to a bandwidth DDOS attack and requires specific knowledge and skills to execute. Therefore its occurrence is less frequent compared to bandwidth attacks. In addition an executed targeted resource DDOS attack will leave characteristics behind related to the knowledge and means used by the hackers, which can be very useful information during forensic investigation. Therefore these characteristics will have a positive effect on successful government interventions (**B3 targeted attack usage**). Depending on the defense policy setting (sub model 3) against targeted attacks this attack is successful or unsuccessful. A successful DDOS attack is in this paper defined as an attack that impact customer service level and result into a response action from the defender towards this attack.

A successful attack will evoke positive word-of-mouth behavior in the hackers communication akin various adaptation models published in (Sterman 2000). This word-of-mouth effect affects future actions since the results are shared in the community. This is the **R4 hacker word-of-mouth** loop. However, the number of attackers that attacks the defender and the total number of attackers are unknown. Therefore we have used a probability function that estimates the attacking behavior instead in this paper. Its initial value has been validated by comparing the number of DDOS attacks with the actual observed attacks that were successful and not successful over time. We believe there are no material differences compared to normal adaptation models.

A successful attack also creates a temporary image the targeted organization has weak defenses which might evoke more attacks. This is the **R11 perceived vulnerable target loop**. A successful DDOS attack will also cause forensic investigation to start obtaining evidence and lessons learned (Specht and Lee 2004). This evidence might be useful for future legal steps or government intervention against the hacker (**B7 forensic investigation**). Forensic research will require some efforts of security staff.

A unsuccessful DDOS attack will result into:

- a hacker finding another target (**B5 hacker finding another target**).
- a hacker working harder by increasing magnitude and duration of the next DDOS attack in order to be successful at a second attempt (**R6 hacker works harder**).
- a hacker searching for new means of operations (MO) in order to be successful in the future (**R8 hacker develops new MO**). In conjunction with finding new MO's the already known MO become more and more common (**R9 hacker understands MO better**). By doing so targeted resource attack execution becomes less difficult to execute. The stock “DDOS attack knowledge MOs” will be the start of an aging chain used in sub model 3 for modelling the defense behavior.

Sub model 2: Defenders perspective: bandwidth attacks

Figure 19 explains the sub model about the defence against bandwidth DDOS attacks. A successful bandwidth attack will be mitigated if the defence capacity for these attacks is equal or higher compared to the magnitude of the attack. Both are usually stated in GBPS. Furthermore Zhang and Parashar (2006), Khajuria and Srivastava (2013) have argued that the DDOS defense should be as close as possible to the attacker. Early detection provides the targeted organization more time to respond as an organization. This means beside defenses at the location and defenses at the internet service provider (ISP) have been included into the model. Also cloud provider related defences that can handle large volumes are included. However the cloud provider and ISP can also be subjected to DDOS attack that might result into non-availability of their defences. All these defences can be improved by:

- proactive supplier policy investments evoking defense upgrade before it is actually needed (**B18 proactive supplier cloud investment**, **B14 proactive supplier ISP investment**
- reactive management intervention after a successful DDOS bandwidth attack (**B15 reactive could investment**, **B20 reactive ISP investment**) although the organization has to deal with handling the consequences of an DDOS attack and related damage before this upgrade. In addition there might be a financial impact as a result of the detection trap.
- proactive management intervention based upon adjustment of Reference Architectural norms (**B12, B13, B19 global DDOS defense improvement**) as a result of threat intelligence analysis. This analysis indicates that defenses are not able to address near future expected attack behavior (see sub model 4: the resilient organization: threat intelligence). These upgrades will usually be included during regular life cycle management upgrades.

Real-time monitoring controls, like abnormal behavior detections, geo blocking at ISP and DDOS monitoring are described in this sub model. If automated DDOS monitoring is not in place the DDOS will be detected after the business services have been disturbed. Thus the DDOS defenses will only work preventively if the DDOS attacks can be detected. In addition the first improvement based on adjustment of the reference architecture norms will also include improvements of these detection mechanisms

If no cyber security impacts are observed or detected over time, there will have a negative impact on the willingness to invest in security capabilities. Martinez-Moyano et al. (2011) call this the detect trap. In sub model 2 this is reflected in **R17, R16 the budgetary pressure for lowering cost levels**. After a period of non-perceived attacks the defences (at location, at ISP and in the cloud) will be lowered.

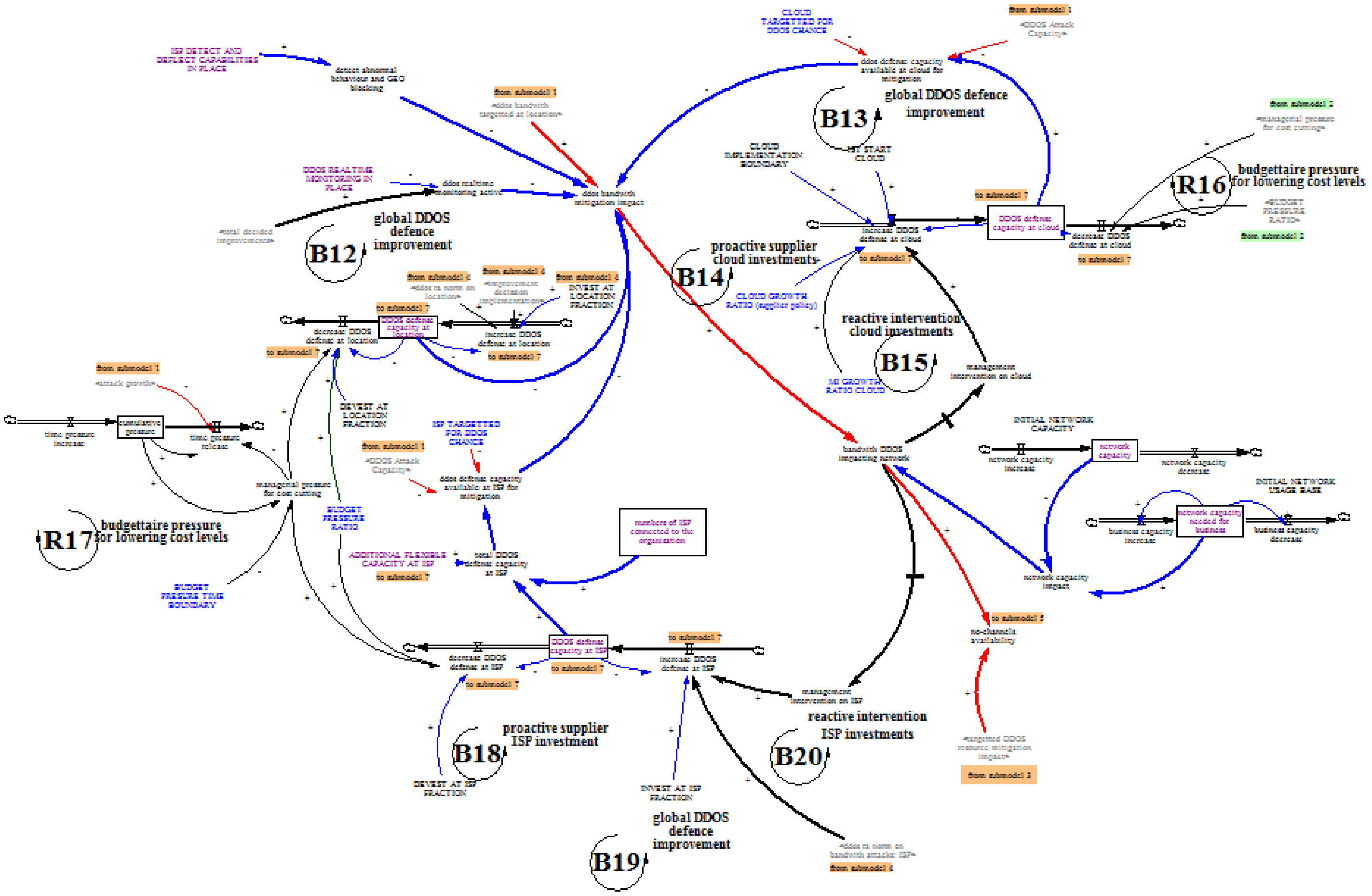

ISP DETECT AND DEFLECT CAPABILITIES IN PLACE
detect abnormal behaviour and GEO blocking
from submodel 1
<ddos bandwidth targeted at location>
DDOS REALTIME MONITORING IN PLACE
ddos realtime monitoring active
ddos bandwidth mitigation impact
<total decided improvements>
B12
global DDOS defence improvement
from submodel 4
<ddos ra norm on location>
from submodel 4
<improvement decision implementations>
from submodel 4
INVEST AT LOCATION FRACTION
to submodel 7
DDOS defence capacity at location
decrease DDOS defence at location
increase DDOS defence at location
to submodel 7
to submodel 7
from submodel 1
<attack growth>
cumulative pressure
time pressure increase
time pressure release
DEVEST AT LOCATION FRACTION
ISP TARGETTED FOR DDOS CHANCE
from submodel 1
<DDOS Attack Capacity>
ddos defence capacity available at ISP for mitigation
managerial pressure for cost cutting
R17
budgettaire pressure for lowering cost levels
BUDGET PRESSURE RATIO
BUDGET PRESURE TIME BOUNDARY
ADDITIONAL FLEXIBLE CAPACITY AT ISP
to submodel 7
total DDOS defence capacity at ISP
numbers of ISP connected to the organization
DDOS defence capacity at ISP
decrease DDOS defence at ISP
increase DDOS defence at ISP
to submodel 7
to submodel 7
to submodel 7
B18
proactive supplier ISP investment
DEVEST AT ISP FRACTION
INVEST AT ISP FRACTION
B19
global DDOS defence improvement
CLOUD TARGETTED FOR DDOS CHANCE
from submodel 1
<DDOS Attack Capacity>
ddos defence capacity available at cloud for mitigation
B13
global DDOS defence improvement
CLOUD IMPLEMENTATION BOUNDARY
MI START CLOUD
to submodel 7
DDOS defence capacity at cloud
increase DDOS defence at cloud
decrease DDOS defence at cloud
to submodel 7
to submodel 7
from submodel 2
<managerial pressure for cost cutting>
R16
budgettaire pressure for lowering cost levels
<BUDGET PRESSURE RATIO>
from submodel 2
B14
proactive supplier cloud investments
CLOUD GROWTH RATIO (supplier policy)
reactive intervention cloud investments
B15
MI GROWTH RATIO CLOUD
management intervention on cloud
bandwidth DDOS impacting network
INITIAL NETWORK CAPACITY
network capacity
network capacity increase
network capacity decrease
INITIAL NETWORK USAGE BASE
network capacity needed for business
business capacity increase
business capacity decrease
network capacity impact
to submodel 5
no-channels availability
management intervention on ISP
reactive intervention ISP investments
B20
<targeted DDOS resource mitigation impact>
from submodel 3
<ddos ra norm on bandwidth attacks ISP>
from submodel 4

Fig 19. Sub model 2 Defenders' perspective: Bandwidth Attack

Sub model 3: Defenders' perspective: Targeted Resource Attacks

Figure 20 demonstrates the defense mechanism against targeted DDOS attacks. DDOS attacks at targeted resources are usually measured in MBps (Megabit per seconds). During the model building process not all relevant model parts could be quantified in MBps. Contrary to the sub model about bandwidth defense not all relevant parts were measured in MBps. Therefore this sub model is based on events (items). Thus an event in this sub model can be one single or multi vector targeted attack at a resource, a vulnerability exploited by a targeted DDOS attack or a vulnerability to be resolved for better defenses against targeted resource attacks. The main structure if this sub model is similar to various aging chain structures published in Sterman (2000) and will be explained below.

Due to the Hackers' search for new means and tools (see sub model 1 '**R8 Hackers develops new MOs'** loop and this model **R24**) the hackers create a "theoretical" stock of possible different manners for using a targeted resource attack exploiting a vulnerability. The attacker can use such attacks for every digital banking channel. Some of these potential attacks will be stopped due to mitigating controls in place at application level, at DNS sever level or at the appropriate resource level. Some of these vulnerabilities are not covered by these controls and still need to be resolved in order to mitigate certain targeted DDOS attack forms.

As a consequence the defender can only resolve these vulnerabilities if the defender is aware of them. DDOS testing is used for obtaining a deeper understanding of the presence of such vulnerabilities **(policy setting DDOS testing)**. DDOS testing can be improved if specific threat intelligence is used. Threat intelligence explaining which type of cyber-attacks are used across the world and what indicators (of compromise) they have. (**B23 threat intelligence provide more accurate DDOS testing** loop is related to sub model 4 'the resilient organization: threat intelligence'). These known vulnerabilities can be resolved. DDOS test preparations and resolving known vulnerabilities will however require efforts of the IT and security staff (**B22 solving DDOS vulnerabilities**). Therefore the list of activities to be done by the IT staff (backlog) will increase (this is visible in the loop **'R35 increase backlog DDOS testing and vulnerability solving'** sub model 5 'the resilient organization: major incident response').

If a targeted DDOS attack is successful management will directs its attention to resolving related vulnerabilities (**B21 management intervention: solving DDOS vulnerability with high prio**) as a reactive security management reaction. For a limited period of time more resources will be allocated to solving known vulnerabilities. Proactively additional defense measures can be put in place if underlying reference architecture will be adjusted (**B25 Global DDOS defense improvement**).

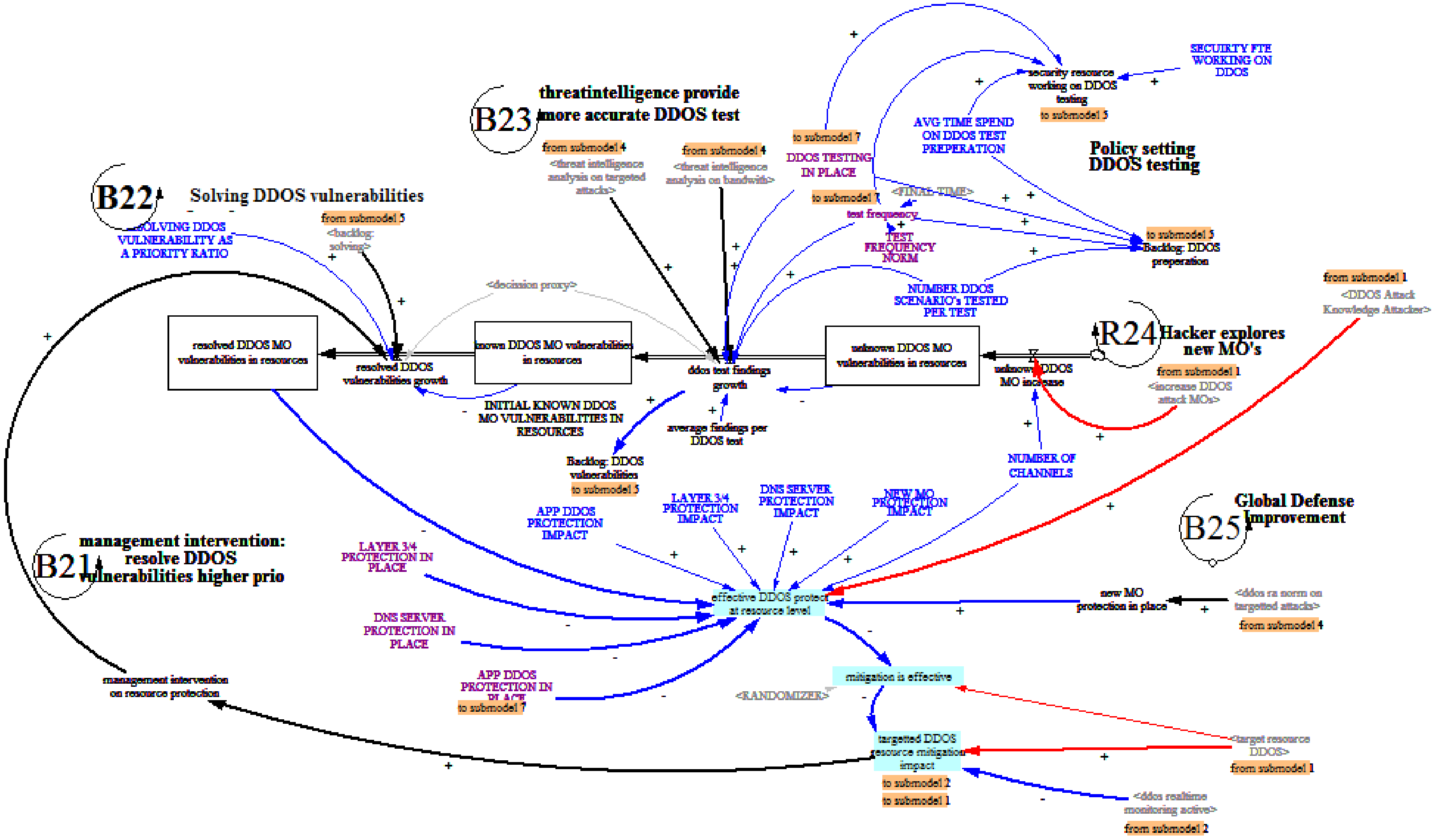

B23 threatintelligence provide more accurate DDOS test
B22 Solving DDOS vulnerabilities
Policy setting DDOS testing
R24 Hacker explores new MO's
B25 Global Defense Improvement
B21 management intervention: resolve DDOS vulnerabilities higher prio
SECUIRTY FTE WORKING ON DDOS
security resource working on DDOS testing
to submodel 5
AVG TIME SPEND ON DDOS TEST PREPERATION
to submodel 7
DDOS TESTING IN PLACE
to submodel 7
<FINAL TIME>
test frequency
TEST FREQUENCY NORM
to submodel 5
Backlog: DDOS preperation
NUMBER DDOS SCENARIO's TESTED PER TEST
from submodel 4
<threat intelligence analysis on targeted attacks>
from submodel 4
<threat intelligence analysis on bandwith>
from submodel 5
<backlog: solving>
RESOLVING DDOS VULNERABILITY AS A PRIORITY RATIO
<decision proxy>
resolved DDOS MO vulnerabilities in resources
resolved DDOS vulnerabilities growth
known DDOS MO vulnerabilities in resources
INITIAL KNOWN DDOS MO VULNERABILITIES IN RESOURCES
ddos test findings growth
average findings per DDOS test
Backlog: DDOS vulnerabilities
to submodel 5
unknown DDOS MO vulnerabilities in resources
unknown DDOS MO increase
from submodel 1
<increase DDOS attack MOs>
from submodel 1
<DDOS Attack Knowledge Attacker>
NUMBER OF CHANNELS
APP DDOS PROTECTION IMPACT
LAYER 3/4 PROTECTION IMPACT
DNS SERVER PROTECTION IMPACT
NEW MO PROTECTION IMPACT
LAYER 3/4 PROTECTION IN PLACE
DNS SERVER PROTECTION IN PLACE
APP DDOS PROTECTION IN PLACE
to submodel 7
effective DDOS protect at resource level
new MO protection in place
<ddos ra norm on targetted attacks>
from submodel 4
mitigation is effective
<RANDOMIZER>
targetted DDOS resource mitigation impact
to submodel 2
to submodel 1
<target resource DDOS>
from submodel 1
<ddos realtime monitoring active>
from submodel 2
management intervention on resource protection
+
-

Fig 19. Sub model 3 Defenders' perspective: Targeted Resource Attack

Sub model 4: the resilient organization: threat intelligence

An architecture can be defined as “The fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution” (IEEE 1471, 2000). A DDOS reference architecture describes all the components of the DDOS defenses, their relation to each other and to the environment. Adjustment of this architecture will be done if threat intelligence about DDOS attack behavior indicate that current DDOS defenses as descripted in the architecture will not hold. In Figure 21 is this visible in the sub model about threat intelligence. Within the context of cybersecurity, threat intelligence represents the synthesis of information detailing potential threats with a solid understanding of network structure, operations, and activities (Chismon and Ruks 2015). This is explained in the **B26** respectively **B27 threat intelligence gathering: bandwidth and targeted resource attack** loops provided the security community has sufficient resources available (no DDOS test preparation, no forensic research and no security incident handling) to handle this information. If the security community lacks staff they cannot analyze incoming threat intelligence (see sub model 5 R4 Reduce proactive security management). This behavior of the security community is comparable to capability trap as described by Repenning and Sterman (2002).

If the threat intelligence analysis indicates that near future DDOS attack are beyond the norms on which the DDOS reference architecture has been built it will evoke a upgrade (**B28 increasing RA norms**). This will take time because the DDOS reference architecture and supportive policies will be upgraded, improvement investments have to be approved and all entities have to implement these improvements (**B29 global improvement initiation**). The model does not include additional backlog items increase based on global improvement initiation because these "peace time"" improvements will be incorporated during regular life cycle management replacement. A part of the items on the backlog will be related to regular life cycle management activities which is part of the day-to-day activities of the IT staff.

This sub model on threat intelligence is based on goal seeking as descripted in Sterman (2000). The defenses (in sub-model 2 and 3) have to be in line with architectural design. If there are not management will take decision to adjust them. The architectural design has to be in line with future attack behavior. If threat intel indicates the architectural design is not, management will take a decision to adjust them.

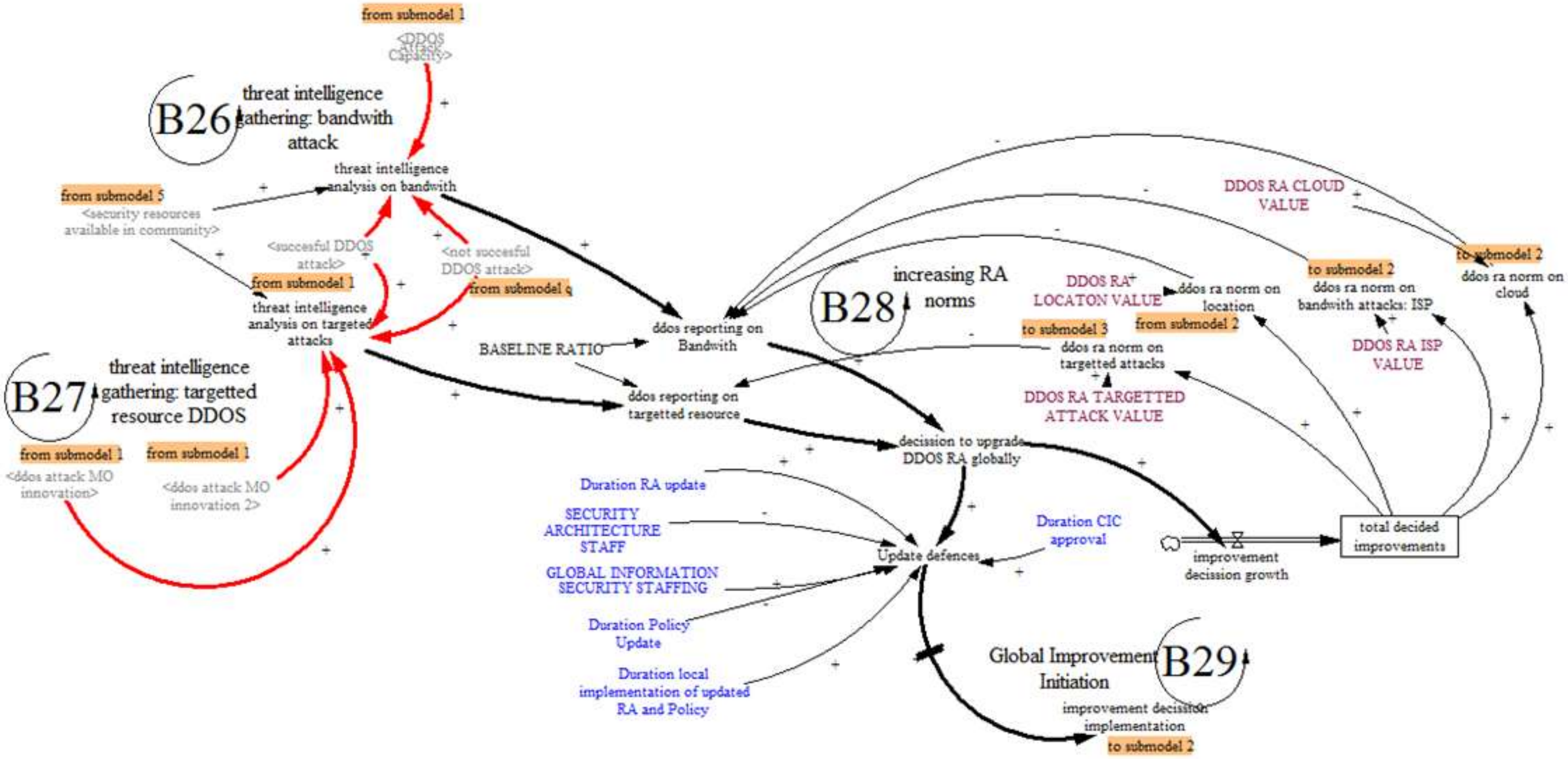

from submodel 1
<DDOS Attack Capacity>
B26
threat intelligence gathering: bandwith attack
threat intelligence analysis on bandwith
from submodel 5
<security resources available in community>
<succesful DDOS attack>
<not succesful DDOS attack>
from submodel 1
from submodel q
threat intelligence analysis on targeted attacks
B27
threat intelligence gathering: targetted resource DDOS
from submodel 1
<ddos attack MO innovation>
from submodel 1
<ddos attack MO innovation 2>
BASELINE RATIO
ddos reporting on Bandwith
ddos reporting on targetted resource
decission to upgrade DDOS RA globally
B28
increasing RA norms
DDOS RA LOCATON VALUE
ddos ra norm on location
from submodel 2
to submodel 3
ddos ra norm on targetted attacks
DDOS RA TARGETTED ATTACK VALUE
DDOS RA CLOUD VALUE
to submodel 2
ddos ra norm on bandwith attacks: ISP
DDOS RA ISP VALUE
to submodel 2
ddos ra norm on cloud
Duration RA update
SECURITY ARCHITECTURE STAFF
GLOBAL INFORMATION SECURITY STAFFING
Duration Policy Update
Duration local implementation of updated RA and Policy
Update defences
Duration CIC approval
improvement decission growth
total decided improvements
Global Improvement Initiation
B29
improvement decission implementation
to submodel 2

Fig 21. Sub model 4: Resilient Organisation: Threat Intelligence

Sub model 5: Resilient organization: major incident response

Figure 22 demonstrates the sub model related to the major incident response. An incident can be defined as an unplanned interruption of the service delivery of an organization. Major incidents label is applicable when this unplanned interruption is increasing across the organization or needs to be resolved quickly. A major incident response will impact the IT staff. In case of a major security incident both IT staff and security staff are impacted. First the major incident response for IT staff will be explained. Here after the more specific behavior related to the field of cyber-security will be explained.
In general the organization has a 'hold the line policy' that implicate that a 'major (security) incident' has to be resolved and operations has to be brought back to its normal state. This means that dedicated resources will be exempted from regular work and solve the incident **(B32 solving major incidents).** If solving the major (security) incident takes too long, overtime will be made, the staff will work harder and more resources are needed. Pencavel (2014) indicated that longer working days and time evoke less productive staff. Therefore even a second or third shift can be needed for time-consuming mitigating activities. In addition most staff involved in the major incident process are senior people. Therefore the remaining workforce will on average have less experience. Since the senior staff resolving an incident they cannot coach and guide the less experienced staff. The remaining workforce is able to continue its work however the team productivity will be impacted due to lack of senior staff and lack of guidance and coaching. More incidents will level to a less productive workforce for their regular activities which is resembles by **R31 reduce solving backlog** loop. This loop results into the inclusion of the capability / adaptability trap (Repenning and Sterman 2002,Rahmandad and Repenning 2015) into this sub model.

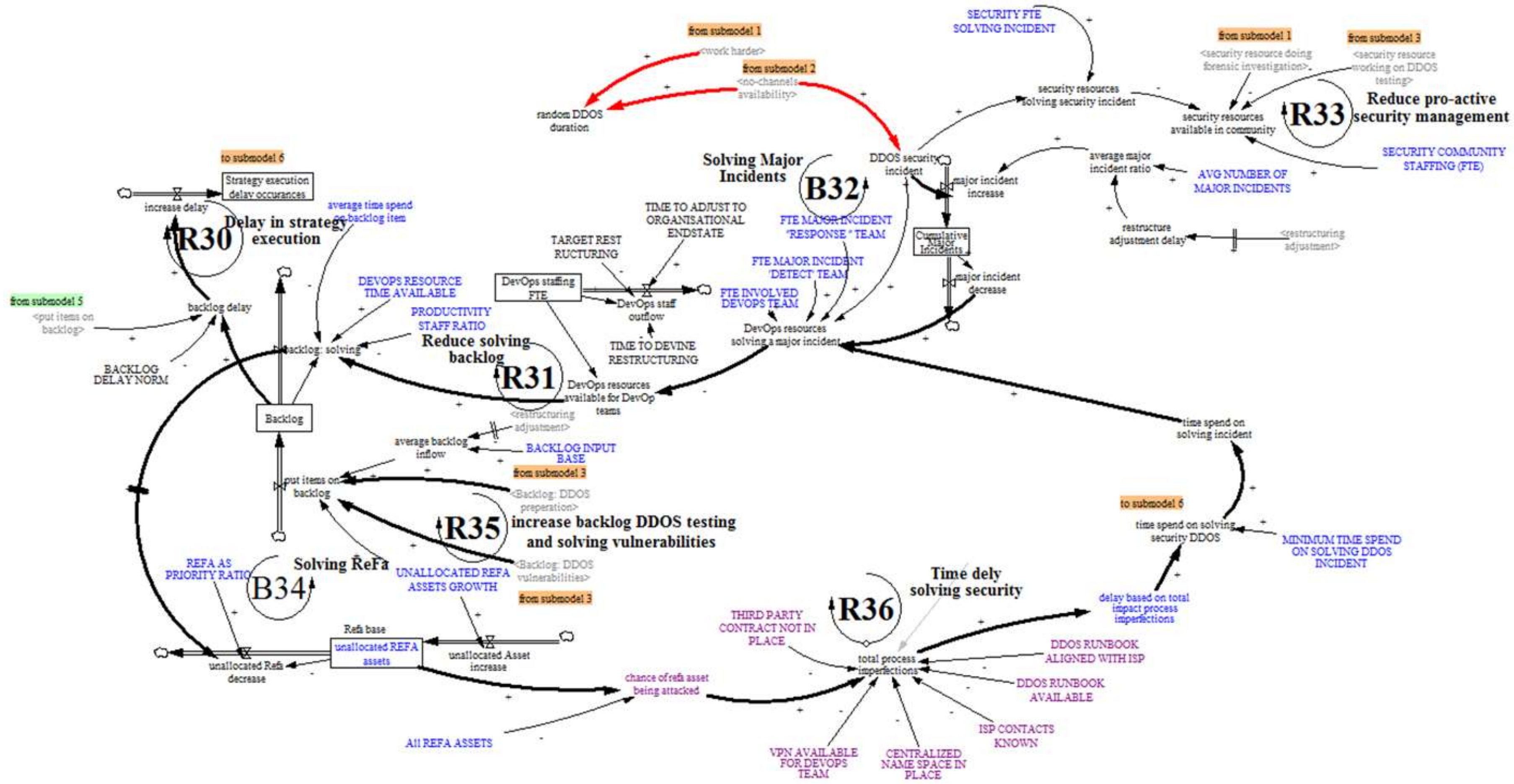
The Agile Manifesto (2001) plead for an agile way of software development. One of these methods is SCRUM because software development was something that could not be planned, estimated and completed successfully by using common methods (Vlaanderen et all 2011). According to Vlaanderen et all (2011) SCRUM addresses flexibility. The only two parts that are fully defined during software development process are the first and last phase (planning and closure). In between. The final product is developed by several teams in series of flexible black boxes called sprints (Vlaanderen et all 2011). At the start of each sprint requirements from a backlog are already specified into tasks and these tasks will be executed during a sprint. Then these tasks meet the defined quality as stated in the definition of done the task is finalized and removed from the backlog. Thus in a development, operations and agile (DevOps) environment activities the tasks to be done are places on a backlog.

These activities will be generated by the organization (autonomous outside the model) as well as delivered from unknown assets that need to be identified, DDOS testing or resolving DDOS vulnerabilities **(R35 increase backlog by DDOS testing and resolve vulnerabilities).** If an activity has been done satisfactory by the specific DevOps team it will be removed from the backlog; including investigating unknown assets (**B35 resolving Refa**) and resolving DDOS vulnerabilities (see sub model 4). Interviews indicate a backlog contains approximately three month of estimated work. When too much staff is solving incidents the backlog will grow since less items can be resolved. If the backlog contains approximately six months of estimated work it is assumed strategy execution will be negatively impacted (**R30 delay in strategy execution**). It was very hard to determine what the impact is of a delay in strategy execution. Based on some interviews is assumed that after 24 months of strategy execution delay a negative financial impact due is expected due to deterioration of organizational focus. However, are realistic response can be that reprioritization of activities will take place in such a case limiting the impact on the organization.

Further to the security staff and major incident response. Across the organization, security staff is positioned working on threat analysis, security testing (including DDOS) , security improvements and providing security related advice. All activities can be considered pro-active security management (Bohme and Moore 2009) . In case of an DDOS attack that requires a response security staff has to respond by solving this security incident and doing forensic research (reactive security management). **R33 reduce pro-active security management** is the reinforcing loop that visualizes the capability / adaptability trap (Repenning and Sterman 2002,Rahmandad and Repenning 2015).

The duration of resolving an DDOS incident depends very largely on the quality of the incident handling process (**R36 time delay solving security incident**). The DDOS reference architecture recognizes for the purpose of efficient DDOS incident handling amongst others the following important processes: the targeted asset or resource is known to the organization, a run book (this is a set of procedures on the day-to-day maintenance and exception handling of an IT system) for handling DDOS incidents is available, this run book has been aligned with the ISP, the ISP contact are known and staff resolving the DDOS incident are able to log on system remotely. SME interviews indicate that imperfect process evoke a delay in solving incidents. When the number of process imperfections increases the time for solving incident is expected to grow exponentially.

Sub model 5: Resilient organization: major incident response



from submodel 1
<work harder>
from submodel 2
<no-channels availability>
random DDOS duration
SECURITY FTE SOLVING INCIDENT
security resources solving security incident
from submodel 1
<security resource doing forensic investigation>
from submodel 3
<security resource working on DDOS testing>
security resources available in community
R33
Reduce pro-active security management
SECURITY COMMUNITY STAFFING (FTE)
average major incident ratio
AVG NUMBER OF MAJOR INCIDENTS
restructure adjustment delay
<restructuring adjustment>
DDOS security incident
major incident increase
Cumulative Major Incidents
major incident decrease
Solving Major Incidents
B32
FTE MAJOR INCIDENT "RESPONSE " TEAM
FTE MAJOR INCIDENT 'DETECT' TEAM
FTE INVOLVED DEVOPS TEAM
DevOps resources solving a major incident
TIME TO ADJUST TO ORGANISATIONAL ENDSTATE
TARGET REST RUCTURING
DevOps staffing FTE
DevOps staff outflow
TIME TO DEVINE RESTRUCTURING
DevOps resources available for DevOp teams
to submodel 6
Strategy execution delay occurances
increase delay
R30
Delay in strategy execution
average time spend on backlog item
from submodel 5
<put items on backlog>
backlog delay
BACKLOG DELAY NORM
DEVOPS RESOURCE TIME AVAILABLE
PRODUCTIVITY STAFF RATIO
backlog: solving
Reduce solving backlog
R31
Backlog
<restructuring adjustment>
average backlog inflow
BACKLOG INPUT BASE
from submodel 3
<Backlog: DDOS preperation>
put items on backlog
R35
increase backlog DDOS testing and solving vulnerabilities
<Backlog: DDOS vulnerabilities>
from submodel 3
REFA AS PRIORITY RATIO
B34
Solving ReFa
UNALLOCATED REFA ASSETS GROWTH
Refa base
unallocated REFA assets
unallocated Asset increase
unallocated Refa decrease
chance of refa asset being attacked
All REFA ASSETS
time spend on solving incident
to submodel 6
time spend on solving security DDOS
MINIMUM TIME SPEND ON SOLVING DDOS INCIDENT
delay based on total impact process imperfections
R36
Time dely solving security
THIRD PARTY CONTRACT NOT IN PLACE
total process imperfections
DDOS RUNBOOK ALIGNED WITH ISP
DDOS RUNBOOK AVAILABLE
ISP CONTACTS KNOWN
CENTRALIZED NAME SPACE IN PLACE
VPN AVAILABLE FOR DEVOPS TEAM

Fig 22. Sub model 5: Resilient Organisation: major incident response

Output model 6: customers perspective

This output model, as stated in Figure 23, is used for calculation the impact of DDOS attacks. Successful DDOS attacks may evoke the following impacts:

- Incidental revenue loss due to non-availability of the service;
- Additional cost due to customer complaints or starting back-up processes;
- Permanent revenue loss due to abnormal customer churn.

In case of a successful DDOS attack electronic services will temporary not be available. This impact might be reduced by having alternative channels and specific customer communications in place. In case different services or channels are available on different infrastructure the services can be differently delivered to the customers. If organizations have a proper communication strategy in place customers usually accept a limited delay in service delivery (Bitner et al 1990). Additional communications evoked by DDOS attacks can usually be absorbed from regular communication budgets. Therefore these costs are not considered in the model.

Additional costs can also be evoked due to a longer DDOS attack duration. After a certain time period customer might complain about service levels. Additional staff (especially in the call center and operations) might be needed to handle customer complaints and questions. In addition customer services need to be restored. If the DDOS attack has not been resolved customers' transactions should be processed through alternative processing methods provided by the back-up and recovery strategy of the organization. All these activities can result into a higher workload for the staff. For a short period staff can handle higher workload through overtime and work harder. For a longer period additional staffing is needed.

There is little research available on cyber security events and customer abnormal churn behavior. Kwon and Johnson (2015) showed that (in the healthcare sector) customer retention will be impacted if medium sized organization suffer multiple breaches in a three year period. Customers leave because they do not trust that the organization can safeguard their valuable assets. So successful DDOS attacks will result into a customer trust decline **(R38 loose customer trust)** and avoiding multiple DDOS attacks will result into bringing back the customer trust to a normal state **(B37 gain customer trust)**. In case of restoring trust a four to six times more effort is needed (Schweitzer et al 2006). The relation between data breaches and impact can be considered non-linear (Edwards et al 2016, Verizon 2015, Net Diligence 2014). If certain thresholds in the customer trust dynamics have been met there will be an customer abnormal churn impact.

For successful and unsuccessful DDOS attacks almost the same calculation mechanisms are used. In case of calculating the damage avoided (= impact of unsuccessful DDOS attack) the impact of the **R39 loose customer trust** and **B38 gain customer trust** loop cannot be used.

Output model 7: financial perspective

This output model, shown in Figure 24, is used for calculating the cost related to DDOS defenses based upon underlying contracts. Web application firewalls, DDOS testing, forensic support and DDOS defense at location have a simple structure based upon volume * price. DDOS defense at ISP and DDOS defense in the cloud have a different behavior.

DDOS defense at ISP level have two cost structures:

1) The organization pays a low fee for being connected to a minimum level of ISP defense. Based on the usage of this defense the organization has to pay the ISP either for an additional usage at a flexible rate or increase the minimum level for defense subscription.
2) The organization pays a moderate fee for the using the full level of ISP defense at given moment in time. When the ISP does not deliver the organization will receive a contract discount related to the non-delivery.

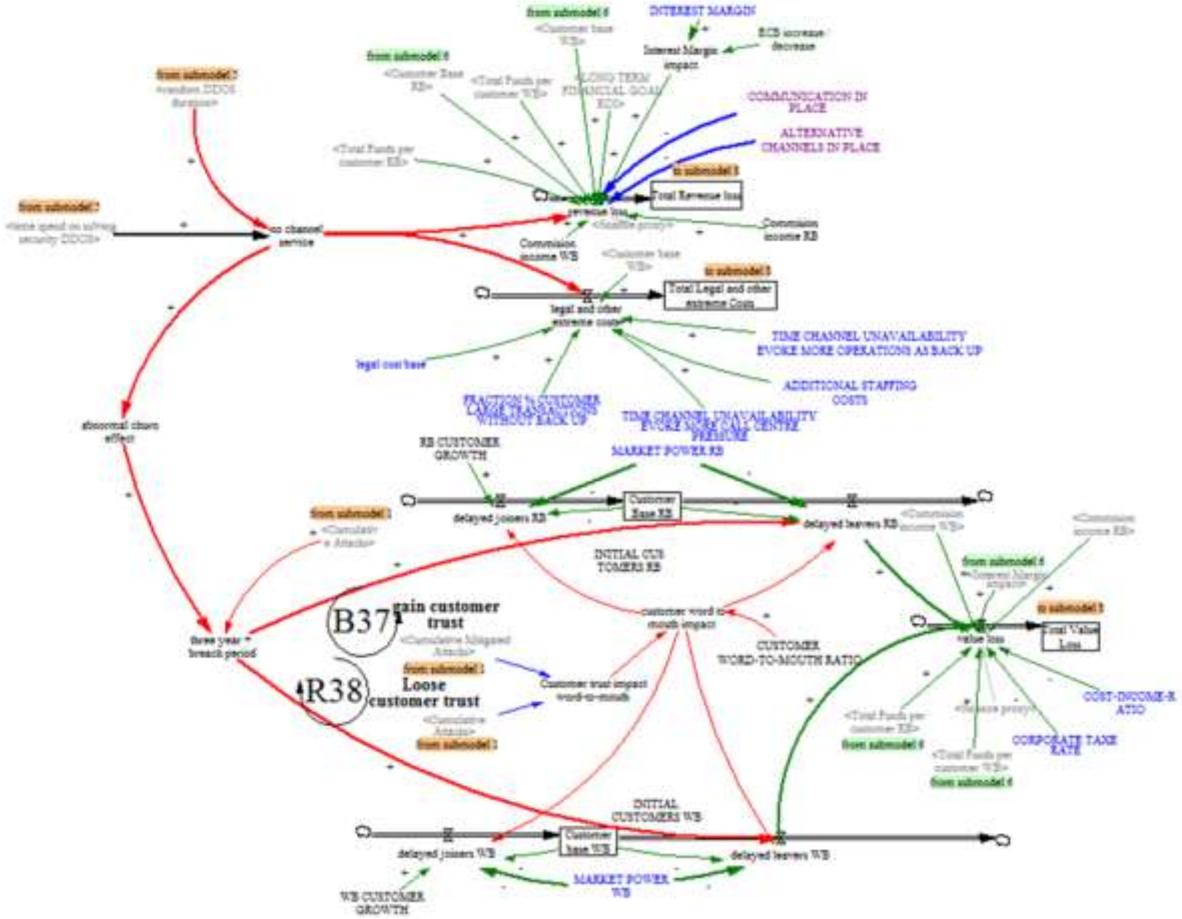


Fig 23. Output model 6: Customers' perspective

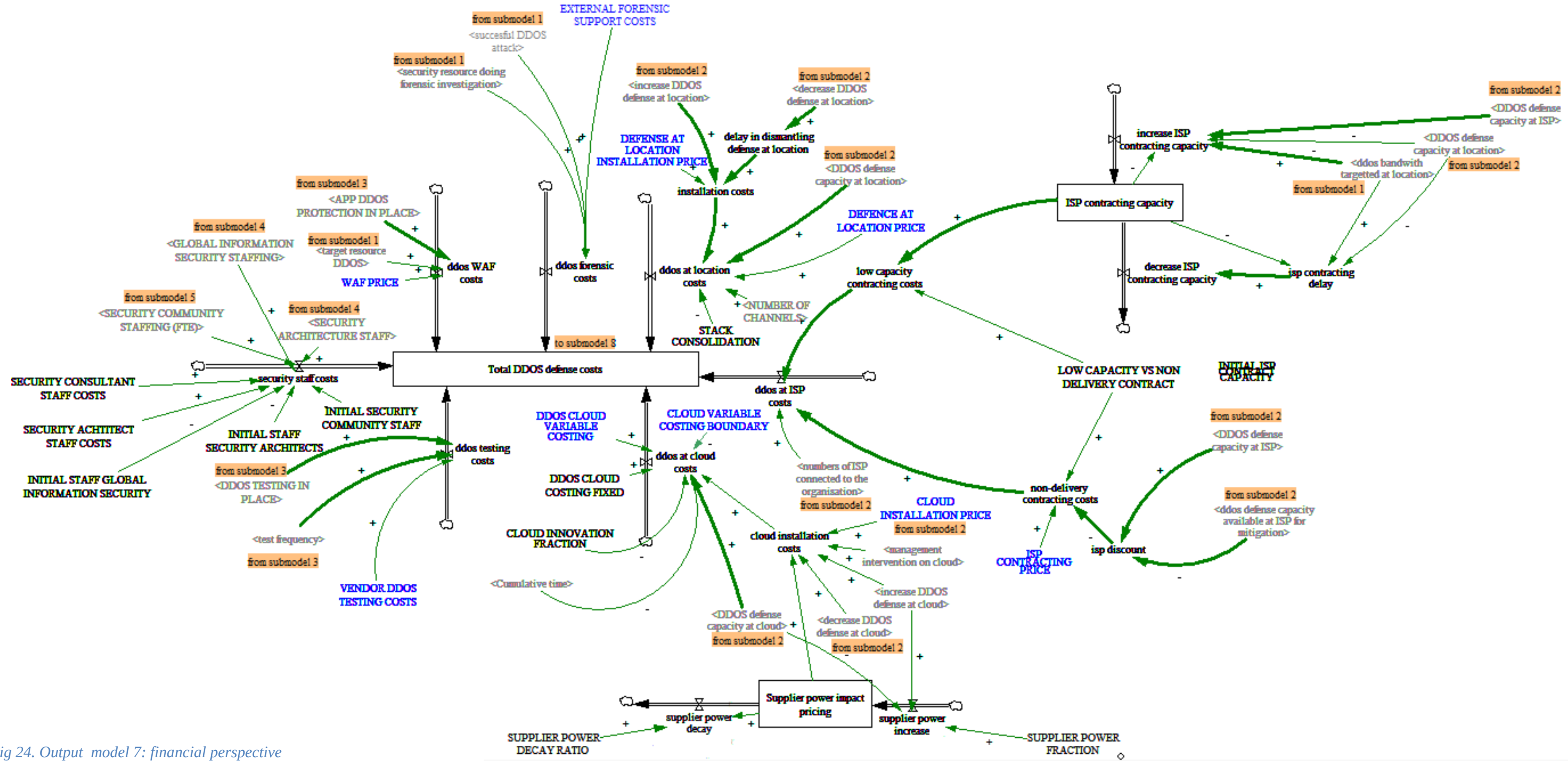

EXTERNAL FORENSIC SUPPORT COSTS
from submodel 1
<succesful DDOS attack>
from submodel 1
<security resource doing forensic investigation>
from submodel 2
<increase DDOS defense at location>
from submodel 2
<decrease DDOS defense at location>
DEFENSE AT LOCATION INSTALLATION PRICE
delay in dismantling defense at location
installation costs
from submodel 2
<DDOS defense capacity at location>
DEFENCE AT LOCATION PRICE
from submodel 3
<APP DDOS PROTECTION IN PLACE>
from submodel 4
<GLOBAL INFORMATION SECURITY STAFFING>
from submodel 1
<target resource DDOS>
WAF PRICE
ddos WAF costs
ddos forensic costs
ddos at location costs
<NUMBER OF CHANNELS>
STACK CONSOLIDATION
from submodel 5
<SECURITY COMMUNITY STAFFING (FTE)>
from submodel 4
<SECURITY ARCHITECTURE STAFF>
to submodel 8
Total DDOS defense costs
security staff costs
SECURITY CONSULTANT STAFF COSTS
SECURITY ACHITTECT STAFF COSTS
INITIAL STAFF GLOBAL INFORMATION SECURITY
INITIAL STAFF SECURITY ARCHITECTS
INITIAL SECURITY COMMUNITY STAFF
from submodel 3
<DDOS TESTING IN PLACE>
ddos testing costs
<test frequency>
from submodel 3
VENDOR DDOS TESTING COSTS
DDOS CLOUD VARIABLE COSTING
DDOS CLOUD COSTING FIXED
CLOUD INNOVATION FRACTION
<Cumulative time>
CLOUD VARIABLE COSTING BOUNDARY
ddos at cloud costs
ddos at ISP costs
<numbers of ISP connected to the organisation>
from submodel 2
cloud installation costs
CLOUD INSTALLATION PRICE
from submodel 2
<management intervention on cloud>
<increase DDOS defense at cloud>
<decrease DDOS defense at cloud>
from submodel 2
<DDOS defense capacity at cloud>
from submodel 2
Supplier power impact pricing
supplier power decay
supplier power increase
SUPPLIER POWER DECAY RATIO
SUPPLIER POWER FRACTION
low capacity contracting costs
ISP contracting capacity
increase ISP contracting capacity
decrease ISP contracting capacity
isp contracting delay
from submodel 2
<DDOS defense capacity at ISP>
<DDOS defense capacity at location>
<ddos bandwith targetted at location>
from submodel 2
from submodel 1
LOW CAPACITY VS NON DELIVERY CONTRACT
INITIAL ISP CONTRACT CAPACITY
from submodel 2
<DDOS defense capacity at ISP>
non-delivery contracting costs
ISP CONTRACTING PRICE
isp discount
from submodel 2
<ddos defense capacity available at ISP for mitigation>

Fig 24. Output model 7: financial perspective

DDOS defense in the cloud have high costs for the installation of decommissioning of this capability. The cost of the cloud service depends on the capacity of the cloud provider. SME interview indicate that long term cloud cost are considered to be flat. The increase in GBPS of the cloud defense will approximately be offset by a decrease in the average price per GBPS. This price decrease can be explained by technical innovations and economies of scale. Implementing cloud defenses directly after successful attack evoke very high cloud defense cost in the first year because the cloud provider has a lot of purchasing power at that time.

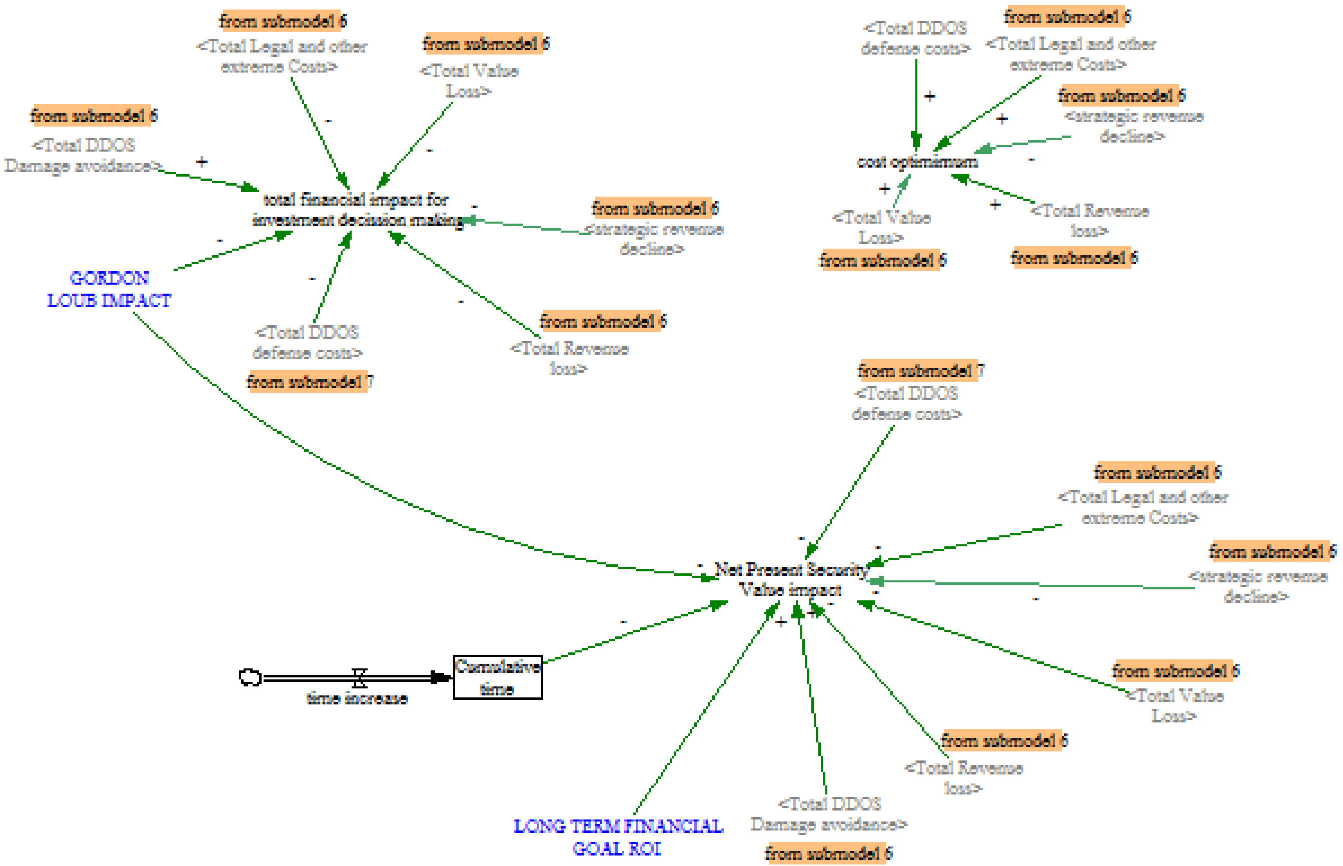

from submodel 6
<Total Legal and other extreme Costs>
from submodel 6
<Total Value Loss>
from submodel 6
<Total DDOS Damage avoidance>
total financial impact for investment decision making
from submodel 6
<strategic revenue decline>
GORDON LOUB IMPACT
<Total DDOS defense costs>
from submodel 7
from submodel 6
<Total Revenue loss>
<Total DDOS defense costs>
from submodel 6
<Total Legal and other extreme Costs>
from submodel 6
<strategic revenue decline>
cost optimimum
<Total Value Loss>
from submodel 6
<Total Revenue loss>
from submodel 6
from submodel 7
<Total DDOS defense costs>
from submodel 6
<Total Legal and other extreme Costs>
from submodel 6
<strategic revenue decline>
Net Present Security Value impact
Cumulative time
time increase
from submodel 6
<Total Value Loss>
from submodel 6
<Total Revenue loss>
<Total DDOS Damage avoidance>
from submodel 6
LONG TERM FINANCIAL GOAL ROI

Fig 25. Output model 8: Financial evaluation

Output model 8: financial perspective

Various evaluation metrics are visible in Figure 24 and explained below.

Zeijlemaker (2016) indicated that from a financial perspective senior security management can take the decision to either spend money on cyber-attack related damages of corresponding cost for the capabilities that defend against these attacks. This is in line with financial management practice where cash flows will be considered for investment decision taking (Dorsman 2003). This decision opportunity is calculated in the cost optimum metrics. This metrics should be as low as possible.

Other metrics for evaluating security investment decision evaluation use the benefits of the investments (less direct cost, less indirect cost and less benefits for cyber criminals since the organisation has been protected against certain attacks) compared to the cost of the security investments (Anderson et al. 2013, Brecht and Norway 2013). From a systems thinking perspective and security economics perspective investments in security defences have the purpose of lowering the number of expected attacks and/or the expected damage per attack. Therefore, the expected impact of both successful and unsuccessful attacks as well as the investment in the defences should be considered. The model has also an evaluation metrics taking into account the benefits (damage avoided) of unsuccessful attacks off-set by the actuals costs of the defences in place and successful attacks. In line with Gordon and Loeb (2003) the benefits of the unsuccessful attacks are considered for a limited percentage of the total amount. Investments in security capabilities have an optimum. This is calculated in the metric total financial impact of investment decision making.

In case of considering the time value of money the net present value of this last metric is calculated taking into account the long term financial RIO of the organisation. From a company perspective management can either spent money on security or spent money on income generating and innovative activities or pay the cash to shareholders as dividend. Therefor the cost of capital should be considered as well.

A problem with considering both “attacks that will be avoided” and “attacks that will affect the organisation” in a metrics is that measures for lowering the impact of damage might have a negative influence on this ratio. Therefore multiple metrics, as shown in Figure 25, should be considered.

Metrics	Best outcome	Considered elements
Cost optimum	As low as possible	Cost of successful DDOS attacks and DDOS defences
Total financial impact of investment decision taking	As high as possible	Cost of (un)successful attacks and DDOS defence
Net present security value	As high as possible	See above and take time value of money from company perspective into account

Fig 25. Overview of different financial evaluation metrics

Appendix 2: Model validation

Forrester and Senge (1979), Barlas (1996) and Sterman (2000) have described various tests for model testing and validation as stated in Figure 27. The DDOS model is tested and validated in line with these activities. This will be explained here after.

Test	Barlas 1994	Barlas 1996	Sterman 2000	Forrester, Senge 1979
Direct Structure Test	**x**	**x**	**x**	**x**
Empirical tests				
structure verification test / assessment	x	x	x	x
parameter verification test / assessment	x	x	x	x
integration error			x	
Theoretical tests				
structure verification test / assessment	x	x	x	x
parameter verification test / assessment	x	x	x	x
direct extreme condition test	x	x	x	x
dimensional consistency test	x	x	x	x
implementation methods				
formal inspections / review		x		
walkthrough		x		
semantic analysis		x		
Structure oriented Behaviour test	**x**	**x**	**x**	**x**
extreme condition test	x	x	x	x
behaviour sensitivity test	x	x	x	x
- behaviour anomaly test			x	x
- family behaviour test			x	x
- suprise behaviour test			x	x
modified behaviour (prediction) test / behaviour reproduction	x	x	x	x
boundary adequacy test	x	x	x	x
phase relation test		x		
qualitative feature analysis		x		
turing test		x		
Behaviour Pattern test	**x**	**x**	**x**	**x**
system improvement			x	x
changed behaviour prediction test				x
boundary adequacy policy test				x
policy sensitivity test				x

Fig 27. Model validation test compared from different papers

Firstly, the direct structure test will be explained. The structure of this model has been based on approximately 30 interviews, the DDOS reference architecture and policy settings. Interviews were held for acquiring information as well as walking through the model and reviewing the model. The level of aggregation of the model is comparable with the DDOS reference architecture and internal reporting on DDOS resilience and presented literature in the first section of this paper. The dimensional consistency has been tested the “unit check” test and model performance by the “check model” test in the software package used for modelling. Parameters in the models are based upon internal data sources, supplier data sources, scientific papers of interviews as specified in appendix 3. The model has been subjected to extreme condition analysis and anomaly behavior and the model has been adjusted accordingly. For this analysis approximately 20,000 different scenarios have been analyzed by using the “synthesis” option in the model software.

Next various structure oriented behavior tests will be explained. Different part of the model has been compared with actual data and other tests that is explained further below per sub model.

Sub model 1: attackers perspective: DDOS attack.

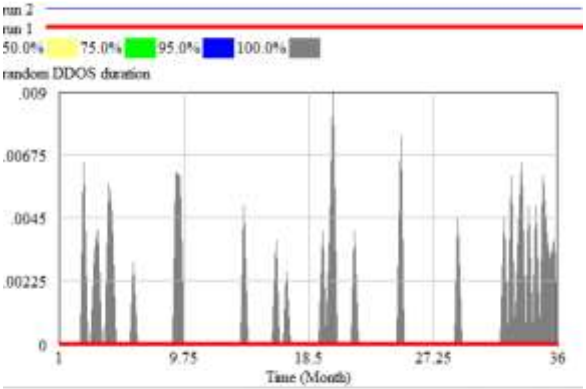


Fig 28. Sensitivity analysis on DDOS attack durations in months

The validation test result of sub model 1 are related to duration of DDOS attacks, size of bandwidth DDOS attacks at location, cumulative mitigated and non-mitigated attacks, Targeted DDOS attacks, DDOS innovation and probability of DDOS attack.

The DDOS attack duration is between several seconds to hours (Imperva Incapsula 2014 and 2015, Atlas 2014 and 2015). Kovacs (2012) indicated that the longest DDOS attack had a duration of 80 days. Based Quora (2016) and Imperva Incapsula (2015) an average duration of approx. 10 minutes is acceptable. From a business perspective, the period between 7:30 – 24:00 is most relevant due to customer activities. Figure 28 presents the model sensitivity analysis for duration of DDOS attacks over time and it is in line with these observations. The longest attack duration of 0.09 corresponds with a duration of approximately 4.5 hours.

These DDOS protection suppliers suggested that in any given year there were about nineteen 100 GBPS DDOS attacks globally (relevant trend is the lowest red line in Figure 29). It should be noted that observed DDOS attacks strongly depends on positioning of DDOS protection equipment. Based on internal data, one DDOS attack of 320 GPBS has been observed (relevant trend related to highest red line in Figure 16). Sensitivity analysis demonstrate that model output shows acceptable behavior since most model behavior are below these thresholds.

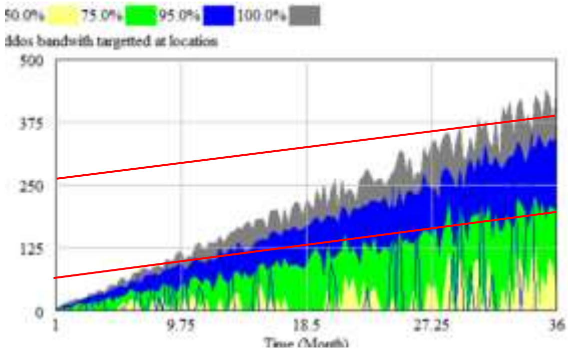


Fig. 29 Sensitivity analysis on magnitude of DDOS attack (GBPS)

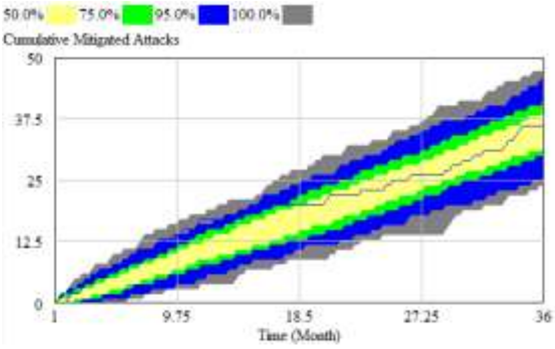


Fig 30. Sensitivity analysis on cumulative number of mitigated DDOS attacks

Internal data analysis based on questionnaires indicate that on average one DDOS attack per month was observed. The model output in Figure 30 (sensitivity analysis) pointed out that, over 3 year period, the number of attacks were between 48 and 25 with an average on 36. During these period of 36 months, no successful DDOS attacks were observed. SME interview indicated that an acceptable level between 0 and 2 successful DDOS attacks is an acceptable outcome. Based on sensitivity analysis the model reflect this outcome in Figure 31.

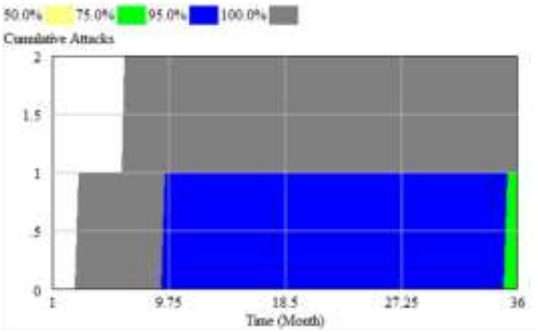


Fig 31. Sensitivity analysis on cumulative number of successful DDOS attacks

Regarding relevant available data on this matter concerns the start of 1996 until the end of 2013, yet average behavior differs from model behavior. The evaluated model has relevant period of 36 months as from the early 2013. However in the available data it was hard to address four types of known attack in a specific time frame.

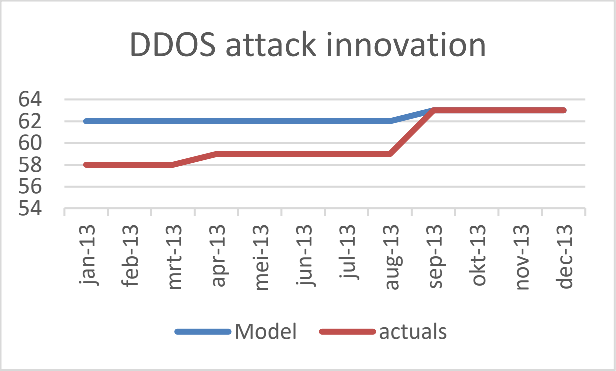


Fig 32. Comparison of model output and actual output in the development of different forms of DDOS attacks

Figure 32 contains the lowest possible outcome of reality compared to the model. Thus the actuals are lacking those four attack forms. Because of the difficulty with allocation four specific attacks forms over time, the small difference between model behavior and actual behavior, and the very low number of targeted DDOS attacks, the model outcome is considered to be at an acceptable close level to reality.

Based on various SME interviews the probability of being attacked in the field of cyber security is a non-linear property which can amongst others be explained by being successful on past attack, word-of-mouth amongst hacker communities, a perception that the targeted organization is vulnerable, looking for other targets after an unsuccessful attempt, government intervention and so on. This behavior is visible in Figure 33. This behavior is comparable with DDOS for bitcoins behavior (DD4BC) in Figure 34 (Akamai 2015). However there are some differences because DD4BC has a global perspective and this model is scoped on one organization. Therefore DD4BC will fluctuate less and the Figures have some different time perspectives. In case of DD4BC an successful attack on another organization is still successful, while from a single organization perspective the attacker choose to attack another organization which result into a decline of the attack behavior.

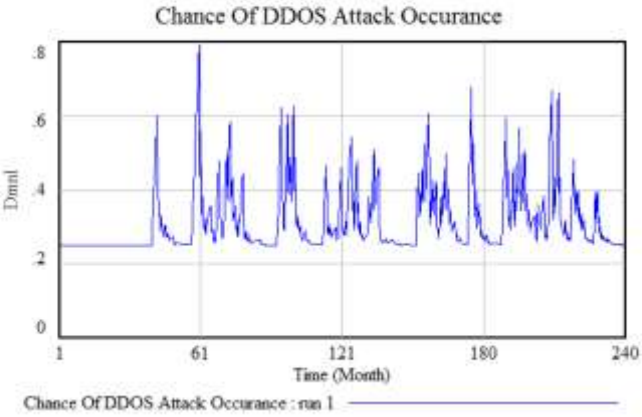


Fig 33. Chance of DDOS attack over time as included in the model

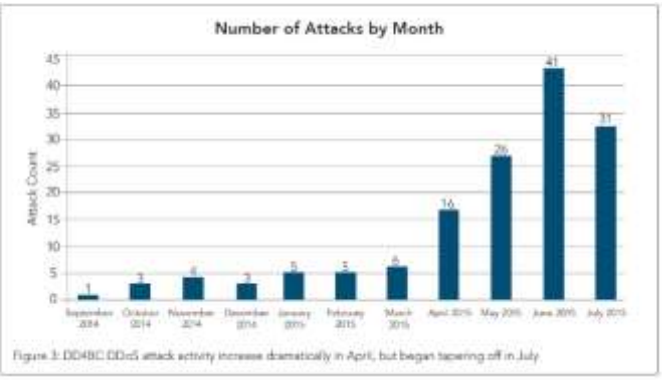


Fig 34. DD4BC frequency table (Akamai 2015)

Sub model 2: defenders perspective: Bandwidth attack

The validation test for sub model 2 is related to DDOS defense capacity at location, at ISP and in the cloud. For the first 36 months in the model the DDOS defenses at location, at ISP and in the cloud have not changed. In Figure 35 the model acts with reality since DDOS defense capacity has not changed during that period.

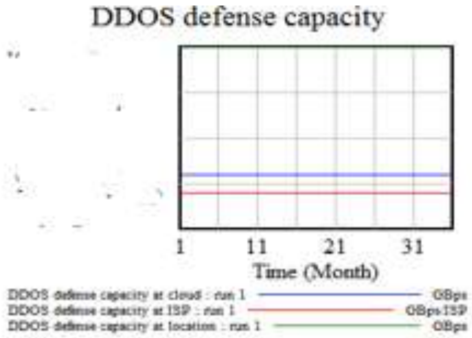


Fig 35. DDOS defence capacity (GBPS) over time

Sub model 3: defenders perspective: targeted resource attack

The validation tests for sub model 3 are related to DDOS testing and resolving DDOS test findings.

The organization issues every 3 months a DDOS test. These tests result into findings about vulnerabilities that can be exploited by targeted DDOS attacks. Sensitivity analysis in Figure 36 suggests that the model behaves with reality (min. findings = 0, max. findings = 31, average findings =6 and standard deviation of findings = 8,2). Given the spread of the data fixed average values have not been used in the model.

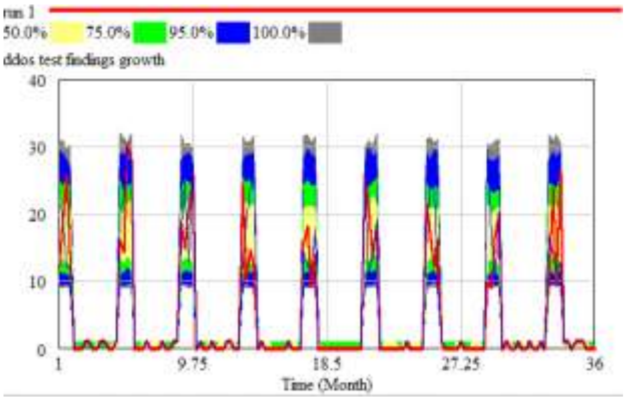


Fig 36. Sensitivity analysis on DDOS testing findings per test

Sensitivity analysis in Figure 37 demonstrates that monthly solved DDOS test findings is also in line with reality (min. findings resolved = 1, max. findings resolved = 15, average findings resolved = 4 and standard deviation of resolved findings is 5.2). On monthly basis test findings will be resolved.

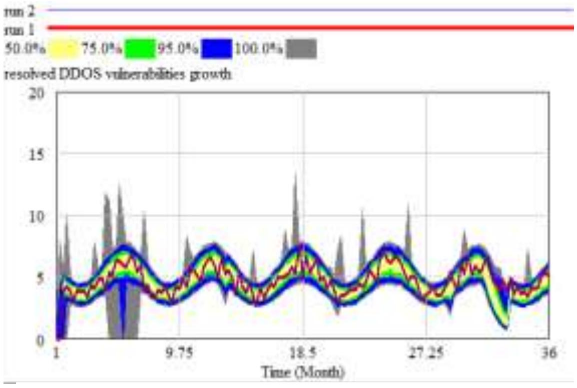


Fig 37. Sensitivity analysis on DDOS vulnerabilities resolved per period

Sub model 4: the resilient organization: threat intelligence

The validation of sub model 4 is related to upgrades of DDOS defense mechanism, because threat intelligence analyses result into upgrade of these defenses, if needed.

There is no architectural adjustment visible in Figure 38. This is in line with actual behavior because at the end of this period the DDOS reference architecture has been updated.

Sub model 5: the resilient organisation: major incident response

The validation tests of sub model 5 are related to major incident development, backlog development and related non-linear behavior.

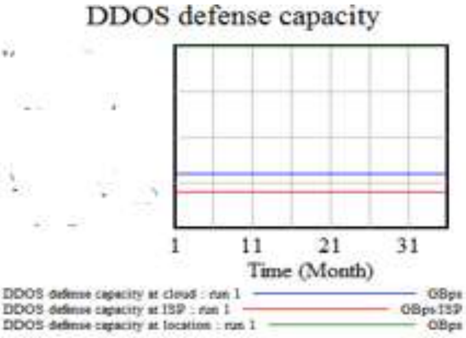


Fig 38. Model output on DDOS Reference Architecture upgrades

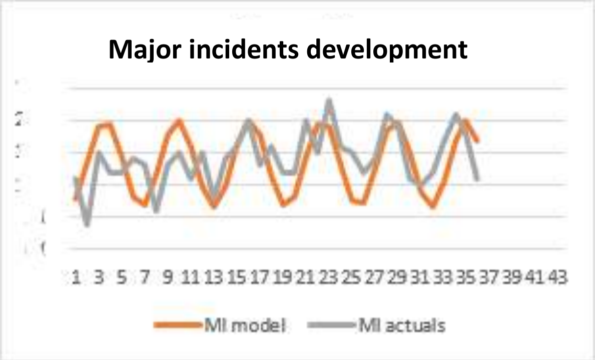


Fig 39. Model comparison with actuals on number of major incidents over time

The number of major incidents included in the model and the number of major incidents actually occurred are more or less in line with each other as stated in Figure 39.

During the 36 months as reference period a scrum agile way of working was implemented. Also a supportive tool for managing the DevOp team’s activities was rolled - out in that period. This roll-out took place during this 36 months period. This roll-out was not part of this model. For the model analysis I have added additional 5 months of data to ensure full roll-out actual information can be compared with the model. As stated in Figure 40 the last 5 months of the model are in line with the actuals behavior of the roll-out tool.

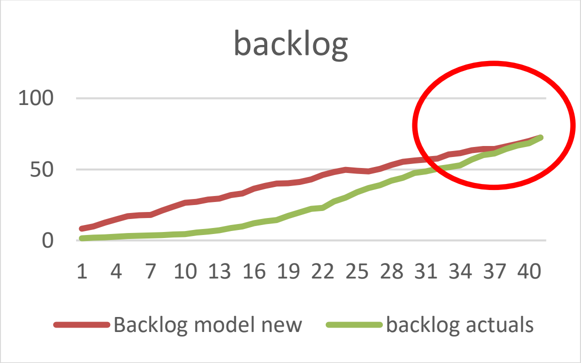


Fig 40. Model comparison with actuals on backlog items

After some model adjustments the inflow and outflow of items on the backlog were in line with actual Figures in the last 5 months. Below are tables (Figure 41 and 42) with Inflow respectively outflow behavior

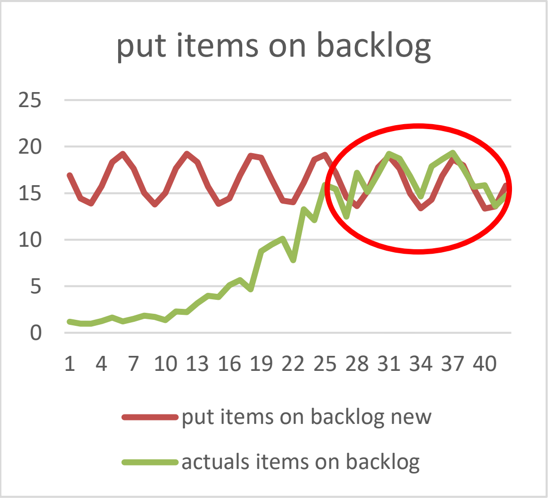
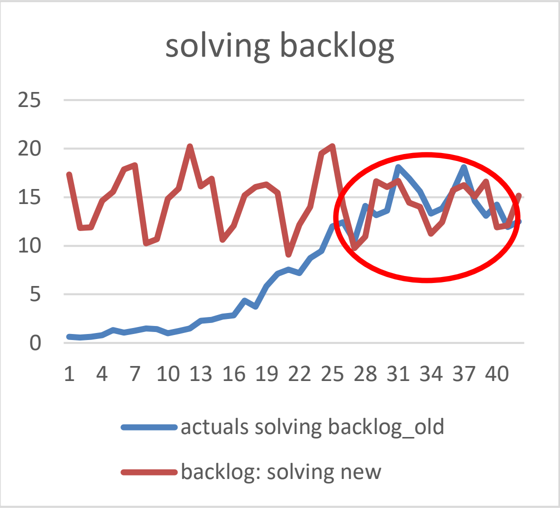


Fig 41. Model comparison with actuals on items put on backlog



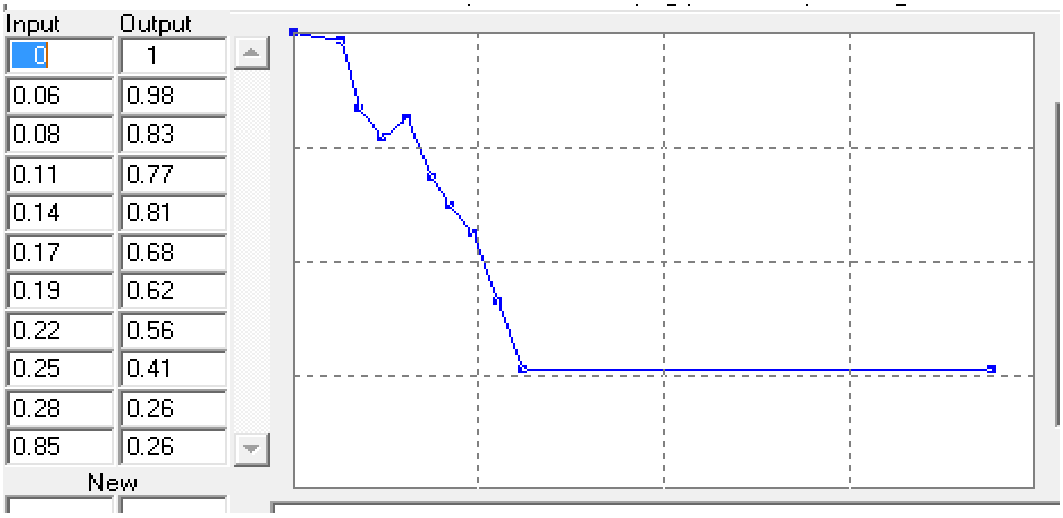
42. Model comparison with actuals on solving backlog items

At operational level of the organization there are various small DevOps teams that have between 8 and 12 staff members. These teams are a mixture between junior, mediocre, senior staff as well as a scrum master. The scrum master will solve issues that the team cannot resolve by its own or where solutions depend on other teams. In this way the DevOps team member can focus on their day-to-day activities. Some senior staff members have based on their experience and knowledge a role in the major incident process. If the organization faces a major incident they stop their regular day-to-day activities and are going to solve this major incidents. At the start of such an incident a lot of senior staff members are involved with detecting the cause of the major incident (root-cause-analysis). If the cause of the major incident is known the number of senior staff members will be reduced. A dedicated staff will continue to resolve this major incident.

The absence of this senior staff member in the DevOp team results into a less productive DevOps team because:

- The senior staff members, one of the most productive type of staff members, is occupied with major incident activities
- The senior staff member cannot provide guidance and coaching to the junior and mediocre staff members during the process of solving a major incident
- The major incident process stops when the incident has been solved. Hold the line policy indicate that the major incident should be resolved as soon as possible. This might lead to working harder, overtime and making longer working days. Staff involved in major incidents will not be directly and fully productive back in the team due to recovery and collective labor agreements.
- If a major incident solving time takes too long a second shift with senior staff usually from the same team will be needed.

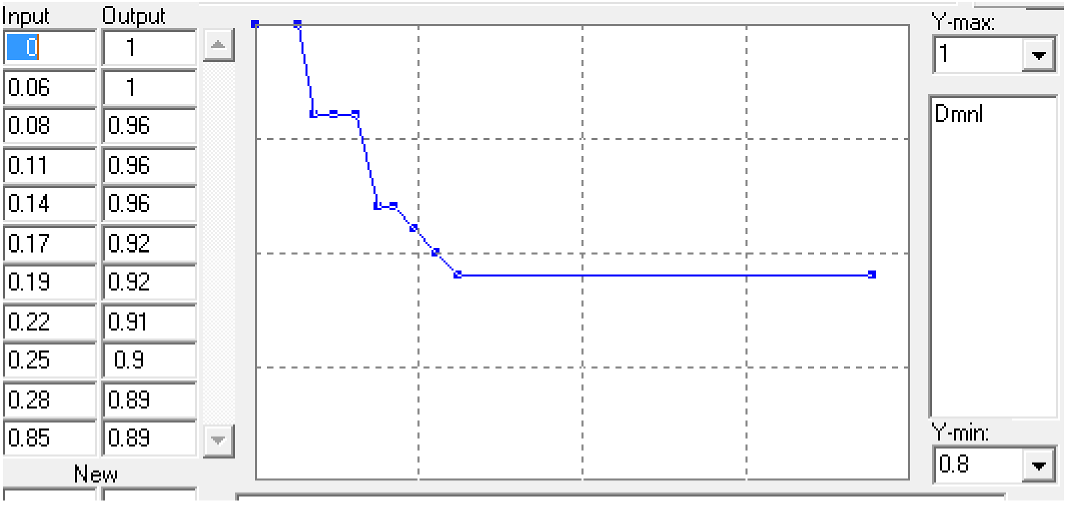
Loss of team production due to lack of senior staff over time is based on organizational insights. The Figure below indicate the loss of DevOps team productivity because senior staff will focus on solving mayor incidents over time. This productivity is lost because senior can neither do their regular DevOps activities nor coach junior staff. The maximum productivity loss is 74%



Input	Output
0	1
0.06	0.98
0.08	0.83
0.11	0.77
0.14	0.81
0.17	0.68
0.19	0.62
0.22	0.56
0.25	0.41
0.28	0.26
0.85	0.26

Fig 43. Model programmed behaviour: duration of major incident handling versus team productivity loss due to senior staff not available to team

The productivity loss due to making overtime while solving major incident has been based on Pencavel (2014). He did research on productivity of working hours. The Figure below indicate that productivity will be lower if the day will be longer. The maximum productivity loss is 11%



Input	Output
0	1
0.06	1
0.08	0.96
0.11	0.96
0.14	0.96
0.17	0.92
0.19	0.92
0.22	0.91
0.25	0.9
0.28	0.89
0.85	0.89

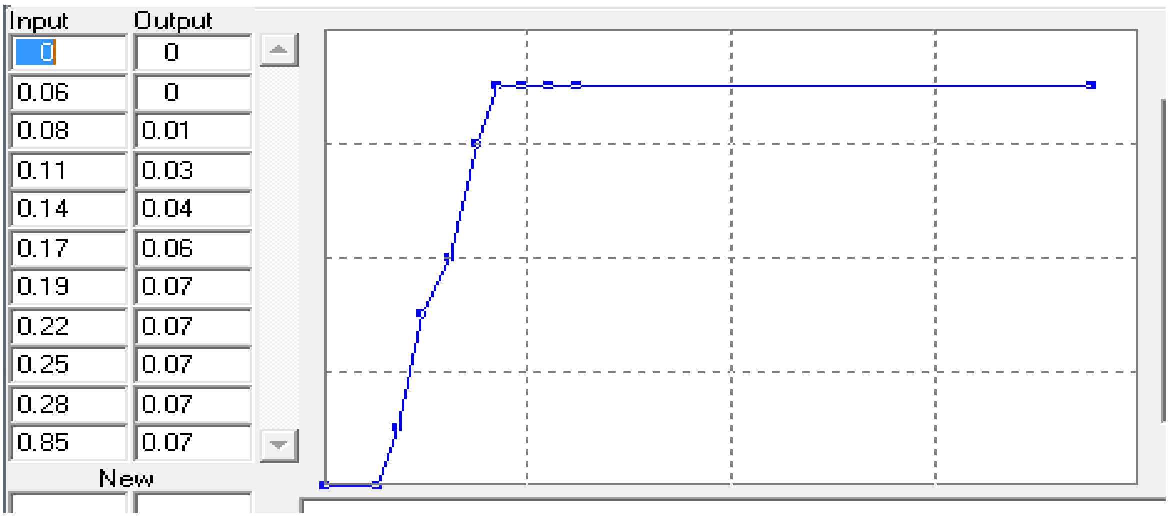
Y-max: 1

Dmnl

Y-min: 0.8

Fig 44. Model programmed behaviour: duration of major incident handling versus team productivity loss due to senior staff making overtime

Productivity loss since senior staff will be compensated for overtime is based on collective labor agreement. Collective labor agreements indicate that overtime outside regular office ours will be compensated extra. In practice usually compensation policy time for time is in please resulting less DevOps activities. The maximum productivity loss is 7%.



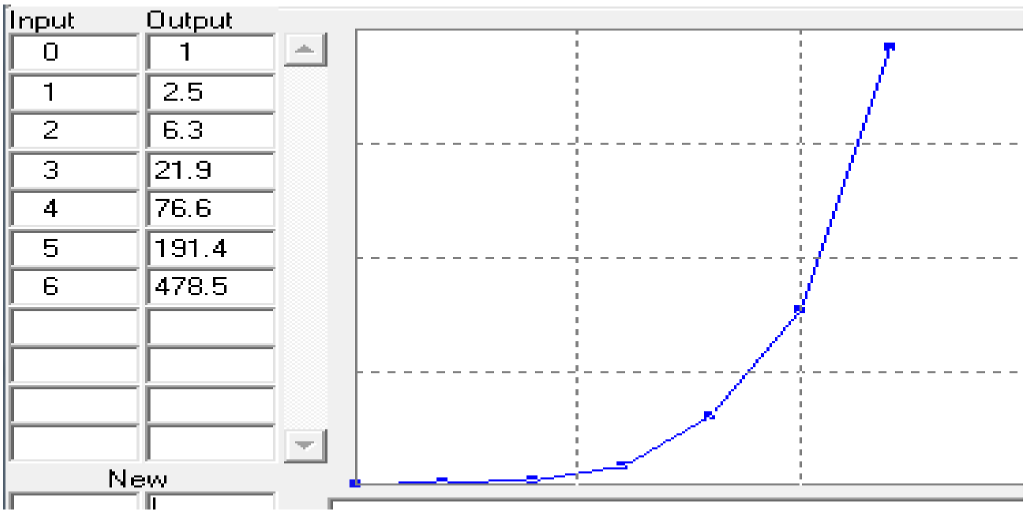
Input	Output
0	0
0.06	0
0.08	0.01
0.11	0.03
0.14	0.04
0.17	0.06
0.19	0.07
0.22	0.07
0.25	0.07
0.28	0.07
0.85	0.07

Fig 45. Model programmed behaviour: duration of major incident handling versus team productivity loss due to senior staff not available due to collective labour agreement time compensation

The time needed to resolve a successful DDOS attack depends on the quality of the response process. SME interviews, real DDOS mitigation cases analysis and policy settings indicated a non-linear behavior. Important proces implicaties are:

- Is the (group of) targeted asset(s) by the DDOS attack known to the responding organization? If the asset(s) are not known the response team has to search for them.
- Are the different participants and their run books in the value chain known? In case of outsourcing the supplier might need to take certain mitigation actions. In some defense tactics the ISP (internet service provider) need to take certain mitigation actions. If these participants are not known or their way of working is not known additional time is needed to Figure this out. In addition they need to align their way of working.
- Does the response team has separate Virtual Private Network (VPN) connections available? Separate VPN networks are independent of the area under attack by the DDOS and dedicated for the response team. Instead of travelling to an office building or war room they can work online.
- Is central name space in used? A central repository of all used naming conventions lowers the search efforts to webpages under attacks and ensures completeness of the webpages that require mitigation efforts.

The Figure at the right indicate the additional time needed for resolving incident compared to the number of process erros. Maximum process errors is 6.



Input	Output
0	1
1	2.5
2	6.3
3	21.9
4	76.6
5	191.4
6	478.5

Fig 46. Model programmed behaviour: number of process imperfections related to additional time needed to resolve the major security incident related to DDOS

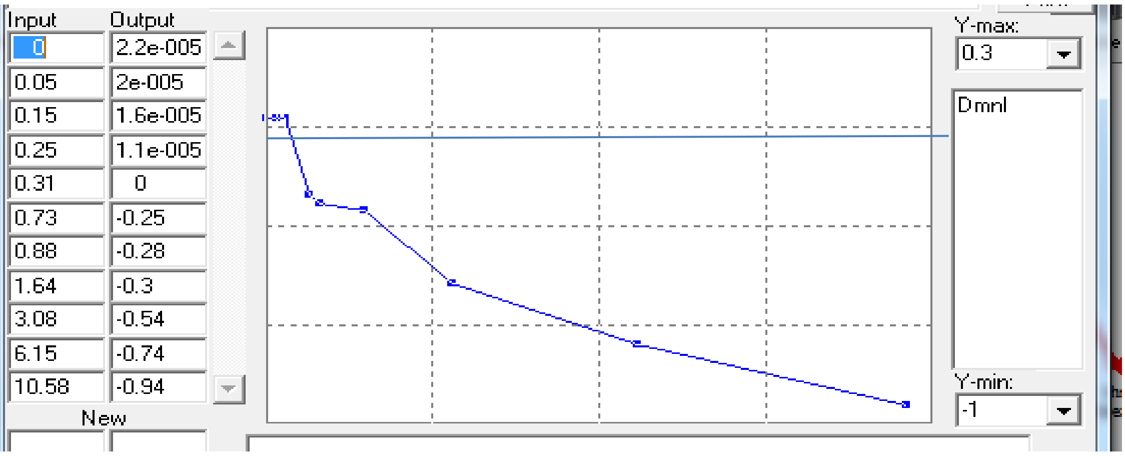
Output model 6: customers impact

Output about customer impact is new, especially, in the area of customer trust in relation to cyber security. Therefore this newly constructed insight cannot be validated by actual datasets. Only by SME interviews which are used for model building and validating the behaviour. Input for this part has been used from internal systems and SME interviews.

SME interview indicated there is a relation between the customer base of an organization and its resilience towards security. However limited insight where available on how to model this behaviour. Various research papers provided components relevant to this matter:

- Kwon and Johnson (2015) indicated that data breach have no impact on start-ups or market leaders and customer abnormal churn impact is visible after multiple breaches and 3 years;
- According to Schweitzer et al (2006) efforts to restore trust were 4 - 6 time higher than losing it;
- Ponemon Institute (2012 - 2015) have had some insight on abnormal churn evoked by data breaches;
- Contrary to Ponemon, Net Diligence (2013 - 2014) and Verizon (2015) have indicated logarithmic scale is relevant for economizing the impact of cyber-attacks;
- Lee and Lee (2010) argued that information security incidents are likely to trigger reactive behaviour such as avoiding online store, switching to other online stores and using offline stores. There the targeted firm should take counter measures to maintain customer trust. Lee and Lee also indicated that phishing and spam seems to have a strong positive effect on perceived damage compared to others; and therefore impact customer decision making.

- Kim et al (2009) believed that firm technical solution and security statements contribute through customer perceived security to security trust



Input	Output
0	2.2e-005
0.05	2e-005
0.15	1.6e-005
0.25	1.1e-005
0.31	0
0.73	-0.25
0.88	-0.28
1.64	-0.3
3.08	-0.54
6.15	-0.74
10.58	-0.94

Fig 47. Model programmed behaviour: ratio successful attacks / unsuccessful attacks impacts customer trust

Based on these components one could argue that between successful cyber-attacks and mitigated attacks there is a non-linear relation with customer trust and through trust with delayed customer outflow. This non-linear behaviour has been observed and validated to SME interview.

This non-liniear behaviour will be explained further. if the unsuccessful and successful attacks reach a certain threshold customer trust starts to decline which over time might eventually affect customer in- and outflow. A very small number of successful attacks will result into customer increase because customers know that the defender is going to protect the organization against future attacks. This relation is visible in the Figure 47.

The yellow markers in the Figure 48 indicate that the change in the ratio successful (green line) and not successful DDOS attacks (grey line) result into a decline of customer trust (blue line). Approx. three year later the number of customers start to decline (red line). This behaviour is more or less in line with previous mentioned research.

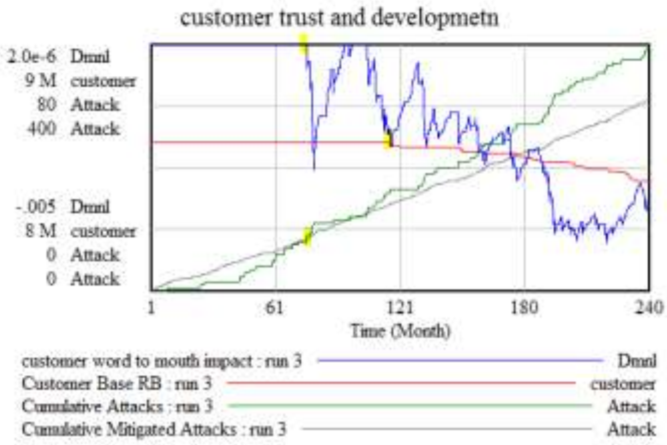


Fig 48. Model output: relation unfavourable successful attacks / unsuccessful attacks ratio impact customer trust and results into delayed customer Retail Banking (RB) outflow

Output model 7: financial impact & output model 8: financial evaluation

Validation tests are related to various financial metrics, DDOS cloud cost and detection trap behaviour. For cost comparison only to blue line in Figure 49 is in scope. For the 36 month in scope only cost for defences were made. There were no cost associated with DDOS related damage. This blue line shows an increasing stable trend for the cost paid on attack related damages and the costs for the defences in place. The blue line is on average in line with reality. The model shows ISP related cost that are acceptable but relatively high. The cloud related costs in the model are at the lower level boundary. The cloud cost behaviour can be explained by the fact that after a 3 years contract period the cost will change (see red line) while in the model these cost change every moment (blue line). Although there is a slight difference in actual and model behaviour the model will not be adjusted. It is believed that this slight difference will not have an impact on the policy evaluation process.

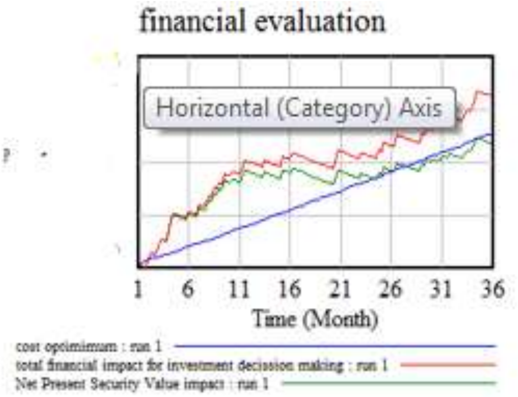


Fig 49. Model output: cost optimum line (blue) and other financial metrics output

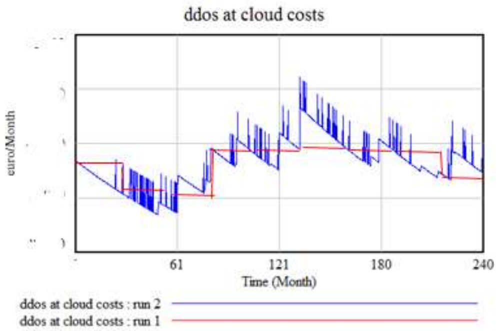


Fig 50. Model output: cloud cost behaviour in the model (blue) and plotted actual behaviour (red)

SME interview indicated that reactive security management also resulted into more supplier power during negotiations of implementing newly purchased security solutions. In this situation management decided to invest after a visible cyber security impact in line with the detection trap (Martinez-Moyano et al 2011). The Figure below contains Figures for 2 scenarios cumulative DDOS cost over time. Run 1 is all defences are implemented. Run 2 cloud defences are purchased after a specific successful bandwidth DDOS attack. Detection trap related cost behaviour is confirmed in Figure 51.

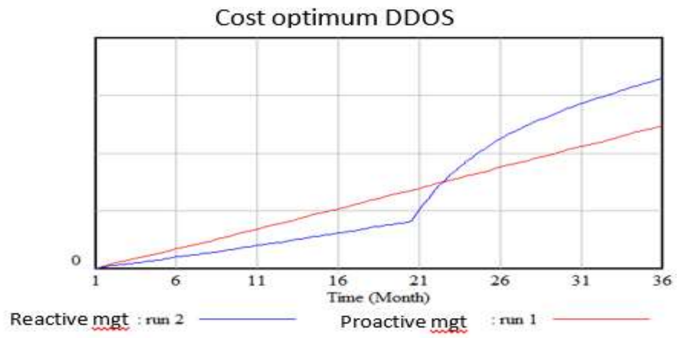


Fig 51. Model output: reactive management versus proactive security management. The cost difference of the detection trap over time

Specific DDOS behaviour

As part of the validation process several simulation have been run where cetribus paribus several parameters have been adjusted and the expected effect will be compared with the actual effect of the model.

NR	Start assumption	Expected effect	Effect in model
1	DDOS capacity growth is 0 (was 9)	Defence capacity decline over time	As expected
2	Time preparation government intervention set on 1 month (was random). Political attack boundary set on 1 (was 3)	DDOS capacity growth will be delayed	As expected
3	Scenario 2 but botnet usage for DDOS is 50% (was 7%) and all government attempts are successful (was random)	DDOS capacity growth will be limited	As expected
4	Budget pressure ratio = 50% (was 25%) and budget pressure time boundary is 18 months (was 36 months). No market power	More successful DDOS attacks and higher DDOS costs (defence and damage)	As expected
5	Strategic delay has no impact. Backlog delay norm on 500 (was 6)	Changing financial behaviour	Turning point (limits to growth) becomes later visible
6	As 5 higher priority on solving DDOS findings is 0.3 (was 0.0003)	Equilibrium in costs but more positive	Very low level on targeted DDOS attack result into same financial behaviour as scenario 5.
7	Multi vector attack analysis is 0.5 (was 0.0037)	Increase in number of successful attacks in the first months due to reactive security management	Slower than expected

Fig 52. Table with specific parameter adjustment, expected behaviour and actual model behaviour

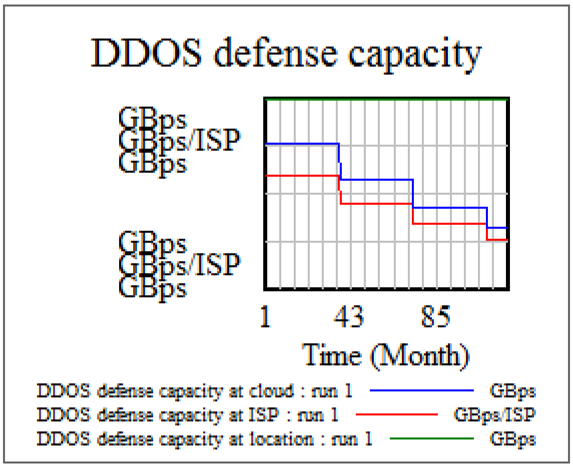


Fig 53. DDOS bandwidth defence capacity development in simulation 1.

Simulation 1. The overall expected and visible model behaviour is that defence capacity at the internet service provider and in the cloud will decline to a more appropriate level under the assumption that the attack capacity remains at a stable level. Defence capacity at location will not decline since that capacity has the minimum required defence level. This behaviour over time is visible in the Figure 53.

Simulation 2. In the Figure 54 the red line has some very horizontal delays in growth. These delays are caused by changes in government invervention model settings. In these settings government will do an intervention action after one succesful attack without any delay. Expected model behaviour and actual model behaviour are the same

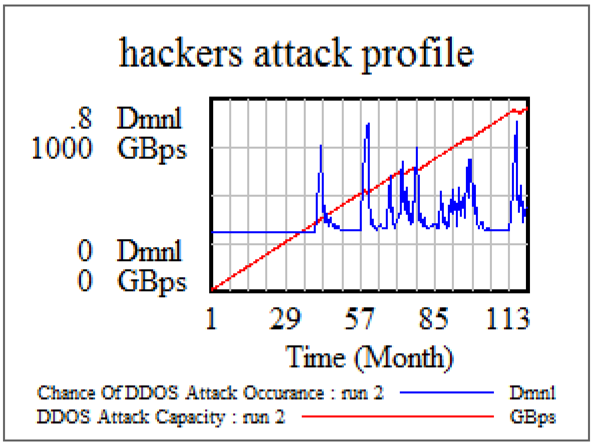


Fig 54. DDOS attack capacity and chance of being attacked over time in simulation 2

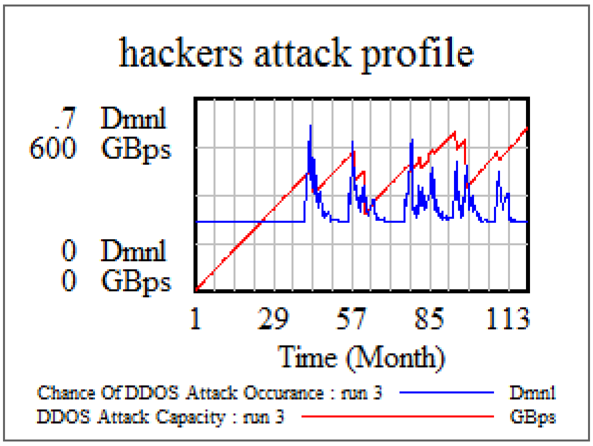


Fig 55. DDOS attack capacity and chance of being attacked over time in simulation 3

Simulation 3. In this simulation the effectiveness of governmental interventions have been increased because it is assumed that every intervention will be succesfull and that botnets are more succefully targetted by govenent. The red line cumulative attack capacity over time in Figure 55 has a saw-tooth behaviour. It declines every time after government intervention and will recover over time. Model behaviour is in line with expectations.

Simulation 4. The model settings resulted in situation that defence capacity for bandwith attacks will be lowered more quickly if no succesful attacks will be observed. In this analysis run 1 is the behaviour of the model without any changes and run4 is the behaviour of the model as stated in simulation 4. In the Figures 56 and 57 the financial behaviour is visible. The cost of DDOS defence cost are more or less the same. However the cost of the impact of DDOS attacks is much higher compared to regular model behaviour. Cumulative revenue loss due to succesful DDOS attacks is

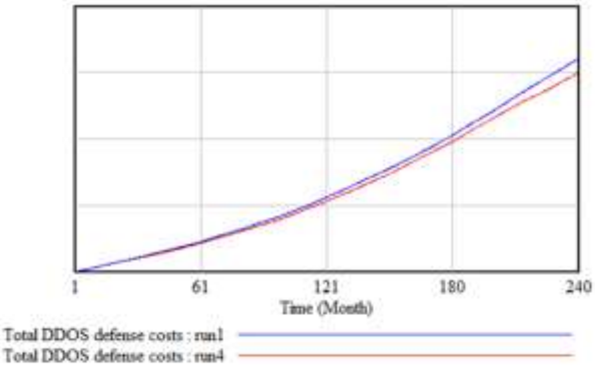


Fig 56. DDOS defence cost over time. Normal model (run 1) versus simulation 4 (run 4)

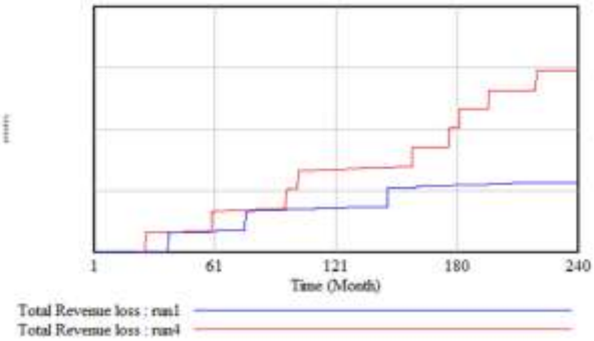


Fig 57. Revenue loss and Total Value loss (= financial impact of customer outflow). Normal model (run 1) versus simulation 4 (run 4)

significantely higher in the simulation (blue line, run4) compared to the normal run (red line, run1). Although the DDOS defence costs are approximately the same the impact of succeful DDOS attacks significantely increases. Therefore we believe this simulation is in line with our predicted results.

Simulation 5 and 6. In terms of financial evaluation both simulation 5 and 6 behave the same as stated in figure 57 because there is no "red line for run4 visible". A strategic delay results into a delay of new income generating features and therefore limits future revenue growth. Since future income declines, the benefits of mitigating these attacks will also decline. Run4 and run5 assume there is no strategic delay and therefore the Net Present security value is higher over time afther month 60.

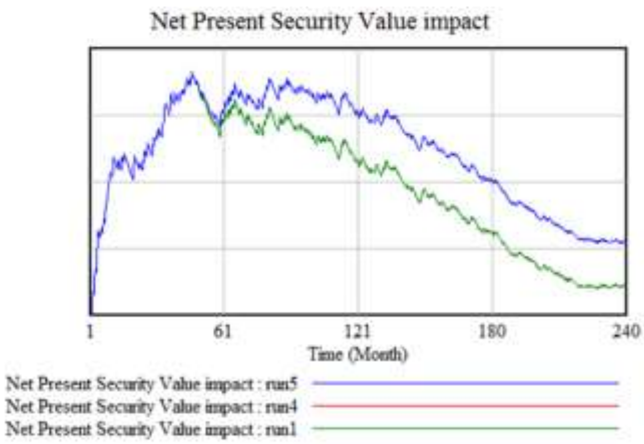


Fig 57. Net Present security value in situation of strategic delay (run 1) and no strategic delay (run 4 and 5)

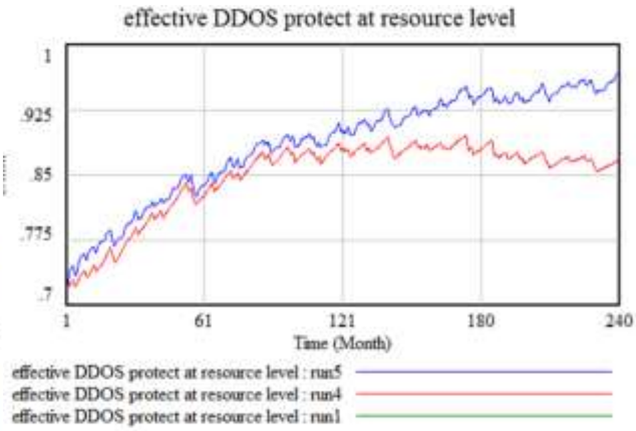


Fig 58. DDOS protection at resource level with low priority (run 1 and run 4) and high priority (run 5)

The increased attention on resolving DDOS vulnerabilities increase the level of effective protection at the level of resources as shown in Figure 58. However, due to the limited targetted attack behaviour in the model a different financial impact will be not be observed (figure 57 does not show different behaviour in blue (run5) and red (run4) lines).

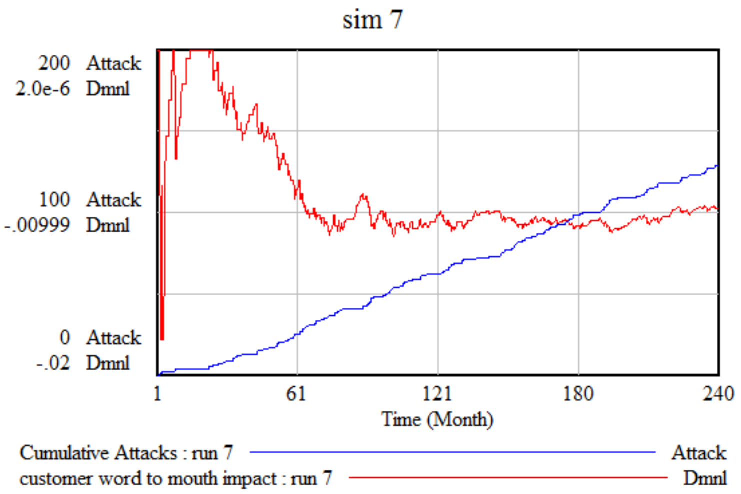


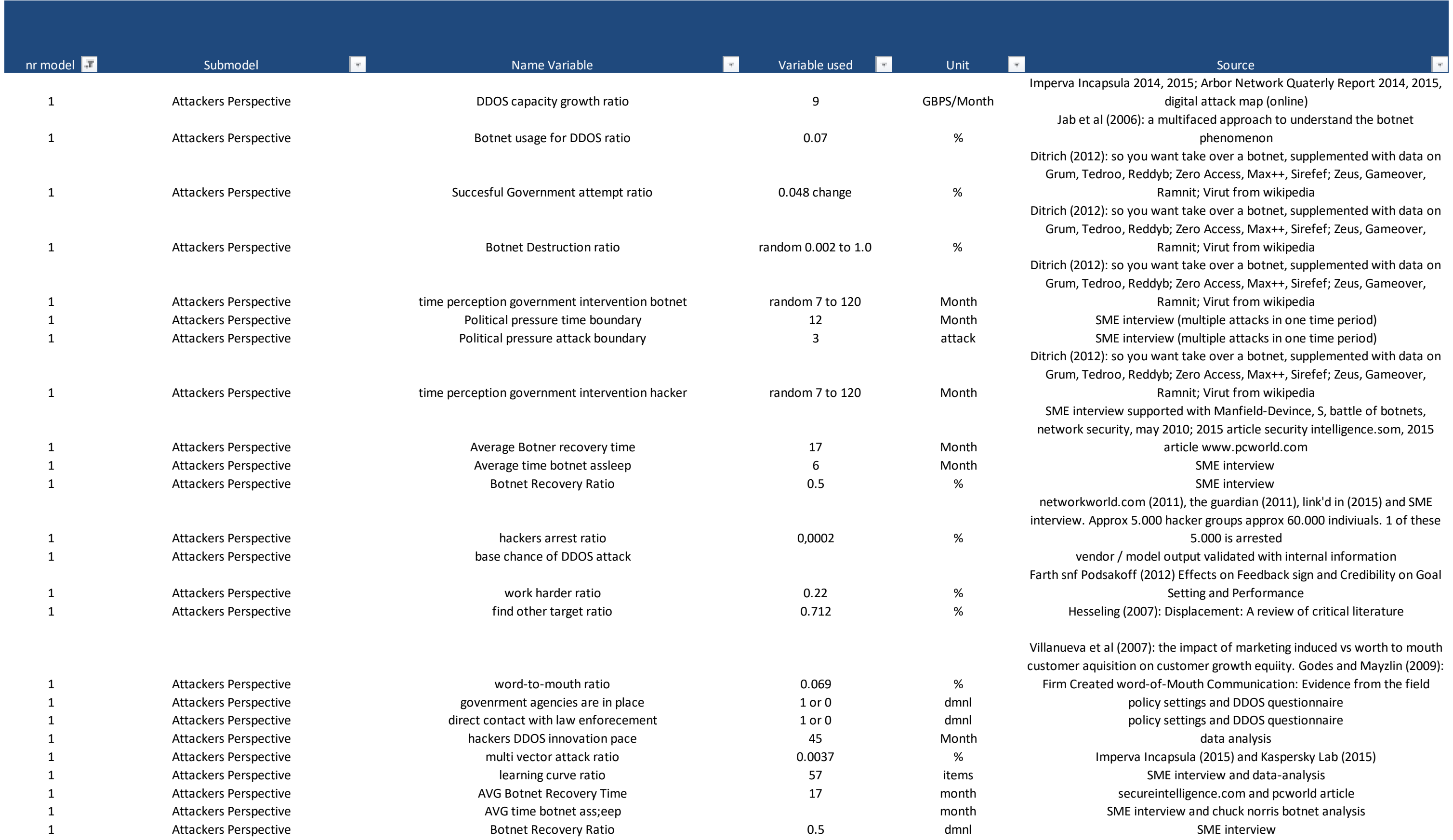
Fig 59. High level targeted DDOS attack impacting cumulative attack trend and customer word to mouth.

Simulation 7. A high level of targetted DDOS attacks evoke a negative customer word of mouth impact (red line) because a lot of these attacks are succesfull (blue line). The anticipation of the organisation takes time but at a given moment customer word of mouth impact stops declining as and the number of succesful DDOS attacks starts to decline. The improvement rate in the model lacks expectation. Although a management decission that will allocate far more capacity to resolving DDOS vulnerabilities in this situation is very realistic and confirmed by interviews this is in line with Vennix (1996) not included in the model.

Appendix 3: Model parameters and used sources

Below a specification per sub model has been included explaining the used parameters in the models and the sources used for their value in the model. Parameter values are based upon internal data sources, supplier data sources, scientific papers of interviews

Sub model 1: Attackers' perspective DDOS attack exogenous parameters and sources



nr model	Submodel	Name Variable	Variable used	Unit	Source
1	Attackers Perspective	DDOS capacity growth ratio	9	GBPS/Month	Imperva Incapsula 2014, 2015; Arbor Network Quaterly Report 2014, 2015, digital attack map (online)
1	Attackers Perspective	Botnet usage for DDOS ratio	0.07	%	Jab et al (2006): a multifaced approach to understand the botnet phenomenon
1	Attackers Perspective	Succesful Government attempt ratio	0.048 change	%	Ditrich (2012): so you want take over a botnet, supplemented with data on Grum, Tedroo, Reddyb; Zero Access, Max++, Sirefef; Zeus, Gameover, Ramnit; Virut from wikipedia
1	Attackers Perspective	Botnet Destruction ratio	random 0.002 to 1.0	%	Ditrich (2012): so you want take over a botnet, supplemented with data on Grum, Tedroo, Reddyb; Zero Access, Max++, Sirefef; Zeus, Gameover, Ramnit; Virut from wikipedia
1	Attackers Perspective	time perception government intervention botnet	random 7 to 120	Month	Ditrich (2012): so you want take over a botnet, supplemented with data on Grum, Tedroo, Reddyb; Zero Access, Max++, Sirefef; Zeus, Gameover, Ramnit; Virut from wikipedia
1	Attackers Perspective	Political pressure time boundary	12	Month	SME interview (multiple attacks in one time period)
1	Attackers Perspective	Political pressure attack boundary	3	attack	SME interview (multiple attacks in one time period)
1	Attackers Perspective	time perception government intervention hacker	random 7 to 120	Month	Ditrich (2012): so you want take over a botnet, supplemented with data on Grum, Tedroo, Reddyb; Zero Access, Max++, Sirefef; Zeus, Gameover, Ramnit; Virut from wikipedia
1	Attackers Perspective	Average Botner recovery time	17	Month	SME interview supported with Manfield-Devince, S, battle of botnets, network security, may 2010; 2015 article security intelligence.som, 2015 article www.pcworld.com
1	Attackers Perspective	Average time botnet assleep	6	Month	SME interview
1	Attackers Perspective	Botnet Recovery Ratio	0.5	%	SME interview
1	Attackers Perspective	hackers arrest ratio	0,0002	%	networkworld.com (2011), the guardian (2011), link'd in (2015) and SME interview. Approx 5.000 hacker groups approx 60.000 indiviuals. 1 of these 5.000 is arrested
1	Attackers Perspective	base chance of DDOS attack			vendor / model output validated with internal information
1	Attackers Perspective	work harder ratio	0.22	%	Farth snf Podsakoff (2012) Effects on Feedback sign and Credibility on Goal Setting and Performance
1	Attackers Perspective	find other target ratio	0.712	%	Hesseling (2007): Displacement: A review of critical literature
1	Attackers Perspective	word-to-mouth ratio	0.069	%	Villanueva et al (2007): the impact of marketing induced vs worth to mouth customer aquisition on customer growth equiity. Godes and Mayzlin (2009): Firm Created word-of-Mouth Communication: Evidence from the field
1	Attackers Perspective	govenrment agencies are in place	1 or 0	dmnl	policy settings and DDOS questionnaire
1	Attackers Perspective	direct contact with law enforecement	1 or 0	dmnl	policy settings and DDOS questionnaire
1	Attackers Perspective	hackers DDOS innovation pace	45	Month	data analysis
1	Attackers Perspective	multi vector attack ratio	0.0037	%	Imperva Incapsula (2015) and Kaspersky Lab (2015)
1	Attackers Perspective	learning curve ratio	57	items	SME interview and data-analysis
1	Attackers Perspective	AVG Botnet Recovery Time	17	month	secureintelligence.com and pcworld article
1	Attackers Perspective	AVG time botnet ass;eep		month	SME interview and chuck norris botnet analysis
1	Attackers Perspective	Botnet Recovery Ratio	0.5	dmnl	SME interview

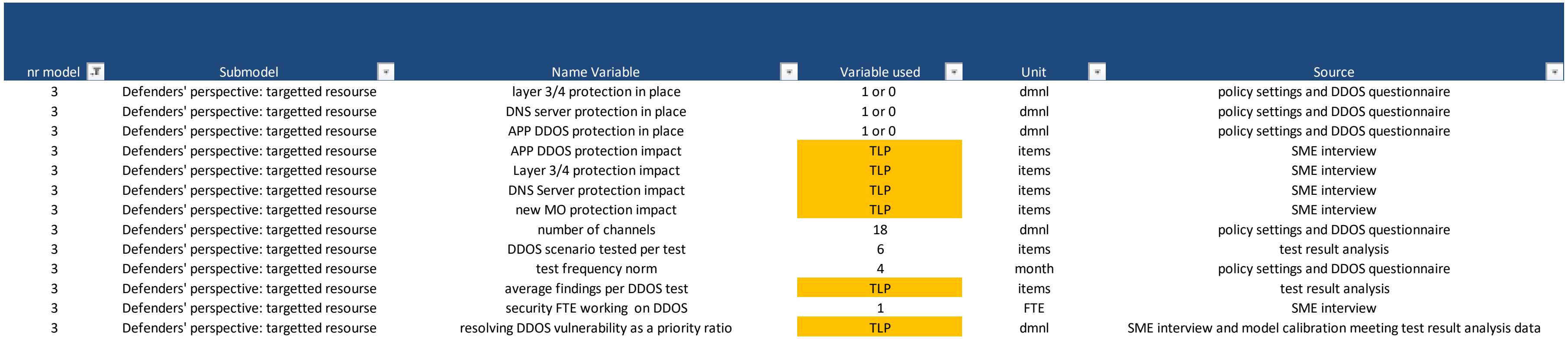
Fig 60. Sun model 1 parameter settings and references to sources

Sub model 2: defenders perspective: Bandwidth attack exogenous parameters and sources

nr model	Submodel	Name Variable	Variable used	Unit	Source
2	Defenders' perspective: bandwith attack	ISP detect and deflect capability in place	1 or 0	dmnl	policy settings and DDOS questionnaire
2	Defenders' perspective: bandwith attack	non-detect change	0.46	%	Altas reporting initative (2014, 2015), Yang (2013) A study on low rate DDOS attacks and SME input
2	Defenders' perspective: bandwith attack	Origin DDOS attack detected	0.70	%	Altas reporting initative (2014, 2015), Yang (2013) A study on low rate DDOS attacks and SME input
2	Defenders' perspective: bandwith attack	DDOS realtime monitoring in place	1 or 0	dmnl	policy settings and DDOS questionnaire
2	Defenders' perspective: bandwith attack	Devest at location fraction	0	GBPS / Month	variable included for simulating alternative investment
2	Defenders' perspective: bandwith attack	Invest at location fraction	0	GBPS / Month	variable included for simulating alternative investment
2	Defenders' perspective: bandwith attack	cloud targetted for DDOS	0.37	%	Kaspersky lab DDOS report in conjuctuin with customer succes stories of Akamai or Arbor Networks
2	Defenders' perspective: bandwith attack	cloud growth ratio (supplier policy)	TLP	dmnl/month	various blogs from (ex) supplier staff and SME interview
2	Defenders' perspective: bandwith attack	MI growth ratio cloud	TLP	dmnl/month	variable included for simulating alternative scenario's
2	Defenders' perspective: bandwith attack	1st start at cloud	TLP	GBPS	model variable needed for delayed cloud investment where inital DDOS defense at cloud is 0
2	Defenders' perspective: bandwith attack	cloud implementation boundary	TLP	month	SME interview. Cloud defense will be implemented as a reaction if the effective duration of the DDOS attack will be longer then predefined time boundary
2	Defenders' perspective: bandwith attack	pressure boundary ratio	36	month	regular period used for contracting
2	Defenders' perspective: bandwith attack	budget pressure ratio	0.25		SME interview. Pressure should be between 0.05 and 0.25
2	Defenders' perspective: bandwith attack	Initial DDOS Defense capacity at ISP			
2	Defenders' perspective: bandwith attack	ISP capacity growth policy (supplier)	0	GBPS	variable included for alternative setting
2	Defenders' perspective: bandwith attack	MI growth ratio ISP	0.005	GBPS	contracting provide means for small adjustments
2	Defenders' perspective: bandwith attack	Invest at ISP Fraction	0	GBPS/Month*ISP	variable included for alternative setting
2	Defenders' perspective: bandwith attack	Devest at ISP Fraction	0	GBPS/Month*ISP	variable included for alternative setting
2	Defenders' perspective: bandwith attack	ISP targetted for DDOS chance	0.41	%	Kaspersky lab DDOS reports
2	Defenders' perspective: bandwith attack	additional flexible capacity at ISP	TLP	%	policy settings and DDOS questionnaire
2	Defenders' perspective: bandwith attack	Number of ISP boundary	5	ISP	Number of Suitable ISP's within the region
2	Defenders' perspective: bandwith attack	DDOS RA ISP connectivity norm	TLP	ISP	policy settings and DDOS questionnaire
2	Defenders' perspective: bandwith attack	time to wait for adjustment ISP contract	12	Month	regular contracting
2	Defenders' perspective: bandwith attack	network capacity			
2	Defenders' perspective: bandwith attack	initial network capacity needed for business	TLP	GBPS	policy settings and DDOS questionnaire

Fig 61. Sun model 2 parameter settings and references to sources. TLP Orange is no open sharable information

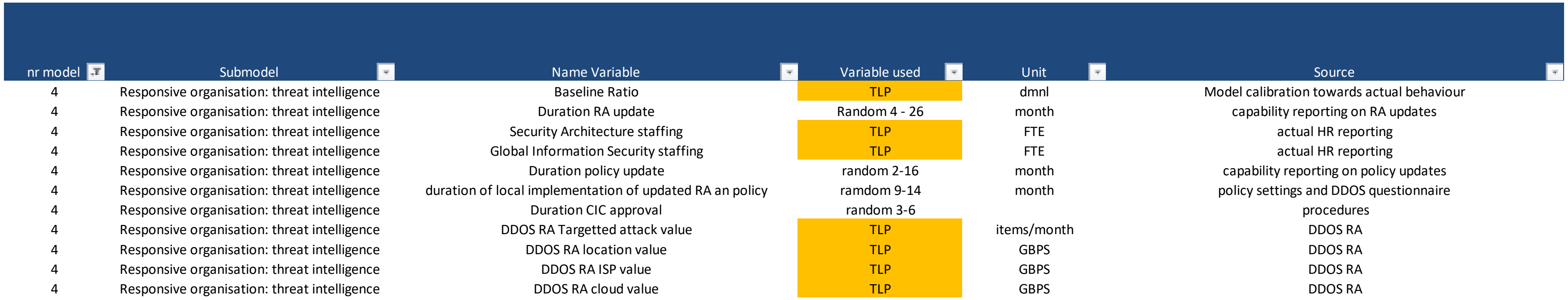
Sub model 3: defenders perspective: targeted resource attack exogenous parameters and sources



nr model	Submodel	Name Variable	Variable used	Unit	Source
3	Defenders' perspective: targetted resourse	layer 3/4 protection in place	1 or 0	dmnl	policy settings and DDOS questionnaire
3	Defenders' perspective: targetted resourse	DNS server protection in place	1 or 0	dmnl	policy settings and DDOS questionnaire
3	Defenders' perspective: targetted resourse	APP DDOS protection in place	1 or 0	dmnl	policy settings and DDOS questionnaire
3	Defenders' perspective: targetted resourse	APP DDOS protection impact	TLP	items	SME interview
3	Defenders' perspective: targetted resourse	Layer 3/4 protection impact	TLP	items	SME interview
3	Defenders' perspective: targetted resourse	DNS Server protection impact	TLP	items	SME interview
3	Defenders' perspective: targetted resourse	new MO protection impact	TLP	items	SME interview
3	Defenders' perspective: targetted resourse	number of channels	18	dmnl	policy settings and DDOS questionnaire
3	Defenders' perspective: targetted resourse	DDOS scenario tested per test	6	items	test result analysis
3	Defenders' perspective: targetted resourse	test frequency norm	4	month	policy settings and DDOS questionnaire
3	Defenders' perspective: targetted resourse	average findings per DDOS test	TLP	items	test result analysis
3	Defenders' perspective: targetted resourse	security FTE working on DDOS	1	FTE	SME interview
3	Defenders' perspective: targetted resourse	resolving DDOS vulnerability as a priority ratio	TLP	dmnl	SME interview and model calibration meeting test result analysis data

Fig 62. Sun model 3 parameter settings and references to sources. TLP Orange is no open sharable information

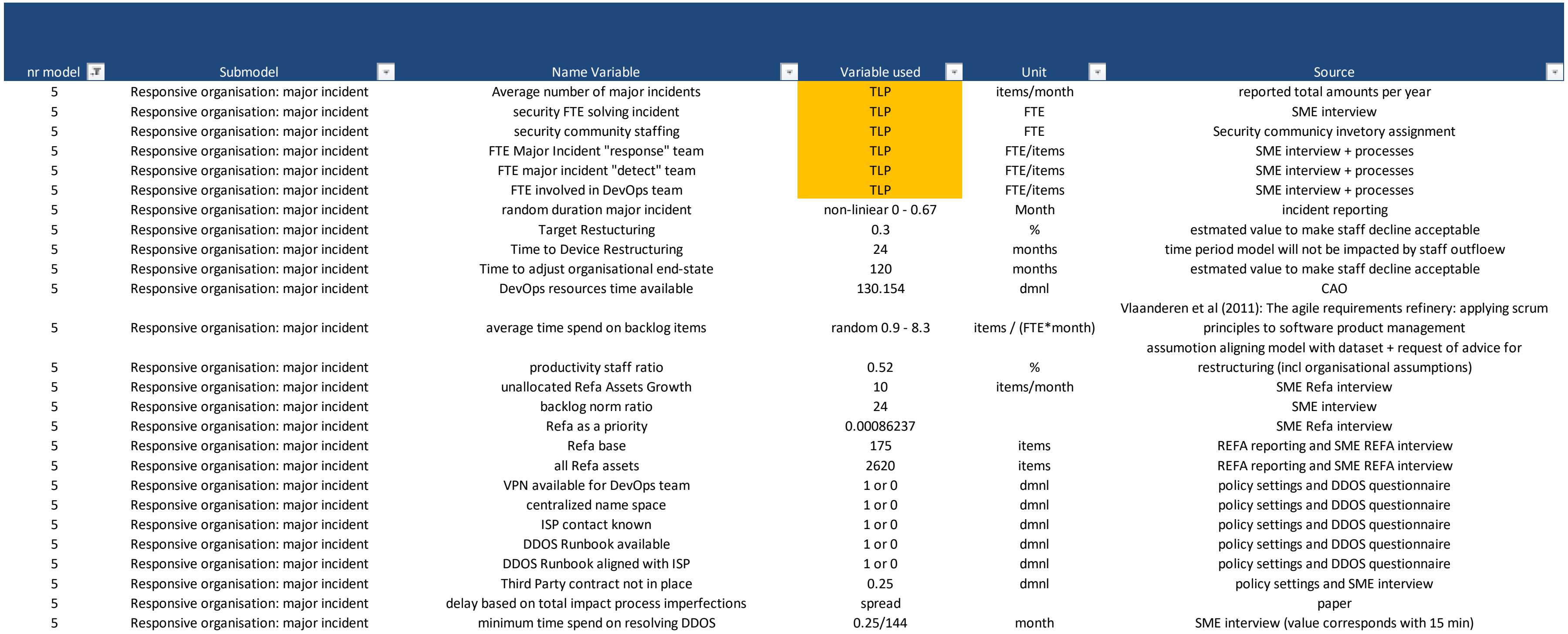
Sub model 4: the resilient organisation: threat intelligence exogenous parameters and sources



nr model	Submodel	Name Variable	Variable used	Unit	Source
4	Responsive organisation: threat intelligence	Baseline Ratio	TLP	dmnl	Model calibration towards actual behaviour
4	Responsive organisation: threat intelligence	Duration RA update	Random 4 - 26	month	capability reporting on RA updates
4	Responsive organisation: threat intelligence	Security Architecture staffing	TLP	FTE	actual HR reporting
4	Responsive organisation: threat intelligence	Global Information Security staffing	TLP	FTE	actual HR reporting
4	Responsive organisation: threat intelligence	Duration policy update	random 2-16	month	capability reporting on policy updates
4	Responsive organisation: threat intelligence	duration of local implementation of updated RA an policy	ramdom 9-14	month	policy settings and DDOS questionnaire
4	Responsive organisation: threat intelligence	Duration CIC approval	random 3-6		procedures
4	Responsive organisation: threat intelligence	DDOS RA Targetted attack value	TLP	items/month	DDOS RA
4	Responsive organisation: threat intelligence	DDOS RA location value	TLP	GBPS	DDOS RA
4	Responsive organisation: threat intelligence	DDOS RA ISP value	TLP	GBPS	DDOS RA
4	Responsive organisation: threat intelligence	DDOS RA cloud value	TLP	GBPS	DDOS RA

Fig 63. Sun model 4 parameter settings and references to sources. TLP Orange is no open sharable information

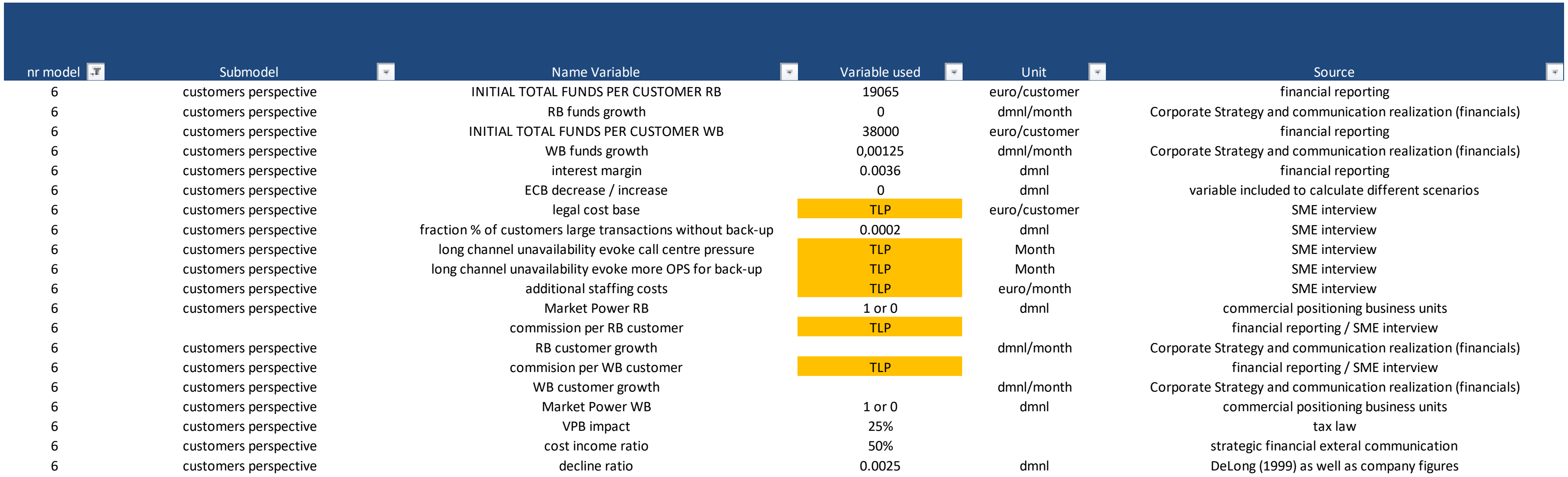
Sub model 5: the resilient organisation: major incident response intelligence exogenous parameters and sources



nr model	Submodel	Name Variable	Variable used	Unit	Source
5	Responsive organisation: major incident	Average number of major incidents	TLP	items/month	reported total amounts per year
5	Responsive organisation: major incident	security FTE solving incident	TLP	FTE	SME interview
5	Responsive organisation: major incident	security community staffing	TLP	FTE	Security communicy invetory assignment
5	Responsive organisation: major incident	FTE Major Incident "response" team	TLP	FTE/items	SME interview + processes
5	Responsive organisation: major incident	FTE major incident "detect" team	TLP	FTE/items	SME interview + processes
5	Responsive organisation: major incident	FTE involved in DevOps team	TLP	FTE/items	SME interview + processes
5	Responsive organisation: major incident	random duration major incident	non-liniear 0 - 0.67	Month	incident reporting
5	Responsive organisation: major incident	Target Restucturing	0.3	%	estmated value to make staff decline acceptable
5	Responsive organisation: major incident	Time to Device Restructuring	24	months	time period model will not be impacted by staff outfloew
5	Responsive organisation: major incident	Time to adjust organisational end-state	120	months	estmated value to make staff decline acceptable
5	Responsive organisation: major incident	DevOps resources time available	130.154	dmnl	CAO
5	Responsive organisation: major incident	average time spend on backlog items	random 0.9 - 8.3	items / (FTE*month)	Vlaanderen et al (2011): The agile requirements refinery: applying scrum principles to software product management
5	Responsive organisation: major incident	productivity staff ratio	0.52	%	assumotion aligning model with dataset + request of advice for restructuring (incl organisational assumptions)
5	Responsive organisation: major incident	unallocated Refa Assets Growth	10	items/month	SME Refa interview
5	Responsive organisation: major incident	backlog norm ratio	24		SME interview
5	Responsive organisation: major incident	Refa as a priority	0.00086237		SME Refa interview
5	Responsive organisation: major incident	Refa base	175	items	REFA reporting and SME REFA interview
5	Responsive organisation: major incident	all Refa assets	2620	items	REFA reporting and SME REFA interview
5	Responsive organisation: major incident	VPN available for DevOps team	1 or 0	dmnl	policy settings and DDOS questionnaire
5	Responsive organisation: major incident	centralized name space	1 or 0	dmnl	policy settings and DDOS questionnaire
5	Responsive organisation: major incident	ISP contact known	1 or 0	dmnl	policy settings and DDOS questionnaire
5	Responsive organisation: major incident	DDOS Runbook available	1 or 0	dmnl	policy settings and DDOS questionnaire
5	Responsive organisation: major incident	DDOS Runbook aligned with ISP	1 or 0	dmnl	policy settings and DDOS questionnaire
5	Responsive organisation: major incident	Third Party contract not in place	0.25	dmnl	policy settings and SME interview
5	Responsive organisation: major incident	delay based on total impact process imperfections	spread		paper
5	Responsive organisation: major incident	minimum time spend on resolving DDOS	0.25/144	month	SME interview (value corresponds with 15 min)

Fig 64. Sun model 5 parameter settings and references to sources. TLP Orange is no open sharable information

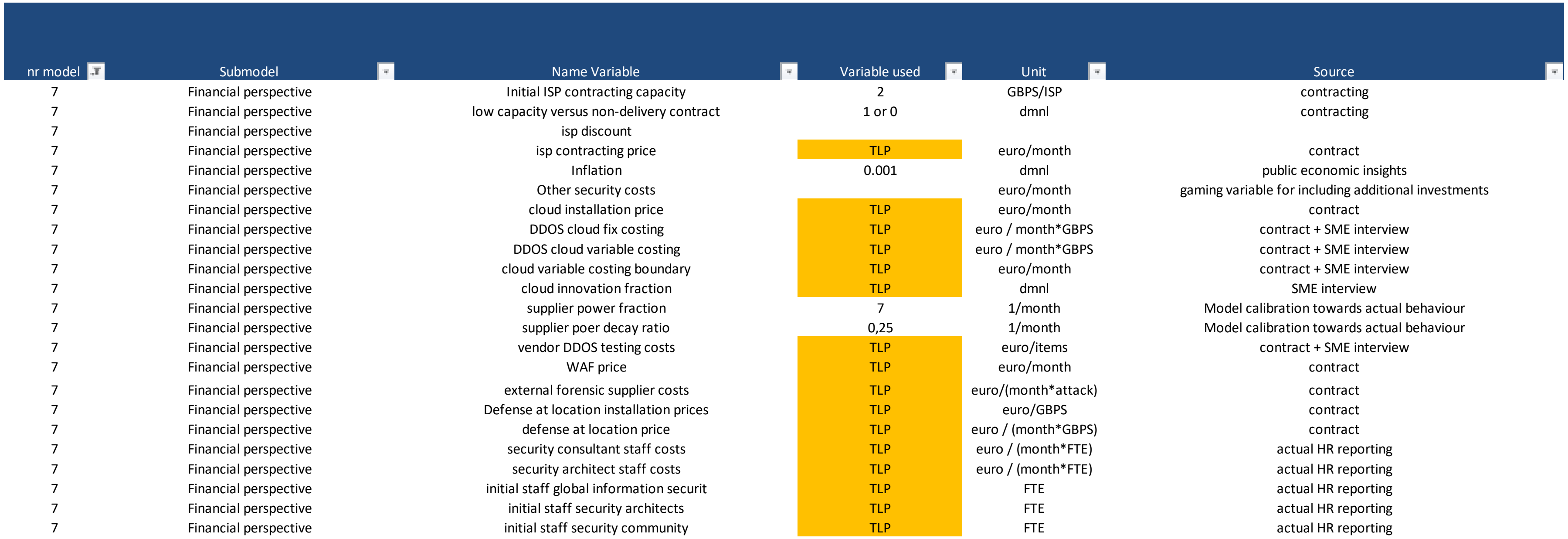
Output model 6: customer impact intelligence exogenous parameters and sources



nr model	Submodel	Name Variable	Variable used	Unit	Source
6	customers perspective	INITIAL TOTAL FUNDS PER CUSTOMER RB	19065	euro/customer	financial reporting
6	customers perspective	RB funds growth	0	dmnl/month	Corporate Strategy and communication realization (financials)
6	customers perspective	INITIAL TOTAL FUNDS PER CUSTOMER WB	38000	euro/customer	financial reporting
6	customers perspective	WB funds growth	0,00125	dmnl/month	Corporate Strategy and communication realization (financials)
6	customers perspective	interest margin	0.0036	dmnl	financial reporting
6	customers perspective	ECB decrease / increase	0	dmnl	variable included to calculate different scenarios
6	customers perspective	legal cost base	TLP	euro/customer	SME interview
6	customers perspective	fraction % of customers large transactions without back-up	0.0002	dmnl	SME interview
6	customers perspective	long channel unavailability evoke call centre pressure	TLP	Month	SME interview
6	customers perspective	long channel unavailability evoke more OPS for back-up	TLP	Month	SME interview
6	customers perspective	additional staffing costs	TLP	euro/month	SME interview
6	customers perspective	Market Power RB	1 or 0	dmnl	commercial positioning business units
6		commission per RB customer	TLP		financial reporting / SME interview
6	customers perspective	RB customer growth		dmnl/month	Corporate Strategy and communication realization (financials)
6	customers perspective	commision per WB customer	TLP		financial reporting / SME interview
6	customers perspective	WB customer growth		dmnl/month	Corporate Strategy and communication realization (financials)
6	customers perspective	Market Power WB	1 or 0	dmnl	commercial positioning business units
6	customers perspective	VPB impact	25%		tax law
6	customers perspective	cost income ratio	50%		strategic financial exteral communication
6	customers perspective	decline ratio	0.0025	dmnl	DeLong (1999) as well as company figures

Fig 65. Sun model 6 parameter settings and references to sources. TLP Orange is no open sharable information

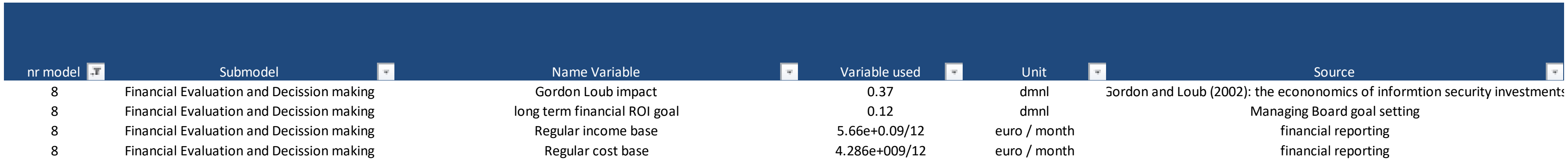
Output model 7: financial impact exogenous parameters and sources



nr model	Submodel	Name Variable	Variable used	Unit	Source
7	Financial perspective	Initial ISP contracting capacity	2	GBPS/ISP	contracting
7	Financial perspective	low capacity versus non-delivery contract	1 or 0	dmnl	contracting
7	Financial perspective	isp discount			
7	Financial perspective	isp contracting price	TLP	euro/month	contract
7	Financial perspective	Inflation	0.001	dmnl	public economic insights
7	Financial perspective	Other security costs		euro/month	gaming variable for including additional investments
7	Financial perspective	cloud installation price	TLP	euro/month	contract
7	Financial perspective	DDOS cloud fix costing	TLP	euro / month*GBPS	contract + SME interview
7	Financial perspective	DDOS cloud variable costing	TLP	euro / month*GBPS	contract + SME interview
7	Financial perspective	cloud variable costing boundary	TLP	euro/month	contract + SME interview
7	Financial perspective	cloud innovation fraction	TLP	dmnl	SME interview
7	Financial perspective	supplier power fraction	7	1/month	Model calibration towards actual behaviour
7	Financial perspective	supplier poer decay ratio	0,25	1/month	Model calibration towards actual behaviour
7	Financial perspective	vendor DDOS testing costs	TLP	euro/items	contract + SME interview
7	Financial perspective	WAF price	TLP	euro/month	contract
7	Financial perspective	external forensic supplier costs	TLP	euro/(month*attack)	contract
7	Financial perspective	Defense at location installation prices	TLP	euro/GBPS	contract
7	Financial perspective	defense at location price	TLP	euro / (month*GBPS)	contract
7	Financial perspective	security consultant staff costs	TLP	euro / (month*FTE)	actual HR reporting
7	Financial perspective	security architect staff costs	TLP	euro / (month*FTE)	actual HR reporting
7	Financial perspective	initial staff global information securit	TLP	FTE	actual HR reporting
7	Financial perspective	initial staff security architects	TLP	FTE	actual HR reporting
7	Financial perspective	initial staff security community	TLP	FTE	actual HR reporting

Fig 66. Sun model 7 parameter settings and references to sources. TLP Orange is no open sharable information

Output model 8: financial evaluation exogenous parameters and sources



nr model	Submodel	Name Variable	Variable used	Unit	Source
8	Financial Evaluation and Decission making	Gordon Loub impact	0.37	dmnl	Gordon and Loub (2002): the econonomics of informtion security investments
8	Financial Evaluation and Decission making	long term financial ROI goal	0.12	dmnl	Managing Board goal setting
8	Financial Evaluation and Decission making	Regular income base	5.66e+0.09/12	euro / month	financial reporting
8	Financial Evaluation and Decission making	Regular cost base	4.286e+009/12	euro / month	financial reporting

Fig 67. Sun model 8 parameter settings and references to sources. TLP Orange is no open sharable information

Appendix 4: parameters used for scenario analysis

Scenario	Parameter	Set on value in Monte Carlo simulation
Increase investment pace (risk mitigation)	Baseline ratio	Between 0.9 to 1.0 was 0.5
Increase footprint of business activities (risk mitigation)	WB / RB fund growth WB / RB customer growth	Between 0.002 to 0.003 was 0.0125 for WB fund growth, RB was 0 Between 0.002 to 0.003 was 0
Engage in a trusted network initiative (risk transfer)	Origin known probability Non detection probability Other security costs	Between 0.97 and 0.99 was 0.7 Between 0.01 and 0.03 was 0.46 Between 10.000 and 12.500 was 0
Lobby for stronger government and law enforcement intervention (risk transfer)	Political pressure attack boundary Political pressure time boundary	Between 1 and 2 was 3 Between 30 and 36 was 12
Accept these cost for doing business (risk retention)	n/a	n/a
Accept lower service levels (risk retention)	n/a	n/a

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, Massachusetts, 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