jamk.fi

Requirements for technical environment of cyber security exercises

Marko Vatanen

Master's Thesis
10 / 2015

Master's Degree Programme in Information Technology

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

DESCRIPTION

Author(s)	Type of publication	Date
Vatanen, Marko	Master's Thesis	19.10.2015
	Pages 56	Language English
	Confidential ( ) Until	Permission for web publication ()

Title
Requirements for technical environment of cyber security exercises

Degree Programme
Master's Degree Programme in Information Technology

Tutor(s)
Karo Saharinen
Mika Karjalainen

Assigned by
JAMK University of Applied Sciences / JYVSECTEC
Jarmo Siltanen

Abstract

The use of Internet and digitalization has driven nations, enterprises, and citizens to be reliant on services provided with information technology. Cyber security exercises provide opportunities for organizations to demonstrate critical capabilities and reveal how effectively they integrate people, processes, and technology to protect their critical information, services, and assets. Cyber exercises also enable organizations to experiment and develop their capabilities. The exercises can help train organizations to improve their ability to mitigate impacts to business from cyber threats and attacks.

In this thesis the focus is on defining the requirements of a technical environment for conducting various cyber security exercises. The research questions chosen for this master's thesis were: What are the requirements for implementation of different cyber threats? What are the requirements for providing a realistic and useful environment for defenders and IT personnel? What are the requirements for controlling the exercise? The requirements are divided into six major categories: general requirements, global world or "Internet", defending team requirements, threat actors' requirement, exercise control, and traffic simulation. The selected requirements are gathered from various scientific publications and other references concerning the technical environment.

As a result of the research there is a list of 35 different generalized requirements for implementing or constructing technical environment for cyber security exercises.

Keywords
Cyber security, exercise, cyber range, technical cyber exercises

Miscellaneous

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

KUVAILULEHTI

Tekijä(t)	Julkaisun laji	Päivämäärä
Vatanen, Marko	Master's Thesis	15.10.2015
	Sivumäärä 56	Julkaisun kieli Englanti
	Luottamuksellisuus ( ) saakka	Verkkojulkaisulupa myönnetty ()

Työn nimi
Vaatimukset kyberturvallisuusharjoituksien tekniselle ympäristölle

Koulutusohjelma
Master's Degree Programme in Information Technology

Työn ohjaaja(t)
Karo Saharinen
Mika Karjalainen

Toimeksiantaja(t)
Jyväskylän ammattikorkeakoulu Oy
Jarmo Siltanen

Tiivistelmä

Digitalisaation ja Internetin käytön yleistymisen kautta ovat valtiot, yritykset ja kansalaiset entistä riippuvaisempia palveluista, joita tarjotaan hyödyntäen IT-järjestelmiä. Kyberturvallisuusharjoitukset mahdollistavat organisaatioiden testata ja koestaa kyvykkyyttään integroida ihmiset, prosessit ja teknologia suojellakseen organisaatiolle kriittisiä tietoja, palveluita ja omaisuutta. Harjoitustoiminta myös kehittää ja antaa mahdollisen testata uusia toimintamenetelmiä sekä järjestelmiä. Harjoitukset kouluttavat organisaatioita parantamaan kyvykkyyttä suojautua liiketoimintaan kohdistuvia riskejä vastaan.

Opinnäytetyö fokusoituu vaatimusmäärittelyyn kyberturvallisuusharjoituksien teknistä ympäristöä varten. Valitut tutkimuskysymykset olivat seuraavat: Mitä vaatimuksia aiheutuu eri kyberhyökkäyksien toteuttamisesta ympäristössä? Mitä vaatimuksia on johdettavissa oikeista organisaatioympäristöistä sekä puolustusteknologioista? Mitä vaatimuksia aiheutuu kyberturvallisuusharjoituksen hallinnasta? Vaatimukset on jaoteltu kuuteen eri kategoriaan: yleiset vaatimukset, globaali maailma tai ”Internet”, organisaatioympäristöjen vaatimukset, uhkatoimijoiden vaatimukset, harjoituksen hallinta, käyttäjä- ja liikennesimulaatio. Valitut vaatimukset on kerätty eri tieteellisistä julkaisuista, kirjallisuudesta sekä muista toimialan lähteistä.

Tutkimuksen tuloksena muodostui lista 35:stä eri yleistetystä vaatimuksesta, jotka tulisi ottaa huomioon suunniteltaessa ja rakennettaessa teknistä ympäristöä kyberturvallisuusharjoituksien järjestämiseen.

Avainsanat (asiasanat)
Kyberturvallisuus, kyberturvallisuusharjoitus, kyberharjoitus, harjoitusympäristö, tekninen vaatimusmäärittely, tekninen ympäristö

Muut tiedot

CONTENTS

FIGURES

ACRONYMS

AS	Autonomous System
BGP	Border Gateway Protocol
BT	Blue Team
C&C	Command and Control
DDOS	Distributed Denial of Service
DGA	Domain Generation Algorithm
DNS	Domain Name Service
ICT	Information Communication Technology
IDS/IPS	Intrusion Detection System/Intrustion Prevention System
ISP	Internet Service Provider
LDAP	Lightweight Directory Access Protocol
MitM	Man in the Middle
MSEL	Master Scenario Event List
NTP	Network Time Protocol
RT	Red Team
TLD	Top level Domain
WT	White Team

1 INTRODUCTION

The use of Internet and digitalization has driven nations, enterprises, and citizens to be reliant on services provided with information technology. Production facilities, critical infrastructure companies, industry, and other businesses use information technology to form a backbone for modern day nations. The digitalization provides new opportunities, however, also introduces new risks, which results in the need to define the ways to secure these new activities. Cyber security has been used as a term to explain the ways to secure non-information based assets that might be vulnerable to threats via information and communication technologies; however, cyber security is often used interchangeably with the term information technology security (Solms & Niekerk 2013, 1).

Solms and Niekerk (Solms & Niekerk 2013, 4-5) determines the relationships between information and communication security, information security, and cyber security. The relationship is shown in Figure 1.

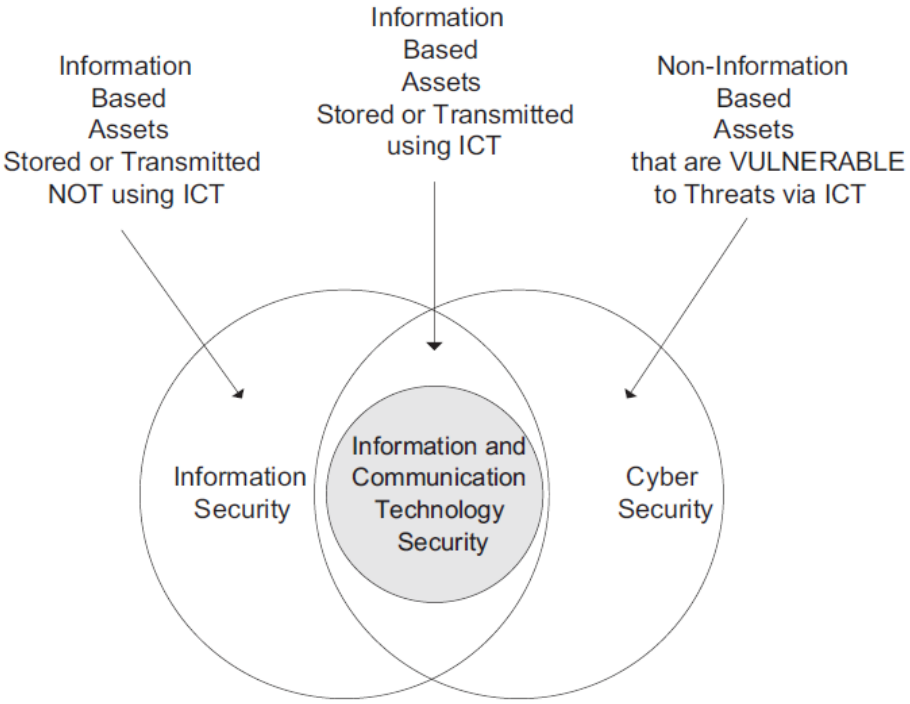

Figure 1. The relationships between information and communication security, information security, and cyber security (Solms & Niekerk 2013, 5)

The International Telecommunications Union (ITU) defines cyber security as follows:

> *"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment."* – (The International Telecommunications Union 2015)

Lately the use of information technology has expanded rapidly to encompass a far wider range of services and applications. The threats posed by cyber hacktivists, cyber criminals, and other actors require a wider knowledge from IT personnel who maintain these services and networks to defend services against those threats.

Cyber security exercises provide opportunities for organizations to demonstrate critical capabilities and reveal how effectively they integrate people, processes, and technology to protect their critical information, services, and assets. Cyber exercises also enable organizations to experiment and develop their capabilities. The exercises can help train organizations to improve their ability to mitigate impacts to business from cyber threats and attacks. Furthermore, exercises provide opportunities for continuous process improvement and the exercise can usually be included easily in the existing improvement programs. The modern organizations depend on other organizations as well (subcontractors, service providers, customers, etc.), which creates the need to exercise organizations' capability to handle complex cyber incidents conserning several organizations at the same time.

The exercises usually range from a one-day long exercise to 1 - 2 –week-long exercises. The time range does not include the time used in planning and preparations of the exercise. The complexity of the enterprise's IT environment has created the need to conduct larger scale cyber security exercises to train personnel and develop business and IT processes to handle different cyber incidents. This creates a need to have

a controlled and separate exercise environment which can be utilized to conduct different levels of cyber exercises.

The goal of this thesis was to create a generalized model of the requirements for technical environment of cyber exercises for the independent cyber security research, training, and development center JYVSECTEC. JYVSECTEC is a part of the Institute of Information Technology in JAMK University of Applied Sciences. The activity of JYVSECTEC started in 2011 as a development and investment project funded by European Union and private companies. JYVSECTEC aims to be one of the leading centers on cyber security in Finland. JYVSECTEC provides services to assist organizations on issues concerning information and cyber security issues. (JYVSECTEC – Jyväskylä Security Technology, 2015a)

2 RESEARCH QUESTIONS

2.1 Research objectives

The need for the research is the lack of publicly available requirements for technical environment of cyber exercises'. Many of the studies and publications state good practices or suggestions on how to conduct the exercise, however, they ignore or cover only shortly how to implement or build a cyber exercise environment (also called cyber range). The aim of the thesis was to find different requirements from literature and define a comprehensive set of requirements for a technical environment to conduct cyber exercises.

The objective was to provide requirements from different point of views:

- What are the requirements for implementation of different cyber threats?
- What are the requirements for providing a realistic and useful environment for defenders and IT personnel?
- What are the requirements for controlling the exercise?

Those are the main research questions for this thesis, however, also other requirements are gathered together to give as comprehensive a list of requirements as possible.

2.2 Research methods

The selected method for the thesis is inductive research approach which was chosen because of the nature of the research questions and the goal to specify an extensive list of requirements for building a technical environment for information and cyber security exercises.

Inductive research approach enables to build a theory based on earlier researches and publications on the topic (Saunders, Lewis & Thornhill 2009, 125-126). Also, the data used in the research is qualitative data.

The inductive approach is considered to begin with detailed observations of the world in order to move towards more abstract generalisations and ideas. In other words, when following inductive approach, a researcher applies to develop empirical generalisations and identify initial relationships as he advances through the research. (Burney, 2008)

One of the reasons for choosing the inductive research approach was also the lack of scientific studies of the requirements for technical environment of cyber security exercises. The idea of this thesis was to compile comprehensive a set of requirements that are not restricted to one type of exercise or other activity. The requirements were gathered from different studies, guides, and journals conducted on cyber security exercises which will outline the basis of the research data. However, also studies and publications on real attacks, defence methods and other supporting data were used as a source for this thesis.

The combination of the various sources enables the research to fulfill the needs to build a set of requirements for a realistic and versatile technical environment for cyber security exercises. The requirements are gathered in section 4 and the complete list of requirements is presented in Appendix I.

3 CYBER SECURITY EXERCISES

3.1 Overview of cyber security exercises

Cyber security, incident, and domain are vital terms to understand when considering conducting cyber security exercises. Cyber security and cyber domain consist of multi-layered worldwide interconnected networks involving IT networks which are operated by government organizations, public authorities and the business community. The quickly growing global cyber domain brings nations, businesses, and citizens even closer together. Although this development has brought wealth and growth, it has also increased the risks. Cyber attacks can interrupt or even bring down the parts of critical infrastructure and society's vital functions. (Secretariat of the Security Committee 2013, 17-19)

To understand elements of cyber security exercises, it is vital to know some key definitions:

- *Cyber domain or Cyberspace* is a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and other IT networks
- *Cyber attack* is an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data; or stealing controlled information
- *Cyber incident* is an action taken through the use of computer networks that results in an actual or potentially adverse effect on an information system[8] and/or the information residing therein
- *Master Scenario Event List (MSEL)* is a collection of pre-written events intented to guide an exercise towards planned outcomes
- *Event/Inject* is an activity executed as a part of master scenario event list

- *Blue Team* is a group of exercise participants that controls a particular organization environment
- *Red Team* is a group of participants that executes cyber attacks and acts as a different threat actors
- *White Team* is a group that controls and manages the cyber security exercise
- *Green Team* is a group that has administrative control of the technical environment used to provide cyber security exercises. Green team is often responsible for building necessary changes to exercise environments based on the exercise's scenario

The term *cyber* in this thesis refers to the people, operations, processes, and technology associated with digital information systems, networks, and the data that traverses them.

Information and cyber security work is an ongoing process within each organization. Private and public organizations are responsible for maintaining their information infrastructure and protecting its functions even during critical cyber attacks and IT incidents. They are also in charge of ensuring the normal operations of the IT systems and infrastructure under normal circumstances using their incident management, change management, and other processes. (Wilhelmson & Svensson 2013, 1-7)

Even when critical incidents increase pressure on an organization, information and cyber security need to be maintained so that IT and communication systems can operate or can be recovered quickly in the event of an interruption. During the normal operations as well as under the cyber attacks data and information will still need to be accessible and able to be transferred without compromising confidentiality, integrity and availability which means that the data and information need to be safe from unauthorized accesses or alterations without risking the access from normal users. (Wilhelmson & Svensson 2013, 1-7)

Cyber security domain operations are critical to the success and credibility of any organization. However, many organizations seldom evaluate and exercise their cyber

security capabilities and business processes to validate if those processes will be sufficient against cyber threats, incidents, or attacks. Organizations can execute many different scenarios during an exercise. The focus should be on assessing effects on critical systems and data which will have an impact on the operation or services. (Kick 2014, 1-4)

Conducting cyber security exercises can improve information and cyber security when combined with the skills to communicate problems and solutions in collaboration with others. The improvements can help an organization to improve normal operating processes and skills as well as train an organization to handle difficult circumstances that require decision-making under time pressure when significant values are at stake (such as material wealth and human life). Information and cyber security exercises complement regular preparedness and crisis management exercises and therefore are of great importance for organizations. (Wilhelmson & Svensson 2013, 1-7)

> *"Exercises to reduce threats, risks, vulnerabilities and consequences and protect critical information infrastructures in contemporary information and cyber security environment are vital in establishing a resilient society."* – (Wilhelmson & Svensson 2013, Foreword)

Conklin and White (Conklin & White 2006, 1) dictates in their paper that the cyber community is beginning to approve exercises as crucial tools for developing processes and skills to strengthen organizations against cyber threats.

Cyber security exercises allow organizations to demonstrate critical capabilities, thus exposing how efficiently they integrate their staff, processes, and technology to defend their information assets and cyber-reliant services. Cyber security exercises also enable organizations to experiment with new ideas and proposed capabilities. Exercises can help educate organizations to strengthen their ability to mitigate impacts to business and national security objectives resulting from targeted cyber attacks. They can enhance existing efforts within an organization to protect their critical assets. When exercises include a hands-on component, they can take an organization into

demonstrating their ability to protect, detect, and respond to various threats. (JYVSECTEC – Jyväskylä Security Technology 2015b)

Corporations and other organizations are reliant on ICT systems and networks. The digitalization is bringing more challenges for organizations to maintain and administer all the ICT systems and network by themselves. Therefore many organizations have outsourced many parts of the ICT to different service providers. Because organizations are dependent on other organizations it is important to train communication, decision making, and situational awareness of cyber incidents together. Cyber security exercises can be a tool for improving processes between different organizations and finding targets for development. In cyber security domain it is often difficult to know what service providers are allowed to do to prevent cyber attacks. (JYVSECTEC – Jyväskylä Security Technology 2015b)

Cyber security exercise is a powerful tool for enhancing an organization's readiness and resilience against modern cyber threats. The aim of the exercises is to identify targets for development of a cyber security incident's effects and consequences. The objective of cyber security exercises is to improve the participating organizations' abilities to detect vulnerabilities in their systems, services, and processes. The events of the exercise mainly emulate the actions of the planned threat actors against an organization's critical assets and data, however, also the impacts of the actions. A cyber security incident might have physical effects or the effects are limited to cyber domain. The objectives of the exercise define the scope and the form for the exercise. Exercises commonly focus on the actions before the cyber incident and the actions after the breach or incident is detected. The contents of the exercise can be roughly divided into the following (JYVSECTEC – Jyväskylä Security Technology 2015b):

1. Recognition, evaluation, briefing
    - Risk assessments
    - Procedures, responsibilities and roles
    - Identifying and categorizing critical assets
2. Protection

- Access control
- Safeguarding data at use, rest, and in motion
- Configuration management, change management, incident management
- Vulnerability management

3. Detection
    - Incident and anomaly monitoring, detection, and evaluation
4. Countermeasures
    - Communication
    - Incident analysis
    - Isolation of incident and impact minimizing
5. Recovery
    - Testing the recovery plan in action

3.2 Structure of cyber exercise

Cyber security exercises involve a number of actors that plan, participate in, and manage the exercise. Therefore, exercises are often planned and carried out as projects (Wilhelmson & Svensson 2013, 9). European Network and Information Security Agency (2009, 16) divides exercises in their "Good practice guide for national exercises" into four parts: identifying, planning, conducting, and evaluating. As seen in Figure 2, the different states of the exercise can include many responsibilities for different actors/participants.

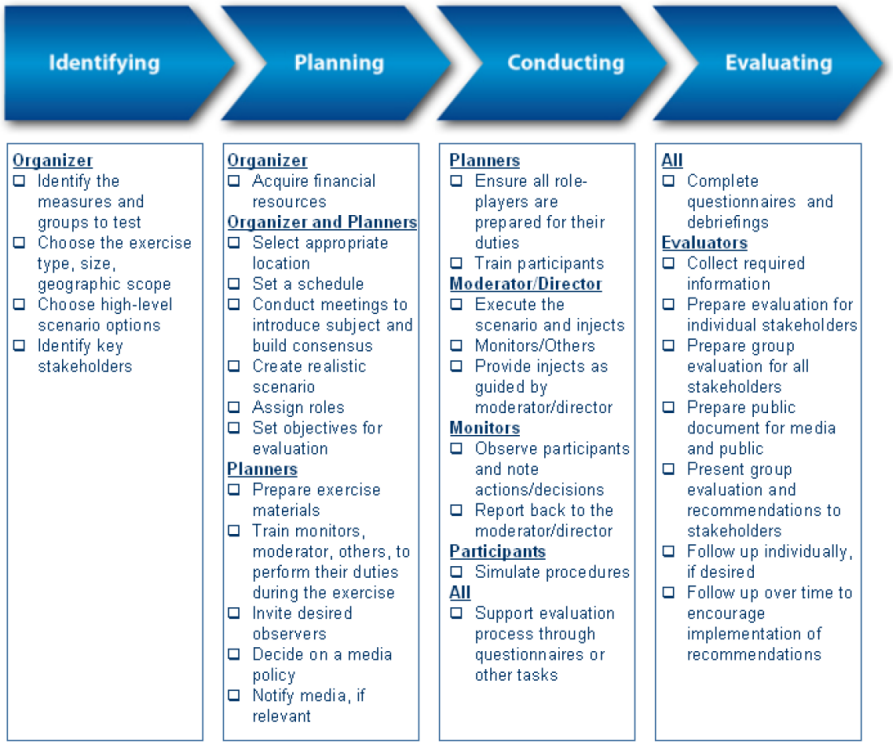

Figure 2. Lifecycle of an exercise (European Network and Security Agency 2009, 16)

The time frame for the lifecycle can vary from 1-2 months to 9-12 months. The different phases of the lifecycle depend on the objectives and forms of the exercise.

In the identifying and planning phase it is important to determine the purpose, limitations, and scope for the exercise. The planning process should be clearly formulated and have a timetable. However, before starting the actual planning of the exercise, the needs and reasons for having the exercise must be clearly formulated. The analysis should answer at least the following questions: (Wilhelmson & Svensson 2013, 15, 29)

- What should the exercise achieve? Overall purpose of the exercise
- Who should participate in exercise? The target group for the exercise with consideration for what the purpose and objectives of their participation are
- What should be exercised? Selecting the approach and content of the exercise
- When should the participants exercise?

- How should the participants exercise? Selecting the format and the practical approach for carrying out the exercise
- Where should the exercise be held?
- What resources are needed?

Defining clear and well scoped objectives for the exercise helps planning, conducting, and evaluating the process and results.

> *"Without clear objectives, planners cannot design a meaningful exercise. The objectives enable planners to clearly structure the scenarios within the exercise to determine if their organization possesses the capabilities necessary to operate successfully within a hostile cyber environment and defend against cyber threats. Different organizations have different guiding principles, tools, tactics, and procedures, which make it important to establish a baseline for each exercise."* – (King 2014, 4)

In the planning phase when the objectives and scope of the exercise are determined, the exercise specific needs for the technical environment also need to be specified. Often a specific scenario can require implemention of new features into the environment. The technical environment should be provided as a base setup with different network topologies, operating systems, application software, configurations, and user accounts (Sommerstad & Hallberg 2012, 3). How these elements are composed and implemented together with the base setup, will depend on the scenario and the purpose of the exercise.

The selected form of the exercise is based mainly on the defined objectives. Different forms of exercises can be roughly divided into three parts: Table top, functional, and hybrid/full live exercise. In the different exercises the participants are grouped usually as Blue Teams, Red Team(s), White Team, and Green Team members. Each of the teams might not be applicable in each type of exercise and grouping depends on the chosen scenarios and ways to conduct the exercise.

Table top exercise

Table top exercises have usually a small training audience and amount of participants which makes it easier to experiment cyber security exercises in organizations. A table top exercise should have well-defined objectives. The events and injects are pre-co-ordinated, often hypothetical, and written down. This type of approach to exercise helps organizations to train communications, processes, and decision making. Many organizations use table top exercises to establish relationships and share information with other organizations and partners. The aim of the table top exercises is to test the readiness of response capabilities and raise awareness. (King 2014, 9)

Functional exercise

Functional exercises enable organization's personnel responsible for operations and processes to verify their IT plans, processes, and their operational preparedness against modern threats and emergencies by performing their duties in a simulated operational environment. These type of exercises are often scenario-driven and include ready-made situations that are simulated during the exercise. (Grance, Nolan, Burke, Dudley, White & Good 2006, 5-1)

Functional exercises can also be called simulation or controlled environment exercises. These sorts of exercises are usually conducted in constructed and partly fictional environments where the infrastructure is built separately from the organization's production IT systems. (Wilhelmson & Svensson 2013, 33)

These types of simulated exercises are designed to exercise participants, procedures, and assets involved in one or more functional aspects of an IT plan. The participants should respond to the events which are conducted based on the scenario and act accordingly. Each event and situation needs to be carried out as if it were a real event. In these cases also the counterplay for participants' responses is needed. The counterplay acts as the outside world of the exercise, acting as in the role of various people and organizations with whom/which the participants may need to come in contact. Conducting these kinds of events and actions, the exercise plan needs to be produced carefully. The plan should include at least instructions to the participants, time

tables, event lists, and materials. A functional exercise provides high educational value for the participants and for those who are counterplaying. The exercises can have different complexity levels and scopes, from validating strictly specified aspects of organizations processes or assets to full-scale exercises that address all parts of the organization's functions. Therefore, the duration of the exercise can be from between several hours to several days. (Grance et al. 2006, 5-1; Wilhelmson & Svensson 2013, 33-34)

Hybrid/Full live exercise

Hybrid and full live exercises are based on real events to increase the realism. Hybrid exercises include elements from technical exercises and functional exercises that are brought together to make realistic events against pre-determined targets (i.e. assets, people, and data). These events are set by the exercise planning group and are usually defined in an events list. Full live exercises include an active adversary team which is called Red Team (RT). Red Team tries to discover vulnerabilities and weaknesses in systems, processes, and communication plans that would contribute to the training to the participants. Red Team counterplays the technical events against the participant technical staff with the guidance of the exercise's control team (usually labelled as White Team, WT). (King 2014, 10-11)

Today organizations depend on other organizations to operate and provide services for internal and external partners. Therefore, a full live exercise should include multiple organizations and interdependencies between the organizations. The exercise requires realworld events that would appear in real life. These sort of exercises are often difficult or risky to conduct in live environments which creates the need for a controlled and realistic environment for stimulating current business processes of the participating organizations. The realism of exercise event, injects, and participants' responses determines the success of the cyber security exercise. Planning the live cyber security exercise, planners must understand the types of threats the training audience would face in a day-to-day situation and then develop injects that will utilize those methods during the exercise. (King 2014, 10-11)

3.3 Technical environment

The technical environment of the cyber security exercises, often also called cyber range, is a controlled environment with systems, networks, services, and users generally isolated from live production networks. Such an environment can be physical or virtual; however, often it is a combination of the two. The hybrid model of using physical and virtual infrastructure allows a cost-effective and versatile platform for conducting different exercise scenarios. The exercise environment provides access to participants from any organizations withour depending on the participants' ability to provide their own equipment. (King 2014, 11-12)

The technical environment for cyber security exercises can be quite extensive depending on the purpose of the exercise and the selected method (exercise form and type). For small-scale and table top exercises it may be sufficient to provide infrastructure to control the exercise and deliver different events and injects to participants. In larger scale exercises such as the hybrid or full live simulation, the exercises require networks of interconnected systems and services to provide realistic and meaningful environment for selected exercise scenario. (Wilhelmson & Svensson 2013, 71)

The technical environment can provide excellent means to demonstrate different cyber security events and threats of an ICT environment to the training participants. The environment should be able to demonstrate desirable and undesirable features towards replicated and implemented critical services and assets. Such an environment should be easily reset and reconfigured to allow to replay opportunities and repeats of the events. Red Team (the adversaries or cyber attackers) should also have abilities to use their capabilities without disruption of real-world networks and systems. The exercise environment should enable different scenarios to train "what if" questions, discover vulnerabilities in systems or processes, or confirm that the existing architecture and procedures are adequate and should be further executed in the organization. (King 2014, 11-12)

Sometimes the exercise's technical environment may have unrealistic and artificial settings to which the participants would normally have access or would normally use. These sort of setbacks should be instructed to the training audience thoroughly. (King 2014, 11-12)

The exercise environment has to be as realistic as possible so the participants can adapt to it easily and do not fight against the exercise. A realistic environment can require a significant amount of labour, hardware, software, and expertise, therefore the realism is sometimes traded against costs. The exercise environment does not need to be one-to-one copy of the real life, but rather a scaled-down and controlled environment which has equivalences to real life. Also real life environments are built to be as resilient as possible and have as few as possible exposed vulnerabilities. The exercise environment should enable a possibility to conduct different attacks against planned and implemented known vulnerabilities. (Sommestad & Hallberg 2012, 3-4)

4 REQUIREMENTS FOR TECHNICAL ENVIRONMENT

4.1 Overview of requirements

The requirements for technical environment are divided into six major categories: general requirements, global world or the “Internet”, defending team requirements, threat actors’ requirements, exercise control, and traffic simulation: however, there are requirements that are initiated from other categories and references to another category.

The purpose is to define generalized model of requirements for the technical environment. The requirements are gathered from scientific publications and literature which cover cyber security exercises. Also other references are used to derive the requirements from normal operations or cyber attacks.

4.2 General requirements

Requirement 1.1: Technical environment should be isolated and controlled

The technical environment of cyber exercises should be isolated from production networks and the Internet to prevent misguided attacks outside of the exercise environment. The separation can be done in various ways, one should consider implementing at least IP level isolation to the environment. The technical environment should be isolated because in many countries running malicious code in live production networks is forbidden, therefore it is important to take care of the isolation of the environment. For example, in Finnish criminal code there is a law against a person who, in order to impede or cause harm to data processing or the functioning or security of data system or telecommunications has malicious or harmful software or devices in their possession or tries to interference with communications (Finlex, 2015b, Chapter 34 sections 9a and 9b). The Finnish Government has stated in their proposal HE 153/2006 (Finlex, 2015b) that the possession of a data system offence

device for the academic or scientific use is excluded. Finnish criminal code acts as an example of the precautions on the isolation that needs to be considered when using real attacks and attacking tools.

Requirement 1.2: Remote usage of the environment should be available

Nowadays the training should not be locked in a specific location. The users demand that they can access the training environment anywhere at any time. The environment's usage should be made as user-friendly as possible because some of the users in the exercises are other than IT personnel who might not have the technical skills to configure their systems for access.

Requirement 1.3: Airlock implementation for using certain real life services from the Internet

Many IT security devices and software are dependent on their access to a manufacturer's public services via Internet. Also, the need for updating threat knowledge and signature databases is easier with automated functionalities of the systems. However, one should consider also limiting the update levels of IT security devices and software on the same levels that the operating systems and applications are (see requirement 2.6). The need for this kind of limitation is often defined in the exercise's scenario or objectives.

Requirement 1.4: Airlock implementation for transferring files to isolated exercise environment

Exercise participants usually like to bring their own tools and files to the environment as a part of the exercise. This kind of controlled method to deliver these files should be implemented to the technical environment. Airlock implementation of files' transfer should be at minimum done at other than network layers to prevent any leakage of data outside of the environment.

Requirement 1.5: Use of virtualization and container virtualization to improve efficiency

Virtualization is a key technology to improve and enchance the computing in modern servers. The network functionality virtualization also brings more opportunities to implement different networking and security systems as virtual machines. The use of virtualization and NFVs gives administration of the technical environment possibilities to create even more complex and realistic IT environments for the exercises. The container virtualization can also help creating small virtualized systems with small resource needs by lowering overhead of virtual machines in hypervisors. Container virtualization is an approach to virtualization in which the virtualization layer runs as an application within the operating systems that can be virtualized in hypervisor level.

The use of virtualization and virtualized network devices does not exclude the need for the use of also physical devices interconnected to the virtualized resources. The technical environment should enable to connect physical devices to the technical resources.

Requirement 1.6: Network traffic capture should be possible from different parts of the technical environment

Koufil et al. (2014) have defined in Cloud-based testbed for simulation of cyber attacks study the need for network monitoring infrastructure which could be a set of probes, a data processing unit and a database. This sort of approach is enough for the analysis of the attacks, it is a single purpose solution. The technical environment of cyber security exercises' should also enable the possibility to capture network traffic in different parts of the technical environment for data analysis, and defending team's monitoring and detection purposes.

Requirement 1.7: The technical environment should have a modular structure

Modularity will give opportunity to develop different parts of the technical environment independently of others. The modular approach enable administration to bring

new features and functionalities as a part of the environment faster and more cost-effectively. The modularity is also a necessity to match the rapid development of the Internet and digitalization. The modular structure also enables the use of templates as a basis for building different exercise scenarios and exercise environments.

The selection of the scale of the modules can be done on many levels. The decision on the scale should be made by the technical environment's administration based on the extent of the environment and available resources on maintaining and further developing the environment. In the simplest manner the modules can be divided into "Internet", defending team environments, and threat actors' systems: however, often it is more reasonable to be more specific on dividing the environment. For example, the Internet can be divided into ISPs' routing core, global web services, and functionality services (e.g. DNS). One should also consider using modules on other parts of the environment to ease the development and implementations as a part the completeness of the environment.

4.3 Global world or the "Internet"

Global world or the "Internet" is needed for bringing realism as a key part of the environment. The realism is a vital part of cyber security exercises for participants to adapt the exercise's scenario and fully utilize their normal activities. The "Internet" also enables social and news media to be a part of the scenario. Nowadays, many cyber threats can harm organizations' public image and therefore it is necessary to also train participants to handle the media pressure or to provide necessary information for media representatives during the cyber attacks.

Many of the current attack vectors also use global Internet infrastructure to utilize the attacks or hide the sources of the attacks. More information on the requirements or references of cyber attacks is presented in chapter 4.5.

Requirement 2.1: Global ISP infrastructure for providing backbone of the "Internet".

The requirement includes a realistic set of different Internet Service Provider (ISP) networks and their real Autonomous System (AS) numbers as well as public IPv4 and IPv6 addresses. The backbone of the Internet should also have different transfer media and technologies which can be real systems or emulated ones. ISP infrastructure should have BGP routing implemented between different ISPs as realistically as possible. The BGP should be implemented with the use of RFC compliant BGP routers; thus any BGP related incidents can be trained during cyber security exercises. The interconnectivity between ISPs should be implemented in a manner which enables, for example BGP Man in the Middle attacks, covered in detail in section 4.5.2, and Cloud DDoS mitigation techniques which uses BGP as a method for traffic diversion.

Requirement 2.2: Global DNS and NTP infrastructure

The global "Internet" of the technical environment should include DNS infrastructure which has the same structures as the Internet's DNS infrastructure. DNS infrastructure should be implemented in the same hierarchical way as the real world counterpart. The hierarchy should include several root DNS servers, a comprehensive set of top level DNS (TLD) servers, and organization level authoritative DNS servers. The DNS servers should be located in a different parts of the technical environment's ISPs to represent the realistic distribution. DNS infrastructure should also include implemented DNSSEC features at least on root DNS server and on a set of TLD servers.

Time is an important factor when considering IT systems and their interoperation functions. The exercise environment should have a defined timing source, for example NTP which is made globally available inside the exercise environment. To ease the implementation of global timing source, NTP infrastructure should have the same functionalities as the real global NTP infrastructure has.

Requirement 2.3: Global certificate and/or PKI infrastructure

The certificates and public certificate infrastructure are the basis for the chain of trust in public networks and services. The certificates and encryption provide confidentiality, integrity, and authentication information of the service for the users. The technical environment should have a defined trusted root certificate authority which can delegate certificates to other certificate authorities. Once the global certificate authority chains have been implemented, the services using certificates as a part the encryption should have certificates signed by a global certificate authority infrastructure. This creates a realistic chain of trust for publicly available services that use certificates as a part the encryption process. The root certifications should be available in the technical environment and they should be deployed to the endpoints so end users would automatically see trusted services as trusted based on the issued certificates.

Requirement 2.4: Comprehensive set of public web services

The technical environment should have a comprehensive set of public web services that include at minimum social media, news sites, end user services, forums, and other services. The set of public web services should also include web sites which can be used as a part of cyber attacks or other activities by cyber criminals (e.g. underground forums, Pastebin like web site, and TOR web sites)

Requirement 2.5: Cloud services as part of global "Internet"

Cloud services can be understood as cloud computing services (i.e. which provides computing services from their data centers.) and cloud web services (i.e. which can include file storages, email services, social media services, instant messaging services, and collaboration services). The cloud services have global significance and provide a set of vital services for modern organizations.

From a technical point of view, cloud services are globally significant and should have data center locations in different parts of the global "Internet". The end users should

be directed to different data centers of cloud services based on their geolocation that is on other hand defined based on user's IP address.

Requirement 2.6: Operating systems' and application update repositories

The technical environment should have controlled update repositories for operating systems and application software. The ability to control the patch levels of operating systems and applications enables to conduct so called zero day attacks without owning knowledge about actual unpatched vulnerabilities. The update repositories can also be used to simulate critical patch availability and therefore exercise participants are able to exercise patch management on those situations.

Requirement 2.7: Social media sites and functionalities should be implemented as part of the technical environment

Social media is a key part of the Internet nowadays. Organizations use social media as a platform to release announcements and communicate to their customers. Social media is also a major part of spreading the news more quickly than traditional news media sites.

Hacktivists and other criminal organizations also use social media as a part of their operations and ways to make their causes more public. Anonymous is one of the best known hacktivist groups that are really active using social media (e.g. Twitter) to spread the threats against their targets.

Social media also enhance the real life like feeling of the exercises and brings the commonly used tools available for the participants.

Requirement 2.8: A set of news media sites should be implemented as part of the technical environment

News media are commonly used to create more real life pressure for the exercise's participants. News media sites should be used as publication platforms for announcing news about different events occurring during the exercise. The set of different news media sites should include real life like sites around the world to enable various scenarios for exercises. The media sites are also targets for organization's end-users who browse the public web services from their workstations.

4.4 Defending team requirements (Blue Teams)

Blue Team environments are either fictional enterprise environments or realistic copies of real enterprise environments. Blue team environment can be one or multiple sites that can include office environments, data centers, research environments, and/or production facilities (e.g. factories). Blue team environments usually include various systems for administrators and IT management as well as several business critical systems and services. The role of the end users of the organizations can not be forgotten because they can provide impulses or incidents that may or may not be part of a cyber incident.

Branlat, Morison and Woods (Branlat et al, 2011) have defined two interrelated goals for cyber defence. Blue teams need to maintain production while preventing attackers from gaining access, and from acting on the network (e.g. stealing or distrupting data, interfering the production processes). Participants of the blue team need to prevent illegitimate activities by mitigating potential vulnerabilities or attack surface and recovering from breaches when discovered. This definition of responsibilities of blue team creates the needs to have functional tools for monitoring and operating the IT infrastructure (covered in **Requirement 3.6**).

Branlat et al. (2011) have created blue team processes for interplaying against Red Team. The Blue Team process is presented in Figure 3.

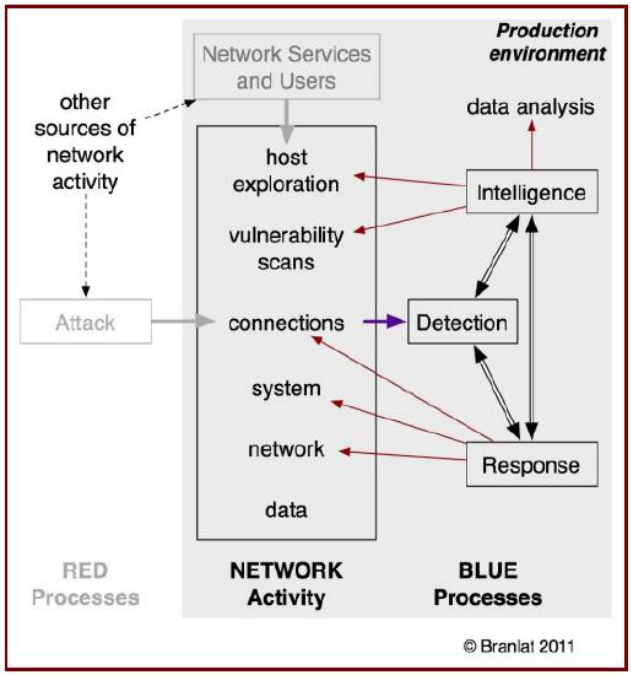

Figure 3. Blue Team interplay process (Branlat et al, 2011)

The Branlat et al. (2011) view of the necessary Blue Team processes lacks information about communication of a detected incident to the end users and 3rd parties (e.g. service providers, subcontractors, cooperation partners etc.). Hence the processes and tools for communicating to organization's employees and business partners need to be implemented as a crucial part of the exercise's technical environment so participants can be trained to handle the incidents as well as the communications (covered in **requirement 3.5**).

Patriciu and Furtuna (Partriciu & Furtuna, 2009) have defined a defence oriented approach for cyber exercises. Their approach is to study and practice the defence methods that can be used during cyber attacks. Patriciu and Furtuna (2009) have divided the cyber defence into the following actions:

- Create a security policy
- Implement the security state
- Monitor the security state
- Test your own security state
- Improve the security

The actions concerning operations of the Blue Teams create the requirements for different detection, monitoring, handling, and recovering the cyber incidents and attacks. These requirements for the operations of Blue Team are defined under **requirement 3.6**.

Patriciu and Furtuna (2009) also dictates that there are at least three ways to organize the exercise:

1. The participants receive the requirements and services they should provide and they must develop their own computer systems to provide them
2. The participants receive default installations for specific systems and services to provide and they must configure them in order to be protected
3. The participants receive already installed and configured systems and they must protect them. In this approach, the attacker can be the instructor or an external party

The first statement states that participants need to have a capability to build their own infrastructure as a part of the exercise's technical environment. This is stated in **requirement 3.1**.

Requirement 3.1: Participants should be able to build their own systems and services

The second statement of Patriciu and Furtuna (2009) can be considered as a ready-made blue team environment which would include different elements defined in **requirements 3.3 to 3.7**.

The third statement of Patriciu and Furtuna (2009) defines the need for ready-made blue team technical environments which can be put in to operation quickly and easily. These sorts of environments can be constructed as templates using e.g. virtualization templates of prepared systems and services.

Requirement 3.2: Providing ready-made blue team systems and services as templates

Patriciu and Furtuna (2009) have stated for potential targets of attacks as:

- Computer networks
- Public services
- Humans
- Trust relationships

The computer network targets need to be a part of the Blue Team environment which can include their internal services (either IT infrastructure services or IT services organization's employees), publicly available services (e.g. web services), and communication systems (either for internal or external communication). These targets generate the basis for the **requirements 2.7, 2.8, 3.3, 3.4, 3.5, and 3.8**.

Requirement 3.3: Internal infrastructure services

Blue Team's internal infrastructure represents core services which provide central user directory (e.g. Active Directory or LDAP), DNS services, NTP services, File services, internal web services and other internal services. These services are usually accessible only for organization's (Blue Team) users or staff.

Blue team internal services can be located in one network segment or they can be divided into several segments based on the objectives and scenario of the exercise.

Requirement 3.4: Public services provided by Blue Team

The Blue team environment should also include publicly available services which represent an organizations core public services. These services could include:

- Authoritative DNS servers and other DNS servers
- Email servers for transferring email

- Web based access to personnel's emails
- Publicly available web sites
- Mockup services to mimic real life services (e.g. e-commerce, online banking)

These kinds of services can be provided via data center segments of the Blue team's environment or by external service provider.

Requirement 3.5: Internal and external communication services

The users should have during exercises similar tools to use in communication that they use in real life. Their communication to organization's internal and external members should be created using services which are implemented either as a part of the organization's exercise environment or as a cloud service. These services should include at least the following: Email services, Voice over IP (VoIP), and instant messaging (for example cloud-based instant messaging, XMPP based chat or Microsoft Lync).

Requirement 3.6: Technical management tools for preventing, detecting, handling, and recovering from cyber incidents

These tools should include at least: Firewalls, central log server with log analysis tools, IDS/IPS systems, network and servers monitoring, incident handling and/or ticketing system, backups, Security incident events management (SIEM) systems, and network analysis tools. These are the tools that the Blue team's technical personnel (systems administrators, security staff, and network operators) use to manage the blue team's environment. The specific tools depend on the exercise's scenario, objectives, and participating personnel.

Silva et al. (2014) have found that the most successful participants of the exercises were the ones that combined their own specialized tools to commonly available and implemented tools, which generates **requirement 3.7**.

Requirement 3.7: Participants should be able to implement and integrate their own tools as part of the exercise environment

Users should be able to bring their own physical devices and implement virtualized systems as a part of the blue team's environment. The participants should also have an administrative access on blue team's systems to deploy their own tools as a part of the system. These sort of possibilities should be documented and instructed to participants.

Requirement 3.8: Services that simulate or mimic real life critical services for enterprises

The services that are business critical systems for enterprises need to be implemented either as a mockup or as an operational copy of the real service depending on the objectives of the exercise. The mockup services should be reusable templates which can be implemented easily into different enterprise environments.

4.5 Threat actors' requirements (Red Team)

4.5.1 Overview of Red teaming and adversaries in exercises

The Ministry of Defence of the United Kingdom (UK Ministry of Defence, 2013, 1-1) defines Red teaming process as a tool to reduce enterprises' risks. The expression "Red Team" among the military is often used to describe a way to think differently and to be able to anticipate and model adversarial behaviour (Brangetto, Caliskan & Roigas 2015, 6). UK Ministry of Defence (UK Ministry of Defence, 2013, 1-2) defines the broader concept of red teaming:

> *"A red team is a team that is formed with the objective of subjecting an organisation's plans, programmes, ideas and assumptions to rigorous analysis and challenge. Red teaming is the work performed by the red team in identifying and assessing, inter alia, assumptions, alternative options, vulnerabilities, limitations and risks for that organisation. Red*

> *teaming is a tool set. Using it will provide the end user (commander, leader, or manager) with a more robust baseline for decision making." - (UK Ministry of Defence, 2013, 1-2)*

Red Teams mimic the mind-set, actions, and operations of the attackers and adversaries to test an organization's cyber security capabilities. They use the tools that are commonly used in penetration testing and information security testing. (Brangetto et al. 2015, 4)

The use of Red team depends on the scope and needs. Red teams can be used to *(UK Ministry of Defence, 2013, 2-1 – 2-2):*

- Test and challenge assumptions and identify potentially faulty logic
- Assess the strength or the quality of information
- Identify alternative options or outcomes and/or explore the consequences of the actions
- Test a system, plan or perspective through the eyes of an adversary, outsider or competitor
- Understand the options available to adversaries

The nature of cyber events is fundamentally adversarial and therefore the interplay between Red team and Blue teams is important to understand. Branlat et al. (Branlat et al., 2011) explains the interplay from the Red team's perspective which is shown in Figure 4.

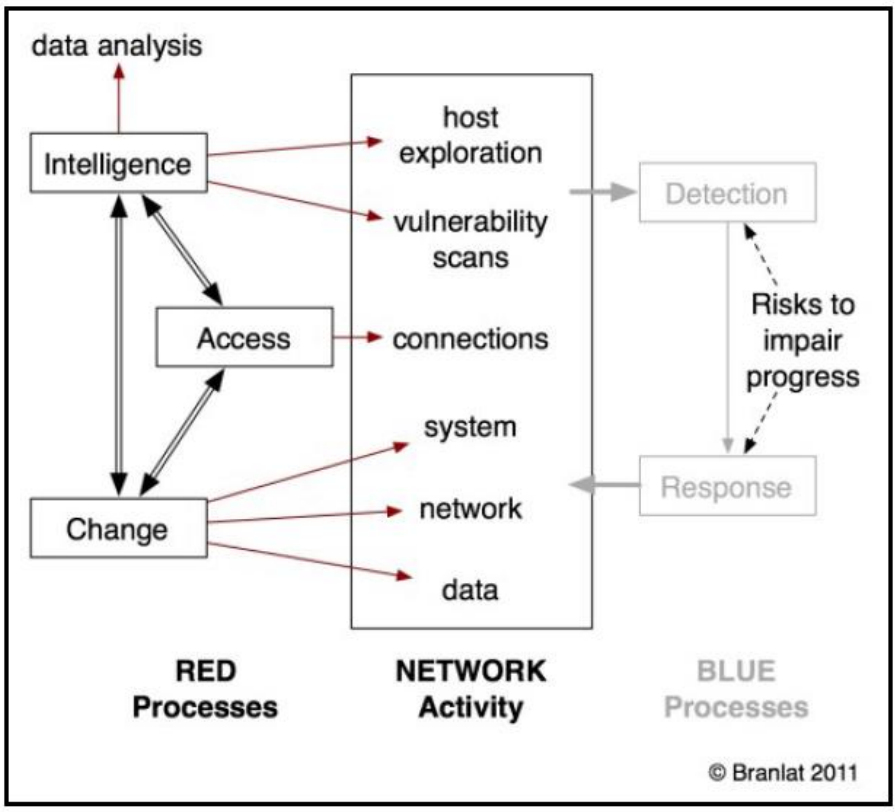

Figure 4. Red Team process (Branlat et al. 2011, 5)

The figure indicates the same functional tasks that the Red Team should perform during cyber security exercises as described earlier by UK Ministry of Defense and Brangetto et al. (2015).

Branlat et al. (2011) dictates for Red Team's goals to defame, perform reconnaissance, invade, and eventually break or destroy targets. This sort of approach determines different requirements for tools and possibilities for Red Team to perform various techniques and objectives in a technical manner as well.

Patriciu & Furtuna (2009) have defined offense oriented approach for cyber security exercises which can be perceived as Red teaming. They have stated that in order to perform real life cyber attack, the following steps should be performed:

- Reconnaissaince
- Scanning and enumeration

- Gain access or perform Denial of Service attack
- Escalation of privileges
- Maintain access
- Cover tracks and place backdoors

King (2014, 12) has listed samples of threats that can be executed in an exercise:

- Natural disaster
- Ignorant user
- Malicious internal user
- Network virus
- Network denial of service (DoS)
- Unauthorized computer on network
- Malicious internal scanning
- Computer compromise
- Frequency phishing via email

King (2014, 12) states that the list is not a comprehensive list of threats but is strives to give an idea what kind of threats can be executed in exercises.

The requirements of Red teaming are covered in the following paragraphs divided into attack categories.

4.5.2 Network attacks

Internal network attacks are a tool for adversaries to intercept users' traffic. In a local area network (LAN) segment one of the most common attack type is ARP (Address Resolution Protocol) spoofing. The ARP spoofing attack usually tries to cheat end user workstations to think that attacker's machine is the gateway for the LAN segment or imposing as an internal host. The attack is performed forging the IP address and the corresponding MAC address, and sending forget ARP packets to the network. The detection of ARP spoofing attack can be performed using real-time traffic analysis of the networks. (Hou, Jiang & Tian 2010)

The basic princible of ARP spoofing attack is illustrated in Figure 5.

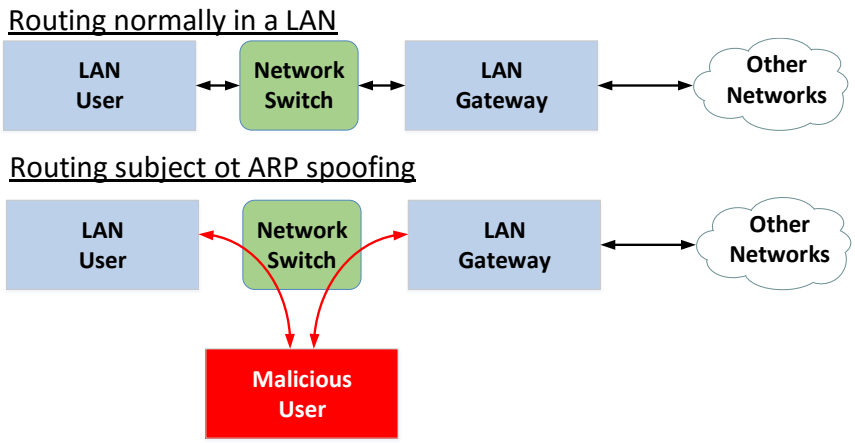

Figure 5. ARP spoofing attack

The demands for the traffic capture are defined in **requirement 1.6**.

The threats are not just directly targeted to organization's systems and networks. The data transferring between organization's physical locations (sites) and to public services can provide knowledge if accessed by adversaries. The attackers seek ways to intercept this kind of information remotely (mainly because of the cost-effectiveness) by hijacking network traffic globally to transfer through attacker's controlled systems. This kind of activity allows attackers either to disrupt, alter, or listen data transfers. This sort of attack vector is called Border Gateway Protocol (BGP) Man in the Middle (MitM) attack. BGP MitM utilizes the global Internet Service Provider (ISP) architectrure which consists of many different Autonomous System domains that control a certain set of public IPv4 and/or IPv6 address blocks. The attacker tries to re-route the target's public IP blocks on a different path and intercept the traffic with modified BGP updates of the target's IP address block. (Pilosov & Kapela 2008, 8-31)

BGP MitM attack vector has been used in the real life in many occasions (Cowie 2013; Madory 2015; Toonk 2015). Some of the incidents are not hostile but just mistakes that might happen when rerouting traffic for example to DDoS Cloud mitigation

service (Toonk 2015). As the threat of BGP MitM is real, it is important that the technical environment of cyber security exercises provides this kind of opportunity in exercise scenarios. The requirement is defined in **requirement 2.1.**

4.5.3 Distributed Denial of Service attacks

Akamai (Akamai 2015) has posted in their "State of the internet" knowledge center information on different kinds of Distributed Denial of Service attacks. The attacks imposing certain demands to technical environment are covered in this chapter.

Reflection DDoS attacks are attacks that sends floods of requests to third party-party servers which are not the target of the DDoS attack. The reflection attack uses the intended target's IP address as a spoofed source IP address to which the third-party servers (e.g. DNS servers) will direct the responses to the spoofed address which is the attacker's intended target. This kind of attack utilizes the characteristics of connectionless protocol UDP.

Requirement 4.1: Spoofing the source IP address should be possible at least on certain parts of the technical environment

NTP (Network Time Protocol) DDoS attacks are an example of reflection DDoS attacks which utilize globally available NTP servers to redirect the attack traffic. This defines the need to have globally available and possibly misconfigured NTP servers to enable this kind of attack vector. The requirement for NTP servers is defined in **requirement 2.2**.

DNS amplification and reflection attacks uses openly available resolving DNS servers to redirect and amplify the spoofed DNS query traffic. The amplification is performed using the fact that the query is often much smaller than the response. In many occasions attackers will use crafted DNS records so the responses would be even bigger than the normal responses for often used queries. (Zargar, Joshi & Tipper 2013, 3-4)

The crafted DNS record enables attacker to amplify the attack traffic up to 54 times the amount of query traffic (US Cert 2015). The elements of DNS DDoS traffic determine the need for DNS infrastructure to the technical environment which is defined in **requirement 2.2**.

The use of amplification attacks generates volumetric DDoS attacks, which means that the attacking traffic tries to overwhelm the target with excessive data flows. These sorts of attacks use as much bandwidth as possible. This kind of attack defines the requirement for the environment to handle excessive traffic flow to some extent.

Requirement 4.2: Technical environment's bandwidths should be scaled-down to create realistic setting for volumetric DDoS attack scenarios

Building the cyber security exercise to handle any level of volumetric attacks would be costly; however using scaled bandwidths in ISP networks and access networks, it is possible to create realistic volumetric DDoS attack scenarios.

4.5.4 Botnets and malware as an attack tools

A botnet is a group of infected computers, mobiles, and servers that are connected together through the Internet. A botnet has three main elements – the bots (i.e. computers, mobiles, and servers), command and control (C&C) servers, and the botmasters. The infected bot machine connects and makes end devices a part of a botnet without the machine owners' knowledge. The control of the bots and the botnet is under control of a malicious person, known as the botmaster who controls all the infected bots and sends orders to the entire botnet through the C&C servers. The aim of the botmaster is to carry out the malicious activities. (Eslahi, Salleh & Anuar 2012)

Eslahi et al. (2012) state that botnets go through the same stages in their lifecycle. Figure 6 shows the general view of a botnet lifecycle stated by Eslahi et al. (2012).

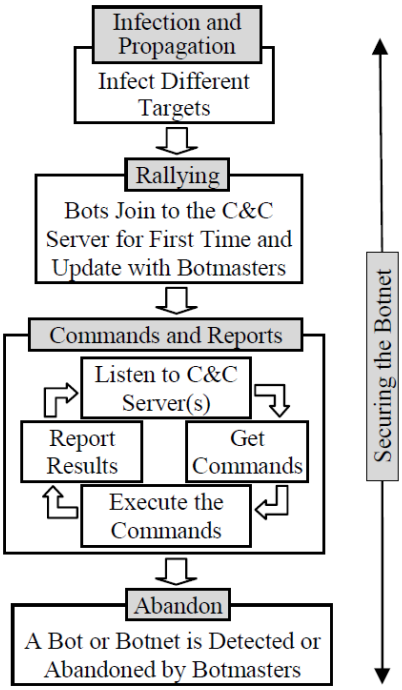

Figure 6. Botnets' lifecycle (Eslahi et al. 2012)

Gu, Zhang and Lee (Gu, Zhang & Lee 2008) state in their study on "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic" that a centralized C&C architecture can be categorized into "push" or "pull" style depending on how the botmaster's commands reach the bots. Figure 7 illustrates the differences of the two styles.

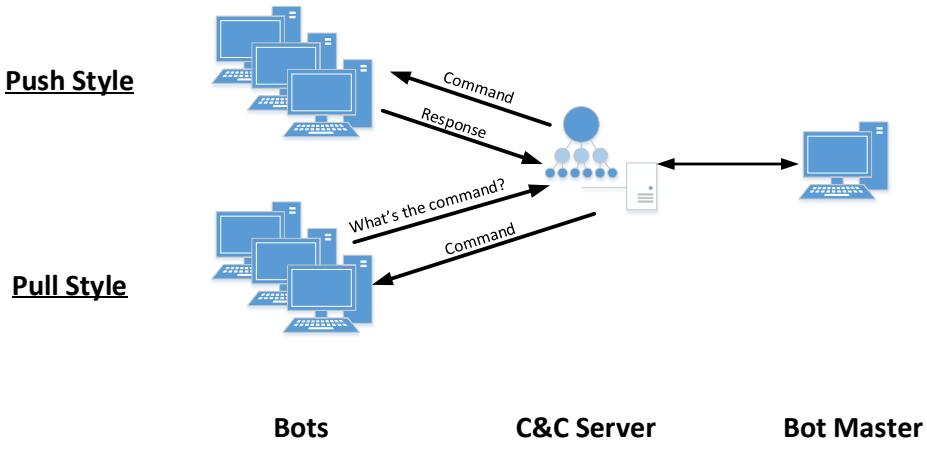

Figure 7. Botnet command and control styles

The botnet's use of style depends on the connectivity method. For example, in botnets that use Internet Relay Chat (IRC) protocol to connect bots to C&C server, the server initiates the conversations between the server and the bot (i.e. push style). However, when using HTTP, HTTPS, or DNS as the connectivity method, the bots initiate the conversation with the C&C server (i.e. Pull style).

The botnets are a common tool for cyber attackers when they scan networks, spread malware or conduct attacks against enterprises and organizations. Therefore it is necessary to have botnet functionalities in the technical environment of cyber security exercises. The environment should have a ready-made architecture of botnets that can gather information on targets, conduct attacks, and spread malware which generates **requirement 4.3**. The botnets also use of different command and control channel, which determines also **requirement 4.4**.

Requirement 4.3: Ready-made architecture of botnets that can gather information on targets, conduct attacks, and spread malware.

Malware is a term used to refer to a variety of forms of malicious, hostile or intrusive software (Moir 2003). Targeted attacks often use custom made malware to exploit known and unknown vulnerabilities of software. The initial exploitation is made by providing malicious content to the targeted organization using email phishing, USB, or other delivery mechanisms. The targeted attacks often uses unknown vulnerabilities of software as Kaspersky states in their Duqu 2.0 technical analysis report and F-secure states in The Dukes - 7 years of Russian cyberespionage report. The malware used in targeted attacks use various command and control channels (F-secure, 2015). Many of the C&C channels use a specific protocol to communicate with C&C server; however, also public services such as Twitter can also be used as communication channel (F-secure, 2015). These sorts of highly developed malware create a need to support various C&C channel protocols and services in the technical environment which is covered in **requirement 4.4**.

Requirement 4.4: Technical environment should provide possibility to use various command and control channels for controlling the botnets and/or malware

Botnets and malware that just use a certain protocol (e.g. HTTP, FTP) to deliver commands and data to C&C server do not create special requirements for technical environment; however, malware that use external services (e.g. social media, cloud storage) to deliver data does. This kind of activity creates the need for **requirement 2.5, 2.7, and 2.8**.

The external services also include DNS architecture which is used in many malicious software to deliver data using DNS queries and responses. These kind of malware use domain generation algorithms and rapidly changing domain names for C&C server communication as stated by Schiavoni et al. 2014 in their study on "Phoenix: DGA-based botnet tracking and intelligence" and stated by Antonakakis et al 2012 in their study on "From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware". This sort of functionality creates the need for **requirement 2.2**.

4.5.5 Social engineering attacks

Social engineering is a set of techniques used to deceive victims to expose confidential information or performing actions. These sort of attacks are non-technical intrusions that utilize human interactions and aim to bypass technological security mechanisms. The social engineering attackers can use various technical and non-technical means to conduct social engineering, such as, phishing, online social engineering, shoulder surfing, and pretexting. (Luo, Brody, Seazzu & Burd 2011, 1-4)

Considering cyber security exercises, pretexting, phishing, and online social engineering are the most likely scenarios to use in exercises. Phishing in particular is often used as a part of Red Team campaign to gain information by sending a masqueraded e-mail that looks like it has orginated from a legitimate source (e.g. bank or credit card company requesting verification, or internal organizations). Pretexting can be

used to impersonate co-workers, authorities or 3rd party contractors whose information might be completely fake; however, it has realistic services for so called call-back checks.

Social engineering attacks can be very difficult to execute successfully in fictional scenario which determines the needs for realism when conducting social engineering techniques. The realism can be realistic e-mails, pretext company web sites, and operational social media services. These requirements are covered in **requirements 2.4, 2.7 and 3.5**.

4.5.6 Watering hole and drive-by attacks

Watering hole attacks use exploited web servers to spread malware to a web site's users. The exploiting of the web servers is usually done through one of the following two methods:

- Web site's server or web application has a vulnerability that the attacker can exploit directly from the Internet
- Attackers gain access via victim's internal networks to get access and control of the web server. Once they have the control, the attackers can configure the site to spread malware to web site's users

The exploitation of the unsuspecting users often utilizes users' outdated software (e.g. web browser or operating system). Watering hole is often associated with the term malvertising which means that the web server spreading the malware itself has not been compromised but the malware is delivered through advertising feeds that are displayed on the web page alongside the victim's content. (Donaldson, Siegel, Williams & Aslam 2015, 282)

The malvertising attack vector, in particular, determines needs to have public web sites accessible by anyone using the exercise's Internet (see **requirement 2.7 and 2.8**). The news media and social media sites usually uses advertisements on their pages, which creates the **requirement 4.5**.

Requirement 4.5: Technical environment's Internet should have an advertising network which can be used to provide advertisements to different web sites

4.6 Exercise control requirements (White team)

4.6.1 Scenario and events handling

Requirement 5.1: The exercises should have web based service for handling the exercise's scenario and the events

Cyber security exercises are conducted with the help of exercise event lists and workflows. The different events will be played out as injects which can be provided to participant teams either as play cards or via technical systems (e.g. emails, VoIP calls). The exercise's control personnel should have centralized web services for controlling the exercise and delivering the different injects for participants.

Koufil et al. 2014 have defined in their study of Cloud-based testbed for simulation of cyber attacks that the environment should include scenario management and configuration systems for controlling the events. The scenario management node in their study is defined to control the environment; however, it is also necessary to provide systems for handling and controlling the actual flow of events and information to participants.

4.6.2 Reporting to exercise management

The exercise's control should be aware of the events detected and actions done in participating teams. The use of specified and formalized reporting about team's actions should be implemented as a part of the technical environment. The reporting is also important for evaluating the actions after the exercise.

Requirement 5.2: Participants should be able to report their actions to exercise's control personnel

4.6.3 Situational awareness of the exercise

Controlling cyber security exercises is essential to ensure that the exercise is conducted according to the scenario and the objectives are met.

Requirement 5.3: The exercise's control should have situational awareness of the exercise provided from technical environment

During the exercises a defending team member (blue teams) should be able to maintain situational awareness of their infrastructure and services. The technical environment should enable the possibility to test simultaneously various systems for providing situational awareness.

Requirement 5.4: The technical environment should enable opportunity to exercise situational awareness during the cyber incidents

4.7 User and Traffic simulation

4.7.1 Overview of user and traffic simulations

Branlat et al. (2011) states the needs for traffic simulations as a part of the exercises. The participants of the blue teams have to make sure they can separate legitimate and illegitimate traffic. When IT administrations of the servers, security, and networks systems are faced with high amounts of activity, they need to distinguish valid traffic from attack traffic. The traffic simulation needs to have distinguishable characteristics of network traffic (type, source, destination, content, volume).

Chen, Zhang and Urvoy-Keller (Chen, Zhang & Urvoy-Keller, 2014) have made an analysis of the modern mid-sized enterprise's traffic profiles. They have focused on profiling different characteristics of 24-hour data capture and have measured volumes, ratios of internal and external traffic, and the amount of local hosts in the captured flows. This sort of study gives a good idea how the traffic simulation variables

needs to be considered to provide realistic traffic profiles and contents for cyber security exercises.

The definition of different traffic profiles however is out of the scope of this thesis, whereas the requirements considering the need and generalized contents for traffic simulation for the exercise environment are discussed in this section.

4.7.2 Simulation of Internet users

The global world ("Internet") should have a great number of simulated end users who can generate different traffic profiles and patterns. The automated traffic should be made as realistic as possible. At least the following traffic profiles/protocols should be generated:

- Web browsing
- Email conversations
- Instant messaging
- Social media simulation

The simulation of Internet based users is used to generate valid end user traffic towards the exercise's Blue Teams and their services if the Blue Team is providing public services in the exercise's scenario. The automated system should support variation of traffic generation meaning that the sources appear as unique users and their activity should be able to randomize or made constant.

Requirement 6.1: Internet based end users should be simulated with an automated system

4.7.3 Simulation of organization's internal users

The organization's internal users (inside the Blue Team environments) should be simulated with an automatic system. The user simulation should generate various traffic profiles that are common in enterprises.

Requirement 6.2: Blue Team based end users should be simulated with an automated system

Internal users that are located in a Blue Team environment should be automated for simulating general activities of normal users within the organization. At least the following activities/traffic profiles/protocols should be generated:

- User logins to internal systems
- Web browsing to internal and external networks
- Usage of non web-based services within the organization
- Access to file storages and other infrastructure services (e.g. DNS servers and NTP servers)
- Incidents for the organization's IT administration

The automated system should support variation of traffic generation meaning that the sources appear as unique users and their activity should be able to be randomized or made constant.

4.7.4 Background noise traffic

Various kind of non-user traffic (also called white noise) occurs on the Internet generated by scanners, web crawlers, abusive systems etc. The technical environment should have an automated system to generate these kinds of traffic patterns to create a realistic "smoke screen" for normal end user and cyber attacks.

This kind of background noise traffic should include:

- Port scanning to UDP and TCP ports
- Low level DDoS attacks
- Traffic with broken protocol implementation (i.e. traffic not matching standards, invalid header options in TCP headers for example)
- Brute force logins to different authentication systems (i.e. SSH and HTTP)
- DNS queries

The automated system should support variation of traffic generation meaning that the sources appear as unique and their activity should be able to be randomized or made constant.

Requirement 6.3: Background noise traffic should be generated with an automated system

5 CONCLUSIONS

Cyber security exercise is a tool for organizations to test their critical capabilities and find out how they integrate personnel, processes, and technology to protect their critical information, services, and assets against modern cyber threats. Regular exercises can be integrated in the organization's cyber security strategy, which also enables an organization to experiment and further develop their capabilities on handling cyber security incidents and events.

Cyber security exercises can have many forms and scopes which creates many demands for the technical environment. The exercises can have multiple organizations at the same and their interdependencies often act as a critical part of an exercise's scenario which needs to be implemented in a technical manner as well. Conducting these kinds of exercises is a challenge for the technical environment which is used as a platform for exercises. The technical environment should be flexible, feature rich, and have real life counterparts of many technologies in order to conduct realistic cyber threats and defence methods. The digitalization and new technologies require agile and rapid changes to the technical environment which can be encompassed with modular structure and use of virtualization even though many technologies also still need physical elements and devices to operate, which is critical to take into account when the planning and constructing the technical environment for cyber security exercises start.

The goal for the thesis was to find generalized requirements for different elements of the technical environment. The used research method was inductive and qualitative and the used references were mainly scientific publications of cyber security exercises or cyber threat testbeds; however, handbooks and best practice guides were also used. The major challenge was to find distinctive requirements for the technical environment mainly because many of the publications focus on conducting, controlling, and managing the cyber security exercises. They often ignore the important role of the technical environment as a part of conducting different kinds of exercises.

This kind of research method helped to find and define the most common requirements for the technical environment; however, it was crucial to use knowledge of normal IT environments, procedures, and cyber attacks to create additional requirements. The restriction of inductive research method in this matter was the lack of publications of requirements. Many of the requirements needed to be derived from real life counterparts either by using other references and the author's own knowledge and experience on conducting cyber security exercises and developing technical environment.

The requirements consist of 35 separate claims that should be considered when implementing a versatile and multi-purpose exercise environment. The list of the requirements is a general reference for constructing and developing technical environment for cyber security exercises. The requirements are kept on a generalized level mainly because the goal was not to define only one purpose requirement specification but to work as a guideline. Also, available resources, physical infrastructure, licenses, and personnel are crucial factors when deciding on what level the environment is possible to be constructed and maintained. Depending on these factors, it is possible to implement a technical environment on many levels.

The overall view of the research can be considered as a first level of requirements for a technical environment. In the future, as technologies develop and digitalization becomes a more integrated part of life, the technical environment for cyber security exercises needs to evolve to encompass new requirements and needs to exercise organizations and personnel in the cyber domain. The gathered requirements do not cover all the aspects of cyber domain because of the lack of research of the area. The further research should consider looking into challenges that the organizations are facing nowadays or in the future. Upcoming researches on creating requirements for technical environment of cyber security exercises should focus on integrating mobile, Internet of Things (IOT), Industrial control systems (ICS), and physical elements as a part of the environment and exercise scenarios.

REFERENCES

Akamai. 2015. Types of DDOS attacks: An explanation of many types of DDoS attacks. Accessed on 3 September 2015. Retrieved from https://www.stateoftheinternet.com/faq-types-of-ddos-attacks.html

Antonakakis, M., Perdisci, R., Nadji, Y., Vasiloglou, N., Abu-Nimeh, S., Lee, W., Dagon, D. 2012. From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware. USENIX Security Symposium 2012.

Branlat, M., Morison, A., Woods, D. 2011. Challenges in managing uncertainty during cyber events: Lessons from the staged-world study of a large-scale adversarial cyber security exercise. The Ohio State University.

Brangetto, P., Caliskan, E., Roigas, H. 2015. Cyber Red Teaming. NATO Cooperative Cyber Defence Centre of Excellence CCDCOE.

Burney, A. 2008. Inductive & deductive research approach. Accessed on 21 August 2015. Retrieved from http://www.drburney.net/INDUCTIVE%20&%20DEDUCTIVE%20RESEARCH%20APPROACH%2006032008.pdf

Chen, J., Zhang, W., Urvoy-Keller, G. 2014. Traffic Profiling for Modern Enterprise Networks: A Case Study. 2014 IEEE 20th International Workshop.

Conklin, A., White, B. 2006. E-Government and Cyber Security: The Role of Cyber Security Exercises. 39th Hawaii International Conference on Systems Sciences.

Cowie, J. 2013. The New Threat: Targeted Internet Traffic Misdirection. Accessed on 4 September 2015. Retrieved from http://research.dyn.com/2013/11/mitm-internet-hijacking/

Donaldson, S., Siegel, S., Williams, C., Aslam, A. 2015. Enterprise cybersecurity. Apress.

Enisa - European Network and Information Security Agency. 2009. Good Practice Guide on National Exercises.

Eslahi, M., Salleh, R., Anuar, N. 2012. Bots and Botnets: An overview of characteristics, detection and challenges. Control System, Computing and Engineering (ICCSCE), 2012 IEEE International Conference.

F-secure. 2015. The Dukes – 7 years of Russian cyberespionage. Accessed on 11 October 2015. Retrieved from https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

Finlex. 2015a. Hallituksen esitys Eduskunnalle Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen hyväksymisestä, laiksi sen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta sekä laeiksi rikoslain, pakkokeinolain 4 luvun, esitutkintalain 27 ja 28 §:n ja kansainvälisestä oikeusavusta rikosasioissa annetun lain 15 ja 23 §:n muuttamisesta. Accessed on 19 October 2015. Retrieved from https://www.finlex.fi/fi/esitykset/he/2006/20060153

Finlex. 2015b. The Criminal Code of Finland (39/1889, amendments up to 927/2012 included). Accessed on 19 October 2015. Retrieved from https://www.finlex.fi/en/laki/kaannokset/1889/en18890039.pdf

Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., Good, T. 2006. Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. National Institute of Standards and Technology (NIST) – TechnologyAdministration U.S. Department of Commerce

Gu, G., Zhang, J., Lee, W. 2008. BotSniffer: Detecting botnet command and control channels in network traffic.

Hou, X., Jiang, Z., Tian, X. 2010. The detection and prevention for ARP spoofing based on Snort. 2010 International Conference on Computer Application and System Model-ing (ICCASM 2010).

JYVSECTEC – Jyväskylä Security Technology. 2015a. JYVSECTEC's web site. Accessed on 21 August 2015. Retrived from http://www.jyvsectec.fi/en

JYVSECTEC – Jyväskylä Security Tecnhonoly. 2015b. Internal document about cyber security exercises.

Kaspersky. 2015. The Duqu 2.0 - Technical Details. Accessed on 11 October 2015. Retrieved from https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

Kick, J. 2014. Cyber Exercise Playbook. The Mitre Corporation.

Koufil, D., Rebok, T., Jirsík, T., Cegan, J., Drasar, M., Vizvary, M., Vykopal, J. 2014. Cloud-based Testbed for Simulation of Cyber Attacks. IEEE Network Operations and Management Symposium (NOMS).

Luo, X., Brody, R., Seazzu, A., Burd, S. 2011. Social Engineering: The Neglected Human Factor for Information Security Management.

Madory, D. 2015. UK traffic diverted through Ukraine. Accessed on 4 September 2015. Retrieved from http://research.dyn.com/2015/03/uk-traffic-diverted-ukraine/

Patriciu, V-V., Furtuna, A. 2009. Guide for Designing Cyber Security Exercises. World Scientific and Engineering Academy and Society (WSEAS).

Pilosov, A., Kapela, T. 2008. Stealing The Internet: An Internet-Scale Man In The Middle Attack. Defcon 16 2008.

Saunders, M., Lewis, P., Thornhill, A. 2009. Research methods for Business Students. 5th edition. Pearson Education.

Schiavoni, S., Maggi, F., Cavallaro, L., Zanero, S. 2014. Phoenix: DGA-based botnet tracking and intelligence. In Detection of Intrusions and Malware, and Vulnerability Assessment. Springer International Publishing.

Secretariat of the Security Committee, 2013. Finland's Cyber security strategy and the background dossier. Accessed on 25 August 2015. Retrieved from http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

Silva, A., McClain, J., Reed, T., Anderson, B., Nauer, K., Abbott, R., Forsythe, C. 2014. Factors Impacting Performance in Competitive Cyber Exercises. Interserv-ice/Interagency Training, Simulation and Education Conference.

Solms, R., Niekerk, J. 2013. From information security to cyber security. Article published in Computers & Security 38 (2013).

Sommerstad, T., Hallberg, J. 2011. Cyber security exercises and competitions as a platform for cyber security experiments. Springer Berlin Heidelberg.

The International Telecommunications Union. 2015. Definition of cybersecurity. Accessed on 3 September 2015. Retrieved from http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Toonk, A. 2015. BGP routing incidents in 2014, malicious or not. Accessed on 4 September 2015. Retrieved from http://www.bgpmon.net/bgp-routing-incidents-in-2014-malicious-or-not/

UK Ministry of Defence. 2013. Red Teaming Guide. 2nd Edition. Development, Concepts and Doctrine Centre. Accessed on 3 September 2015. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/142533/20130301_red_teaming_ed2.pdf

US-CERT. 2015. UDP-based Amplification attacks. Accessed on 3 September 2015. Retrieved from https://www.us-cert.gov/ncas/alerts/TA14-017A

Wilhelmson, N., Svensson, T., 2013. Handbook for planning, running, and evaluating information technology and cyber security exercises. The Swedish National Defence College.

Zargar, S., Joshi, J., Tipper, D. 2013. A Survey of Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE COMMUNICATIONS SURVEYS & TUTORIALS.

APPENDIX I: COMPLETE LIST OF REQUIREMENTS

GENERAL REQUIREMENTS:	
Requirement 1.1:	Technical environment should be isolated and controlled
Requirement 1.2:	Remote usage of the environment should be available
Requirement 1.3:	Airlock implementation for using certain real life services from Internet
Requirement 1.4:	Airlock implementation for transferring files to isolated exer-cise environment
Requirement 1.5:	Use of virtualization and container virtualization to improve effi-ciency
Requirement 1.6:	Network traffic capture should be possible from different parts of the technical environment
Requirement 1.7:	The technical environment should have a modular structure

GLOBAL WORLD OR THE "INTERNET":	
Requirement 2.1:	Global ISP infrastructure for providing backbone of “Internet”.
Requirement 2.2:	Global DNS and NTP infrastructure
Requirement 2.3:	Global certificate and/or PKI infrastructure
Requirement 2.4:	Comprehensive set of public web services
Requirement 2.5:	Cloud services as part of global “Internet”
Requirement 2.6:	Operating systems’ and application update repositories
Requirement 2.7:	Social media sites and functionalities should be implemented as part of the technical environment
Requirement 2.8:	A set of news media sites should be implemented as part of the technical environment

DEFENDING TEAM REQUIREMENTS:	
Requirement 3.1:	Participants should be able to build their own systems and services
Requirement 3.2:	Providing ready-made blue team systems and services as templates
Requirement 3.3:	Internal infrastructure services
Requirement 3.4:	Public services provided by Blue Team
Requirement 3.5:	Internal and external communication services
Requirement 3.6:	Technical management tools for preventing, detecting, handling, and recovering from cyber incidents
Requirement 3.7:	Participants should be able to implement and integrate their own tools as part of the exercise environment
Requirement 3.8:	Services that simulate or mimic real life critical services for enterprises

THREAT ACTORS' REQUIREMENTS:	
Requirement 4.1:	Spoofing the source IP address should be possible at least on certain parts of the technical environment
Requirement 4.2:	Technical environment's bandwidths should be scaled-down to create realistic setting for volumetric DDoS attack scenarios
Requirement 4.3:	Ready-made architecture of botnets that can gather information on targets, conduct attacks, and spread malware.
Requirement 4.4:	Technical environment should provide possibility to use various command and control channels for controlling the botnets and/or malware
Requirement 4.5:	Technical environment's Internet should have an advertising network which can be used to provide ads to different web sites

EXERCISE CONTROL REQUIREMENTS:	
Requirement 5.1:	The exercises should have web based service for handling the exercise's scenario and the events
Requirement 5.2:	Participants should be able to report their actions to exercise's control personnel
Requirement 5.3:	The exercise's control should have situational awareness of the exercise provided from technical environment
Requirement 5.4:	The technical environment should enable opportunity to exercise situational awareness during the cyber incidents

USER/TRAFFIC SIMULATION REQUIREMENTS:	
Requirement 6.1:	Internet based end users should be simulated with an automated system
Requirement 6.2:	Blue team based end users should be simulated with an automated system
Requirement 6.3:	Background noise traffic should be generated with an automated system