TALLINN UNIVERSITY OF TECHNOLOGY

Faculty of Information Technology

Department of Computer Engineering

ITC70LT

Ferenc Szalai 144934IVCM

DOES CYBER SECURITY EXERCISE INFORMATION SHARING WORK?

Review and analysis of technical cyber security exercises and their information sharing

Master thesis

Supervisor: Olaf Manuel Maennel

Ph.D. (Dr.rer.nat.)

Professor

Tallinn 2016

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Ferenc Szalai

19.05.2016

Abstract

This thesis focuses on the analysis of cyber security exercises and their information sharing. Cyber security exercises are primarily organised to train participants through practice or to offer a competence contest. To gain understanding about how the exercise's information sharing works and how it affects team effectiveness in cyber security exercises, this thesis gathers a dataset consisting of over 120 exercises and reviewing literature, such as studies on cyber exercises and cyber exercises after-action reports. The dataset is used to describe the evolution of exercises and exercise types including the considerations of building a cyber security exercise. Statistical analysis is carried out on the dataset to identify the main patterns of development and information sharing. Additionally, a method is created and tested that identifies key exercise preparation indicators in technical cyber exercises. In 2016 three technical cyber security exercises were used to test the identified indicators and distinguish the information sources for preparation. The thesis indicates the positive effects of technical exercises on being successful in technical competitions, and identifies the key sources information that participants used to prepare for the exercises. The results of this thesis can be used to enhance the effectiveness of information sharing.

This thesis is written in English and is 63 pages long, including 5 chapters, 20 figures and 5 tables.

Annotatsioon

Informatsiooni jagamise tähtsus küberturbe õppustel

Tehniliste küberõppuste analüüs ja info jagamise printsiipide ülevaade

Käesolev magistritöö keskendub küberkaitse harjutustele ja neis toimuvale informatsiooni jagamise analüüsile. Küberkaitse harjutused on peamiselt läbiviidud selleks, et läbi praktika õpetada osalisi ning pakkuda teadmiste võistlust. Selleks, et mõista kuidas informatsiooni jagamine harjutustel töötab ja kuidas see küberkaitse harjutuse kestel mõjutab meeskonna efektiivsust, on magistritöö jaoks kogutud andmestik üle 120 harjutuse ja kirjanduse nagu küberharjutuste uuringud ja küberharjutuste pärast tegevuse aruannet. Andmestikku on kasutatud selleks, et kirjeldada harjutuste ja harjutuste liikide arengut ning vaadata läbi küberkaitse harjutuste loomine. Selleks, et identifitseerida peamisi arengu ja informatsiooni jagamise mustreid, on andmestiku töötlemiseks läbiviidud statistiline analüüs. Lisaks on loodud ja testitud meetod, mis tehnilistes küberkaitse õppustel identifitseerib peamised harjutuste valmistamise indikaatorid. Selleks, et testida leitud indikaatoreid ja eristada valmistumiseks vajalikke informatsiooni allikaid, kasutati 2016 aastal kolme tehnilist küberkaitse õppust. Et olla edukas tehnilistel võistlustel, osutab lõputöö tehniliste harjutuste positiivsele mõjule ning leiab võtme allikad, mida osalejad kasutasid harjutuste ettevalmistumiseks. Lõputöö tulemusi saab kasutada selleks, et tõsta informatsiooni jagamise efektiivsust.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 63 leheküljel, 5 peatükki, 20 joonist ja 5 tabelit.

Table of Abbreviations and Terms

BT	Blue Team
CTF	Capture the Flag
ENISA	European Union Agency for Network and Information Security
EU	European Union
GT	Green Team
INCIBE	Spanish National Cybersecurity Institute
ISO	International Standardisation Organisation
IT	Information Technology
LS	Locked Shields
NATO CCD COE	NATO Cooperative Cyber Defence Centre of Excellence
NIS Directive	Network and Information Security Directive
PISA	Programme for International Student Assessment
PLC	Programmable Logic Controller
ROE	Rules of Engagement
RRT	Rapid Reaction Team
RT	Red Team
UNESCO	United Nations Educational, Scientific and Cultural Organization
VM	Virtual Machine
VPN	Virtual Private Network
XS	Crosses Swords

Table of Contents

List of Figures

List of Tables

1. Introduction

Since Cyber Security became a security buzzword, the number of Cyber Security courses, exercises and competitions is continuously increasing. They are offered by different Universities, public and private organisations and learning websites. A well-educated cyber security professional is crucial for an organisation. During the last decade's financial crisis, companies recognised the importance of IT investment and understood that they could still grow and be more efficient by investing in IT. There is significant growth in high-tech employment and one of the best performing countries in Europe is Estonia with 5.2% [1] growth. To keep up with the latest changes companies would like to have well-trained IT security experts with deep and flexible knowledge who can react to security challenges in the sector. Security professionals and students learn more effectively and efficiently [2] when they need to solve a problem. Using this concept, the number of practical training courses and hands-on exercises offered by different organisations are continuously increasing and gamification has also begun trending as a topic [3], [4].

Security exercises, technical workshops and university programs offer an environment to extend knowledge through practice. Universities and organisations are developing their own exercises [5], training environments [6] and training objectives. With this individual experimentation, a lot of knowledge is developed within an organisation regarding exercise planning, development, and execution. However, little of this knowledge has been shared and validated [7].

1.1. Hypotheses

The problem addressed was the lack of information about these exercises and about exercise information sharing. While the numbers of national and international cyber security exercises are growing each year, the gathered knowledge and experience does not show a similar pattern. This exercise information would contribute to the future development of exercises and the skill development of participating individuals who would be better prepared for everyday challenges.

Three hypotheses are tested in the thesis:

1) The number and complexity of cyber exercises are growing.
2) The existing information sharing patterns are used only to share pieces of information.
3) There are key indicators to prepare for technical exercises.

The experiment used to test hypothesises was the following. Online available exercise information was collected and a survey was conducted to maximise the dataset of exercise information available for analysis. Exercise studies were also used to support the analysis. These information sources are used in statistical analysis to identify trends and patterns. In the last part of this thesis, exercise preparation key success indicators are identified and tested through technical cyber security exercises by collecting survey information from exercise participants, by using a scoring system during the exercise and by interviewing exercise planners.

There were limitations to the research, some of which could be controlled while others needed to be accepted. The first limitation was the source of exercise information. The security incident and procedure information is confidential in some cases [8] and there are also economic reasons to keep it confidential [9]. This limits the availability of relevant data. The other issue is the limitation of interview and survey answers which interpret the subjective opinion of the participant about the best information source they use for preparation. To address this limitation, the survey questionnaire includes exercise performance indicators of the participants to weight their answers. Consequently, the effectiveness of their information source can be measured using this method.

Given this context, the contributions of this thesis are:

- Identification of the patterns of information sharing in the technical exercises, including ‘new exercise’ development.
- A statistical summary of existing technical exercises, including post-exercise information sharing.

- Development of new supplementary model to the existing exercise classification model.
- Identification of key indicators to prepare for technical exercises.
- A test of the key exercise preparation indicators through technical exercises.
- Identification of the possible future developments of information sharing patterns.

1.2. Outline

Chapter 1 provides information on the hypothesis and background of the thesis.

Chapter 2 presents an overview of related work.

Chapter 3 presents an overview of exercises, their information sharing and a statistical analysis of exercises.

Chapter 4 presents an analysis of the effectiveness of existing information sharing methods.

2. Overview of related work

2.1. Role of exercises in cyber security

There is an extensive amount of related work in cyber security education, which includes individual and collective trainings, awareness trainings and information assurance curricula. Each and every stakeholder has their own understanding about the best way to prepare cyber knowledge and develop individual knowledge. Furthermore, each and every nation has its own system to provide the best curricula. The curricula should provide high standards as well as creativity. In the IT field, teaching pure facts could never be efficient, because of the ever-changing environment. The curricula in IT security should provide the main principles and standards, but at the same time it should avoid teaching too many facts. Besides, it is also very important to teach flexibility and creativity and provide hands-on experience to be able to respond in this environment. The hands-on exercise can be designed to be modular and flexible so that it is easy to fit into an existing curricula [5] without significant changes. Some countries have state-level curricula for the education institutes and changing the curricula is not flexible in these states, as they usually required national consultation about required changes. It could take years to reach an agreement and to apply the changes. Nations are mostly using their own experience to improve the existing curricula. Furthermore, they use other nation's curricula to collect best practices. The UNESCO International Bureau of Education in Geneva [10] supports development and information sharing to have a cross-border curricula. The organisation focuses on and collects present and past education models. They also provide professional advice to nations to build their national curricula. The organisation uses curricula from all over the word from the last few decades. Even if one nation decides to use another nation's curricula to get inspiration for building a new national system, it is understandable that there is no single solution which is suitable for all nations. Every nation has a different background, different primary and secondary school systems, where Information Technology (IT) education should fit in. There are examples from Asia where the Programme for International Student Assessment (PISA) test shows very high potential and well-implemented system that provides applied knowledge in the field of real

subjects. But these curricula cannot be efficient in South Europe [11] as the key findings indicate.

There is an Italian example of flexible curricula building (ITIS Majorana Brindisi, Secondary School, Italy). The teachers and students produce their own curricula and even their own local books and e-books to have a flexible environment of learning. The content is produced directly by teachers with the participation of students. Within four years it has developed into a large network including more than two hundred schools. This system provides flexibility and easy reaction for future changes and new training requirements. Those training requirements can be translated very easily into training solutions. Through adaptive learning, the delivery of the content is easier because of higher student engagement [2] and hands-on exercises, which put the student in the centre of the learning process. This approach can also be used in cyber education through exercises.

2.2. Evolution of exercises

The increase in cyber security exercises has accelerated in the recent years [12], [13]. The number and the complexity of cyber security exercises have also grown. The main accelerator of the growth is demand by policy. The main aim of the law and policy is to increase efficiency and effectiveness in government. Figure 1 explains the demand by policy and the actual requirements [13] identified by European Union Agency for Network and Information Security (ENISA).

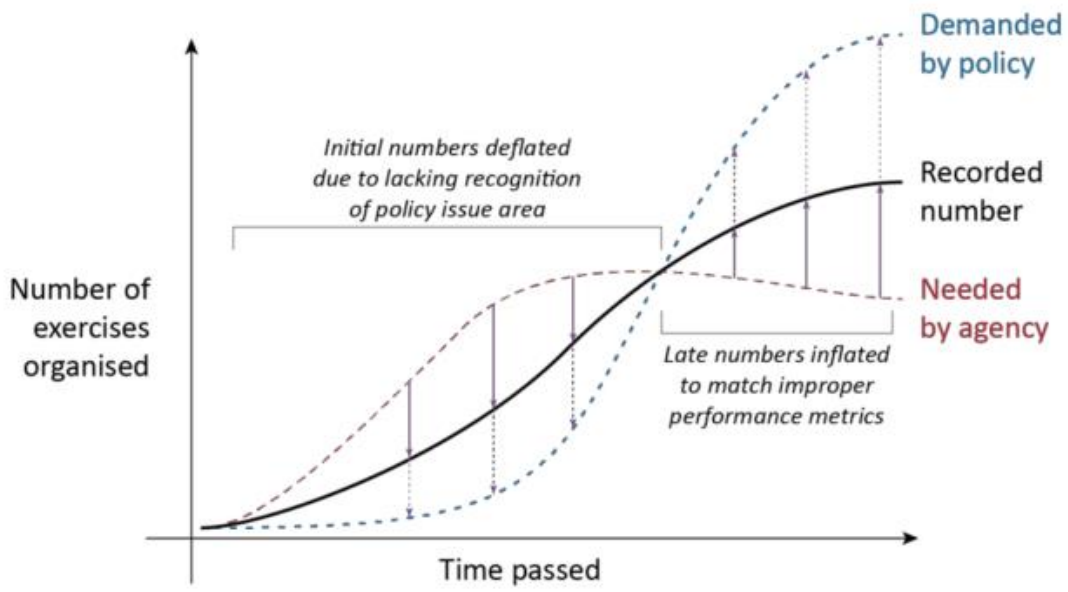


Figure 1. Policy vs. competence pressure by ENISA [13].

The increased number of countries implementing national cyber security strategies [14] has supported increased awareness and participation in national and international exercises to enhance cooperation. Likewise, the agreed [15] EU Directive in Network and Information Security (NIS Directive) and European Union Cybersecurity Strategy [16] has also provided guidance by identifying strategic priorities and actions, achieving cyber resilience, reducing cybercrime, developing cyber defence policy and capabilities and establish a coherent international cyberspace policy for the EU.

There is still demand for table-top exercises, not only in public sector, but also in private sector and in academia [17]. The exercise's training audience has shifted lately from aiming at one sector. As a consequence, the vertical sector involvement is also increasing [18]. The information gathered during the exercise planning, preparation, execution is richer and the training audience is more complex. This requires more complex exercise planning to reach all the exercise objectives. Hence exercise planning is more complex and it requires new tools [19]. A tool developed for Livewire and CyberStorm 2009 to support the exercise scenario planning with a web-based collaborative tool is called CyberSMART. This tool helped establish objectives, scenarios, game track, and event list. As a result it supported the development of an engaging scenario and events list that challenged the participants, even with a diverse of information assets, monitoring methods and response doctrines.

There is an effort to reduce exercise preparation time and create a unified model. The model can be used to create a basic scenario and the workflows for the exercise participants and organisers [20]. This model can reduce the time of preparation, however significantly more preparation time is needed for large scale exercises. The time-span for some large-scale multi-level multi-national exercises like Cyber Storm IV, can reach 24 months [21], of which the planning period is the most time consuming.

In any competition preparation time is needed to create scenarios supporting training goals and the training environment. However, time can be saved if the exercise planners reuse injects or scenarios from previous years. In the past decade there are more exercises [13] that are part of an exercise series than newly developed individual exercises. They take place on a quarter, yearly or biannual basis. This approach saves costs for the exercise planners by reusing the scenario or injects or part of the virtual environment. It is also supports better and more responsive problem solving and the use of lessons from previous years.

Universities are also searching for [22], [23], [24], [25] the best ways to provide hands-on training, active learning experiences for students to help them apply theoretical concepts in a technical environment. The cyber security exercises provide this experience in a challenging and competitive environment, not only for students doing technical studies, but also for management-oriented graduates.

2.3. Role of information sharing

Information sharing models support preventing, detecting and responding cyber security incidents and facilitate standardized information sharing. It is essentials in the business and government deeply interconnected environment. The main element of these knowledge sharing models has been an important research topic [26], [27]; however cyber security exercises are still using ad hoc solutions such as web pages, emails, portals, wikis to share non automated information. One of the initiatives to facilitate cyber security information exchange is EISAS system developed by ENISA [28]. The other initiative is from the NATO Communication and Information Agency, the definition of Cyber Security Data Exchange and Collaboration Infrastructure (CDXI) [29]. There are initiatives also from the United States. The International Telecommunication Union (ITU) ITU-Ts X.15xx series standard includes many of the

information sharing techniques. The ITUs Study Group 17 [30] describes methods for exchanging cyber security information [31]. The first model of the formal mechanisms is the Information Sharing and Analysis Centre (ISAC) described in Presidential Decision Directive 63, introduced in 1998 [32]. Numbers of ISACs were developed, some focusing on sharing information on intrusions and vulnerabilities. The mechanism relies on the functioning central hub, which makes the system vulnerable to delays and system failure. It is also important to note, that intrusion and vulnerability information is not usually actionable. Alerting the counterpart after the compromise is already too late to mitigate attack before damage occurs. The second model is the Post-to-All model which enables the entities to share directly rather than going to a central hub. The dissemination is prompt and can be easily scaled. This model is used in exercise information sharing mostly, due to it is inexpensive and allows information sharing to others from the members where the data were collected and analysed. There are hybrid models for sharing cyber information, when a post-to-all and hub-and-spoke methods are used for different purposes; one is used for sharing indicator of compromise (IOC) information, the other is sharing post investigation or post exercise information. Each model has its benefits and there is no single solution that fits to all. There are examples for all models in exercise information sharing [33], [21].

3. Overview of exercises and their information sharing

3.1. Method

The dataset used to analyse the exercise and their information sharing consists of over 120 exercises and reviewing literature such as studies of exercises and after-action reports. The gathered information and the newly developed classification method are used to provide an overview of exercises and their information sharing. The key input to the analysis was the ENISA report on cyber exercises [12], [13] and the cyber exercises taxonomy [18] by the Spanish National Cyber Security Institute. The data collection included open-source information gathering on cyber exercises. The gathering incorporated finished and planned exercises. The data gathering also used exercise information survey, which has two major parts: the first reflects exercise general information and the second disseminates exercise results.

It is important to note that statistics resulting from open-source scanning do not fully reflect reality, as it did not include sensitive exercise information and classified exercise information. There were several other occasions when the information was only partial, as some exercises do not share all the exercise information or exercise outcome and lessons learned.

My contribution is the statistical analysis of exercises and the supplement of an existing method on information sharing analysis. The new supplementary method is applied to the data set to analyse exercise evaluation and information sharing. The aim of development of new method was to provide common understanding in classification of exercises and their information sharing; furthermore the model can be used as meta-data in exercise information sharing databases.

The existing models are used to identify exercise level, exercise method, exercise design, sector involvement and participation scope. With the new additional data, the exercises and exercise reports can be identified more precisely, facilitating the information sharing. Figure 2 shows the identified new categories to facilitate detailed understanding and information sharing.

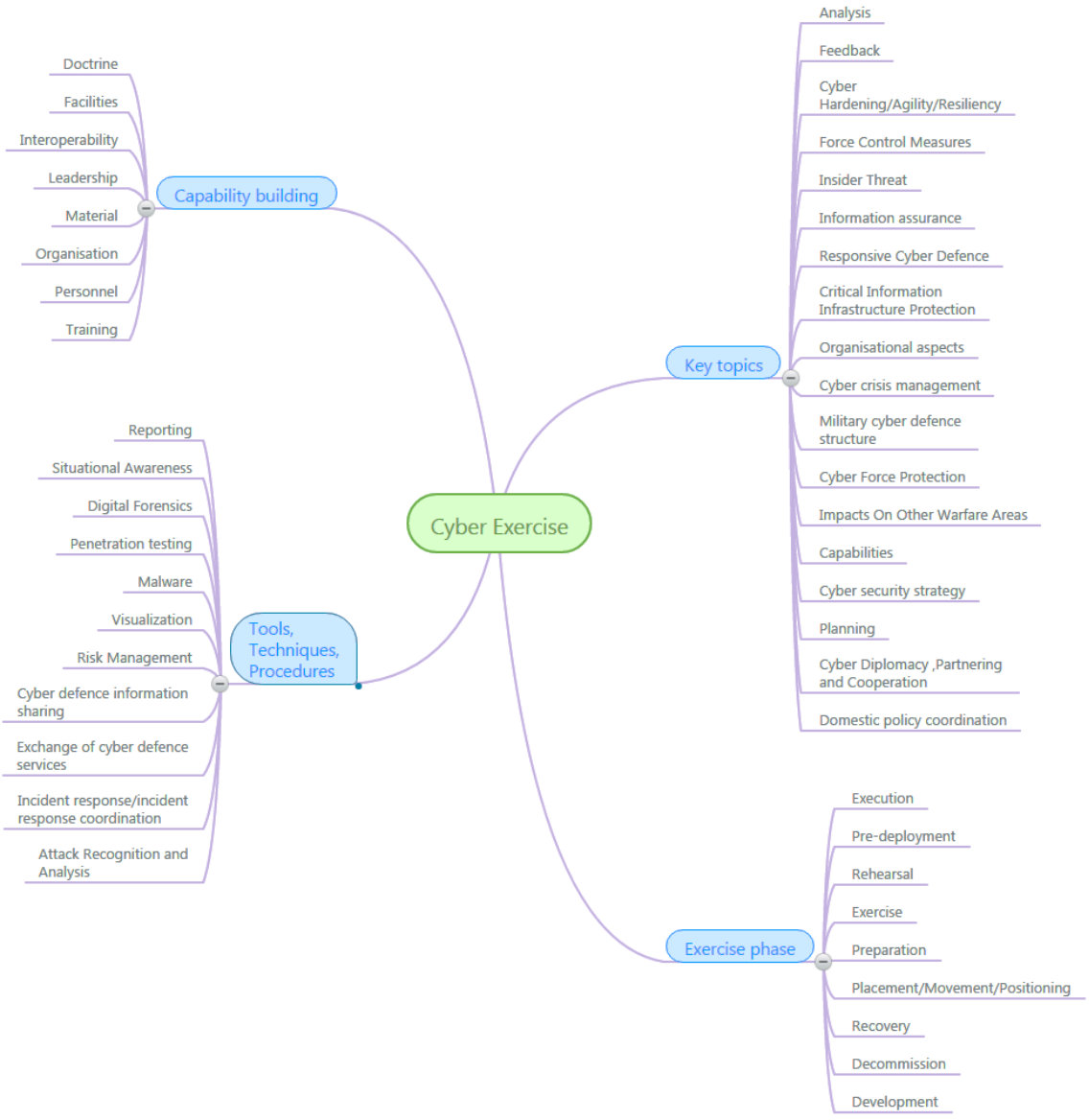


Figure 2. Model for exercise data information sharing.

The new model has been applied on the gathered dataset and the gathered after action reports to identify and characterize the exercises, and their information sharing more accurately.

3.2. Types of exercises

There are significant differences among cyber exercises in their training audience, topics that affect exercise design, and exercise method consequently creates main types of exercises. This chapter gives an overview of types of exercises. The gathered dataset included many types of cyber security exercises. The grouping was done by using the

method applied in the 2015 report on exercises [13]. This method was applied on the identification of types of exercises.

A cyber security exercise usually involves one fictional state or team competing against others who conduct social engineering, network reconnaissance, cybercrime, large scale denial of service attacks, network attacks, system attacks and critical infrastructure attacks. The scenario and the execution can be different in each case, although in execution they have very similar effects. The exercise can measure effect, understanding and competence and it can also test new procedures, skills and tools. The International Standardisation Organisation (ISO) guidelines for exercises uses different exercise objective classification [34], such as orientation, learning, cooperation, experimentation and testing.

These exercise objectives can be achieved through different exercises within the organisation like defensive cyber exercises, small internal capture the flag competitions, red team against red team competitions and integrated semester-long exercises in universities.

The defensive cyber exercises originate in US military service academies in 2001, when they introduced CDX as an inter-academy competition [35], [36]. The teams designed, implemented, managed and defended their computer networks. The objective of the exercise was to test the application of the learned skills in practice and keep the system functional while a profession group of penetration testers attacked the infrastructure repeatedly over the exercise period. It was a defensive exercise, so the hack-back or any offensive activity was heavily penalized. The attacker team conducted equally balanced attack campaigns against all participating teams. The student teams installed and hardened the services to meet service requirements, and built monitoring and defensive measures around systems. By focusing on defensive objectives all team members learned the network, use of security tools and user security concepts in a practice setting. The exercise participants felt that it was a very useful experience and none felt adequately prepared for the exercise [25], as stated by Conklin. Most participants went home with identified items and initial thoughts on how to improve their performance.

The exercise used virtual private network (VPN) tunnels to connect the independent gaming networks. The disadvantage of this exercise [37] was the strictness of the rules

and infrastructure. The cadets were provided with the Rules of Engagement (ROE), which outlines the services and limitations of the game. One of the biggest real-time defensive international cyber exercise is the Locked Shields (LS) organised annually by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). The exercise is unique in that it uses realistic technologies, networks and attack methods. In 2015, new attack vectors included Industrial Control Systems (ICS/SCADA) Windows 8 and 10 operating systems, as well as an element of active defence [38]. In addition to technical and forensic challenges, LS also includes media and legal injects. This, it provides insight into how complex a modern cyber defence crisis can be and what is required from nations in order to be able to cope with these threats.

Capture the flag (CTF) competitions are run locally in small communities in high schools, universities and are also available nation-wide or as a multinational competence through a year period. CTFs have been around for fifteen years. Initially it was used to test offensive security skills in the DEFCON 1999. Since then CTF competitions are replicated including UCSB iCTF [39], Ghost in the Shellcode [40], RuCTFe [41], Nuit du Hack CTF [42], CCCAC CTF [43], Insomni'hack [44], DEF CON CTF [45], Codegate CTF [46], Hack.lu CTF [47], PlaidCTF [48], PHD CTF [49], HackIM [50], SECCON CTF [51] and so on. There are around one hundred CTFs competitions tracked by 'CTF Time' ranking site [52]. Each competition has a different goal. In some games the students are given pre-configured hosts, network and services to practice their skills and abilities to defend it: an offense-oriented game. In other games the students build their own services and test it against other teams. In red team, blue team competitions the red team is assigned with goals to gain access in the blue team's system. The blue team should provide the services while being attacked. The teams will get points when they achieve the objectives according to the designated scoring. Some competitions began as a classroom competition and have grown into a multinational events [24]. The University of California, Santa Barbara, International Capture the Flag Competition (UCSB iCTS) was born as a final for the graduate class in the university. Now the UCSB iCTF contest is multi-site, multi-team hacking contest where a number of teams compete against each other independently. Each team uses a pre-configured virtual machine with undisclosed vulnerabilities. The exercise every year is built around one theme to set up challenges, give hints, and make it more entertaining for the audience. Since 2007, the organisers rebuild and rewrite everything in every year

providing a completely new design. After a certain amount of time each team can attack the others to find the flag in the others system. The scoring system uses bots to determine the availability of services then assign points for maintaining the services and after flags form other teams. The students must conduct offensive actions to win. CTFs also provide a game-like experience. The competitors submit the answer to a challenge and when it is accepted they know that it was the correct one. This incremental feedback and points system keep the teams engaged throughout the whole game. Competitors typically learn individually and apply knowledge to succeed.

The exercise framework [53] is also shared for free. The framework is a customisable framework: each service provides a renewable authenticated functionality. To get the framework the requestor select the services, configuration tailored to the training audience, skill-set and the tool generates the virtual machines (VMs). In the package the requestor gets the services that are vulnerable, the procedures to set and get the flags, the central database and the score-bot. The university also expects the community to contribute to the framework by submitting services. This service is suitable for organisations that have no previous CTF experience and would like to have a plug-and-play competition, or start to experiment with the framework to design their own exercise. There is also an initiative to collect and share CTF exercise information with the community [33] by using web2 tools.

3.3. Considerations in exercise building

After understanding the main types of exercises, there are considerations need to be taken into account during the planning phase, while building an exercise to build an effective, affordable, secure and entertaining exercise. Cyber security competitions and exercises are either created using a completely new setup or using an existing model, framework or infrastructure.

Resource considerations of building exercises should include the exercise planner’s perspective as well as the exercise participants. The resources should include cost of renting or having a laboratory for the preparation and exercise and also renting the exercise planning venues. This cost can be decreased by using remote access to the game network and co-location of exercise planning events. In the case of annual exercises, the cost can be decreased linking the previous year's evaluation with the next

year's first planning event. This would also facilitate the better use of lessons learned from the previous year. The next resource is the management of the exercise, which may have a potential cost. The following resource is the external support which depends on the quality of the internal expertise. Contracting personnel or requesting volunteers with experience can be appropriate. Internal personnel often require man-months' allocation by the management to support exercise planning, preparation and execution. Administrative and technical personnel support is also needed. There are examples of using observers in technical exercises besides data capturing. Observer training is needed to maintain observer awareness of cyber security and cognition [54].

The next resource is procurement to have appropriate hardware to support the execution. The dual use of the hardware resources is necessary to provide a cost-effective solution. Cost effectiveness can be reached through bi-lateral and multi-lateral agreement of shared use of cyber range capability [55]. There can be limitations of exercise objectives due to limitations of hardware or software resources. The use of virtualised environments and open-source software solutions can reduce costs significantly. The exercise environment should be available for the planned event that requires scheduled maintenance and upgrade. Budgeting and planning for maintenance and exercises is necessary to provide an upgraded training environment. In the case of sharing the same environment with others, the agreement should also cover the service level. Among the costs, the allocated time of internal personnel has already been mentioned. One of the most significant costs is the time of exercise director, exercise planners and infrastructure experts. It requires a great effort in preparing the scenario, environment, coordinating the tasks, setting up the exercise venue and overseeing the whole preparation process. The institution should analyse the benefits and potential costs of having and future developing an exercise after a certain size. The exercise can be linked to other training events. One example of this is using the technical exercise outcome and situational reports for a follow-up decision-making exercise or workshop. The other link can be the integration of preparation phases with courses, university training events so that exercise and exercise preparation can be integrated into university curricula.

Legal considerations of exercises should cover exercise preparation, execution post exercise information sharing and legal play of the exercise. The identification of

exercise objectives is the first step when legal consultation needed. The exercise can be designed in a way that teams need to break into another team's network to capture a flag, while other teams defend their own infrastructure; consequently red teams go against red teams. The training objective also can be more defensive, when every kind of responsive approach is forbidden during the game. The team needs to defend a certain network from red team attacks, hence red team against blue teams. The exercise rules and infrastructure setup should follow the exercise training objective. The exercise objectives or the size of the exercise can lead also the use of real data and user information. In case of real data involvement, exercise participants and organisers should be aware of the applicable laws and regulations. The relevant topics include, but are not limited to, unauthorised intrusion, access to data, violation of individual privacy rights or contractual obligations. The exercise planners should analyse these risks and take all necessary steps to avoid anyone breaking the laws and regulations. Counter measures consist of segregation networks and infrastructure elements, thus only systems involved in the exercise should be connected. The exercise planners should control the exercise environment and the exercise data. It should be described in the exercise documentation which services, which data, which users and roles will be involved with clear responsibilities, rights and segregation of roles. This set of rules should be clearly explained to the exercise players, including supporting student from universities [56]. Break these rules should be penalised. Before sharing any exercise data, the exercise planners and participants should identify the sensitivity or classification of data and have a mutual agreement of sharing such data. Legal and media play can give an important flavour to the exercise. It expands the scope of the pure technical play and enhances the understanding of the complex environment for technical people. The legal play of the exercise can be done through separate scenario or using legal injects in some scenarios. The benefit of using inject in some scenarios is to enhance the understanding of cross-dependency and interdisciplinary of cyber actions. Injects should be well linked to the play either way.

Scoring considerations should be taken into account if the exercise planners would like to create a gaming environment to enhance exercise performance and experience. Carefully designed and balanced scoring can also be used to measure individual performance, even for the personal assessment of an exercise participant. The whole exercise assessment must be done after the exercise; it will provide understanding for

the exercise participant when and where the attack happened, which tools and procedures were used and whether they were identified by the defenders. The assessment should include the attackers and defenders strategies, their steps and understanding of the exercise. This can be done using automated tools to record network and host activity, analysis of the log files of the tools used by the teams and also through non-technical means. The non-technical elements are the situational reports submitted by the exercise participant during the execution, feedbacks, surveys and observations from the preparation and execution phase. After the exercise, participants can use network or host forensics analysis to fully understand what happened during the exercise. An example of post-exercise assessment is the forensics challenge workshop [57] and large scale packet analysis course [58] after the Locked Shields (LS) 2016 exercise.

Communication considerations of the exercises should include the communication among exercise participants. The communication between the team enhances teamwork; crisis communication should be included in the exercise objectives. The media considerations should cover the media training of the key personnel of the exercise and information disclosure about the event. Rules should be addressed to the participation teams describing when and what information can be shared. In case of a defensive exercise, the aim of the network defence exercises is to provide hands-on experience defending under attack. The main focus for the exercise is not to attack systems. This training objective should be clearly communicated to every party involved and to the wilder public.

Information sharing considerations of the exercises should cover the identification of the best channel to reach the audience. Cyber exercise information sharing remained a challenge even if an exercise has been conducted for many years and have an extensive background and knowledge base [21]. The main obstacle for better information sharing is the sensitivity of data, however with careful planning it can be avoided. In some cases researchers build an environment to determine the effectiveness of cooperation. The Pacific Rim Collegiate Cyber Defence Competition (PRCCD) identified data sources [59] to provide realistic network data, so anonymised data was no longer needed as thought to be the main obstacle of exercise data information sharing.

3.4. Statistical summary of exercises

The statistical summary provides an overview of exercises planned, executed in the last five years. It provides an overview of the main development path. The grouping was done by using the method applied in the 2015 ENISA report on exercises [13].

The interest of cyber exercises is also reflected in academic context, where the number of published academic resources, such as books, journal articles, conference proceedings, dissertations is growing. Google scholar, Scopus and Tallinn University of Technology Library Primo search in Figure 3 gives an overview of the search hint for 'cyber exercises' in the last five years.

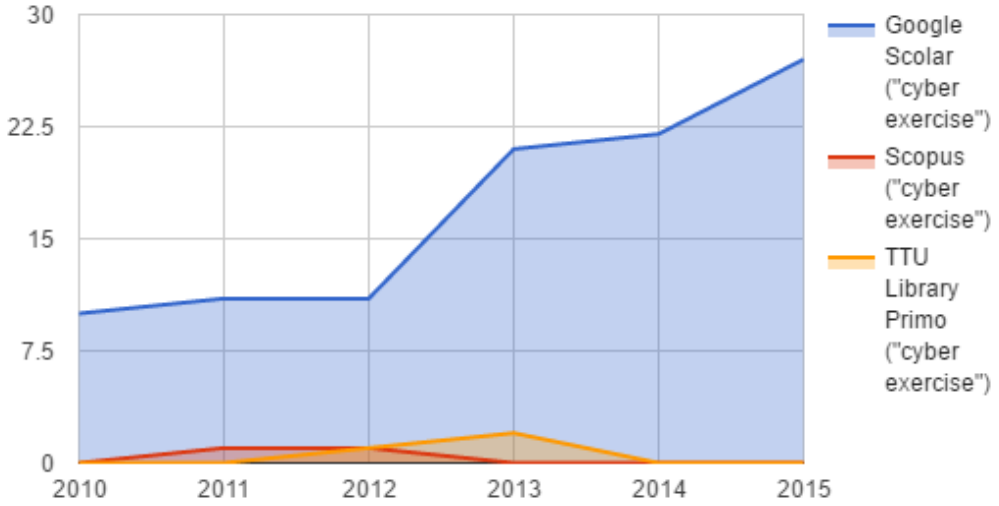


Figure 3. Search hint 'cyber exercise'.

Figure 4suggest that the appearance of the term 'cyber' AND 'exercises' has been increasing even more rapidly than the general hint in the last five years. This indicates that cyber elements in exercises are becoming a more popular topic in academic research.

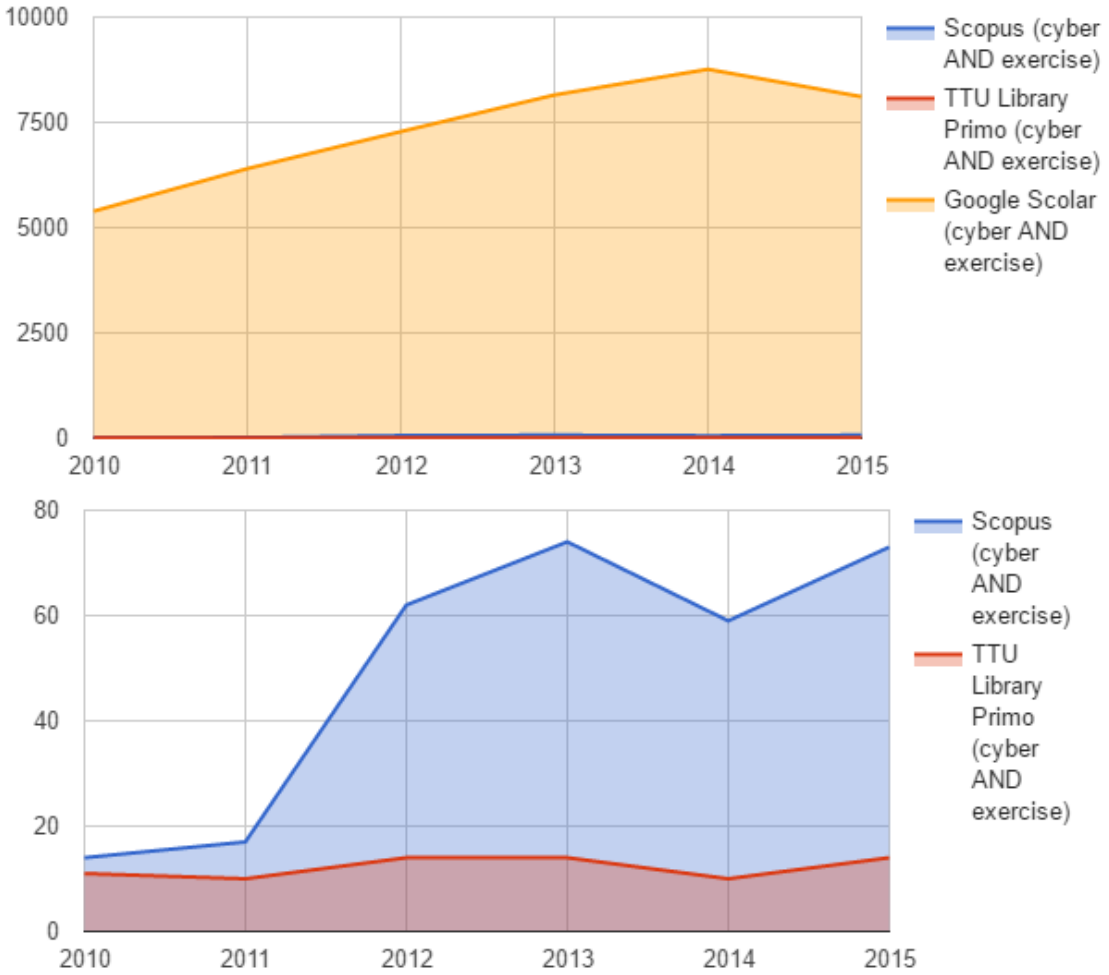


Figure 4. Search hints: cyber AND exercise.

Despite the large number of hints in the topic, it was hard to identify the relevant studies have been conducted under the term cyber exercises and cyber exercise information sharing. Understanding whether cyber exercise information sharing is effective was also an issue.

In parallel the growth of academic research hints, the analysis of collected exercise data shows in Figure 5 that there has been growth, in the number of exercises conducted recently and the growth is accelerating.

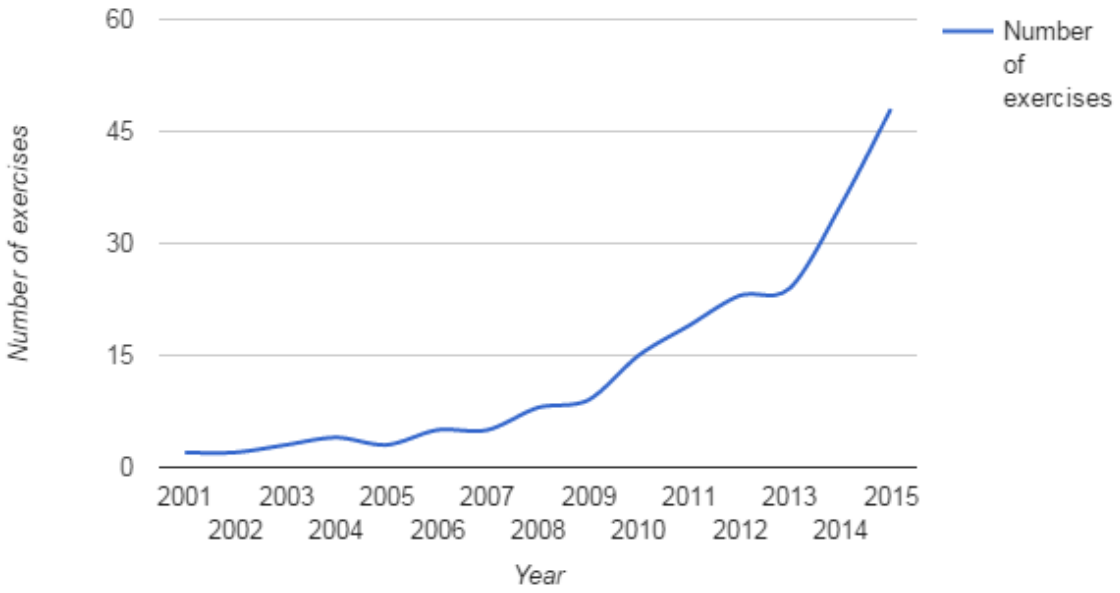


Figure 5. Number of exercises 2001-2015.

The rapid increase in exercises is not only the increase of one-time exercises, but also the growth of annual and bi-annual exercises conducted by nations and organisations. This pattern suggests that a number of exercises become annual exercises. It also shows that the exercise planners and participants are sharing more exercise information with the community that led to build more exercises. The increase is also driven by the awareness of stake holders.

3.4.1. Exercise profiling

There are two main models to support exercise profiling. The models are useful tools to provide better understanding of cyber exercises, profile them by common characteristics. The first model defined by the Spanish National Cybersecurity Institute (INCIBE) has five basic elements as showed in Figure 6. The basic elements support the identification of focus of the exercise, the model that the exercise uses, the sector involvement, the scope of the exercise and the result dissemination.

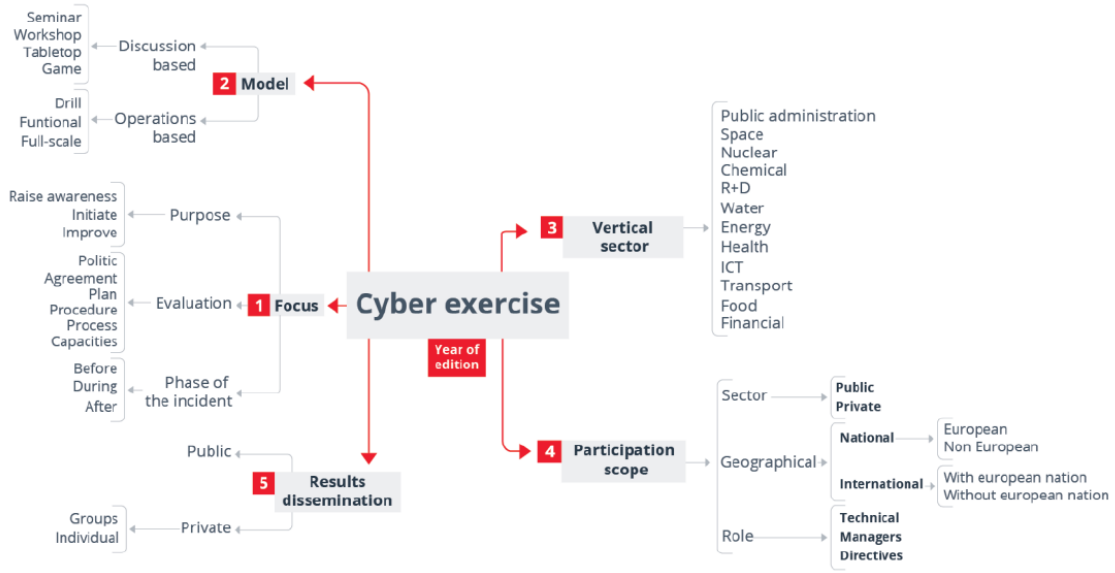


Figure 6. Exercise dataset model by INCIBE.

The second model defined by ENISA has five main elements also as seen in Figure 7.

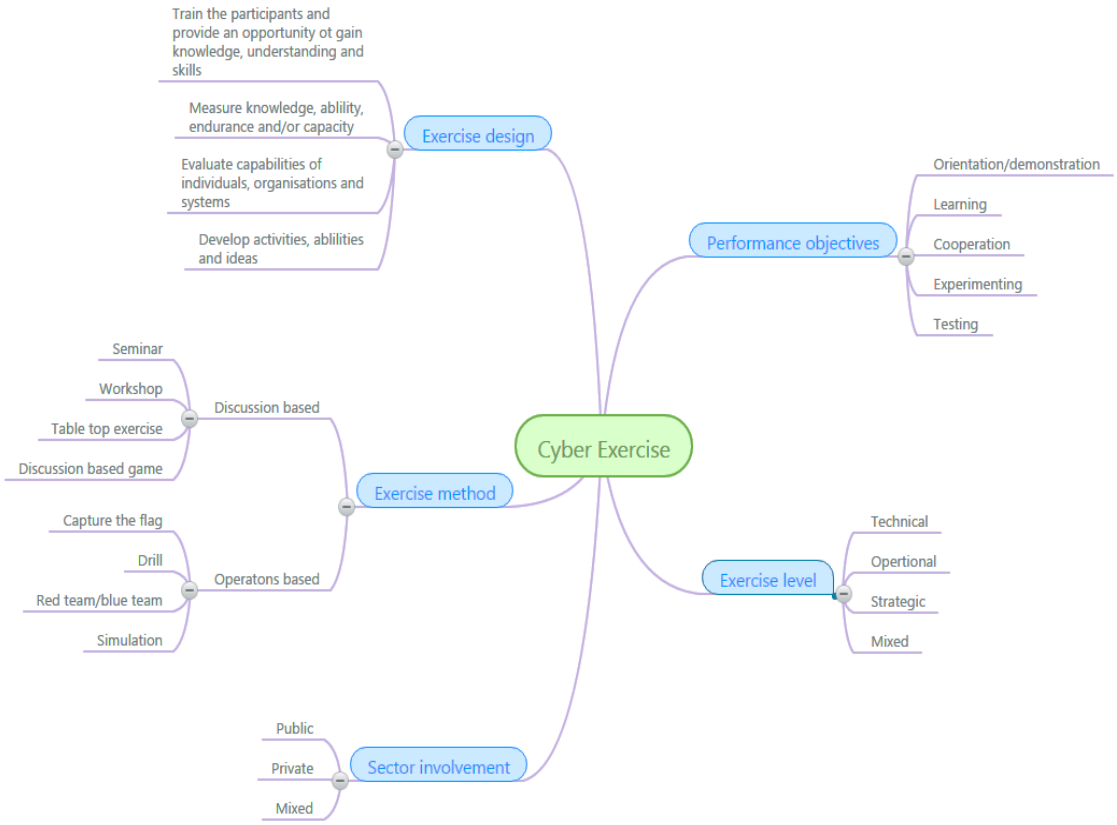


Figure 7. Exercise dataset model by ENISA.

The main elements have not provided characteristic about information sharing or phase of the incident, exercise. However they are very good to identify exercise method, design information.

The future analysis and statistical summary was done by using the method applied in the 2015 ENISA report on exercises [13]. ENISA used ISO 22398 guidelines for exercises to identify categories and input from experts to narrow down the data types. The used data-set included broad set of exercise types, which was also filtered following the ENISA methodology. The result shows that the exercise design follows four different categories as shown in Figure 8.

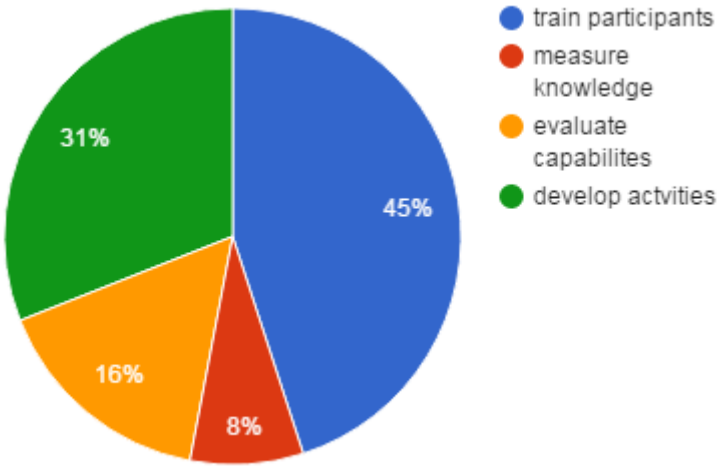


Figure 8. Exercise design.

Training of participants (45%) had been the focus of most exercise designs. This provides an opportunity to exercise participants to learn new skills, gain knowledge and deeper understanding. The following main focus area was the development of activities, abilities and ideas (31%). There were exercises designed to evaluate capabilities (16%) and measure participant knowledge, ability, endurance or capacity (8%).

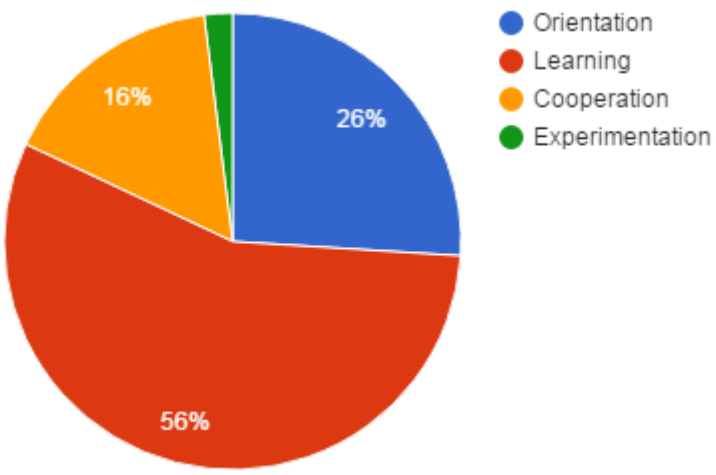


Figure 9. Performance objectives.

Learning was dominating among performance objectives as shown in Figure 9. Most of the exercises were focusing on learning (56%) rather than orientation (26%) or cooperation (16%). It is more complex to design and execute cooperation exercises and it requires involvement from more stakeholders. A few exercises were used to test and experiment (2%) new ideas, procedures and concepts. During experimentation exercises a well-trained group of experts test a new procedure or idea. The number of experimental exercises is expected to increase in the future.

The increase of exercise complexity can be identified through the increase of participants as showed in Figure 10, and also the increase of the numbers and variety of organisations and stakeholders through the exercise planning, execution. Consequently the planning is more complex, which can take a whole year.

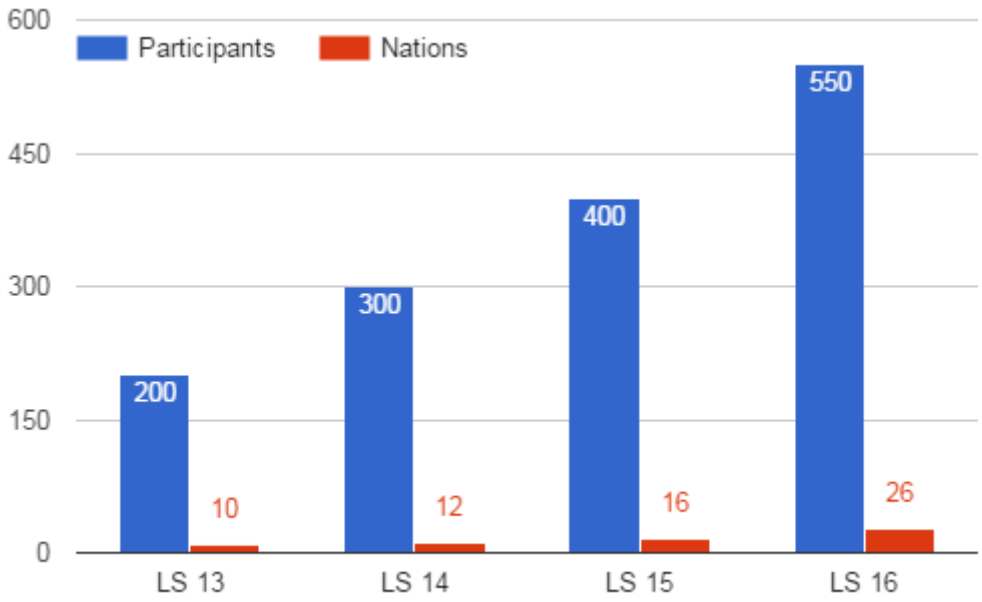


Figure 10. Locked Shields (LS) exercise participants.

The exercise evaluation has become more detailed. Large-scale exercises are publishing after-action reports that review the exercise objectives, planning and execution and provide detailed insights into the scenario and strategies followed by the participants. Those exercise after-action report are rich source of data for future analysis.

3.4.2. Extended exercise profiling

Using the exercise after action reports and the gathered dataset the introduced extended model in Figure 2 had been applied to identify more detailed metrics. The more granulated metrics would enable better understanding and furthermore better exercise information sharing.

Two exercises that published their after action reports had been selected to apply the model. The model has been applied to information in the after action reports and the gathered dataset.

The first selected exercise is LS' 13 exercise as presented in Figure 11.

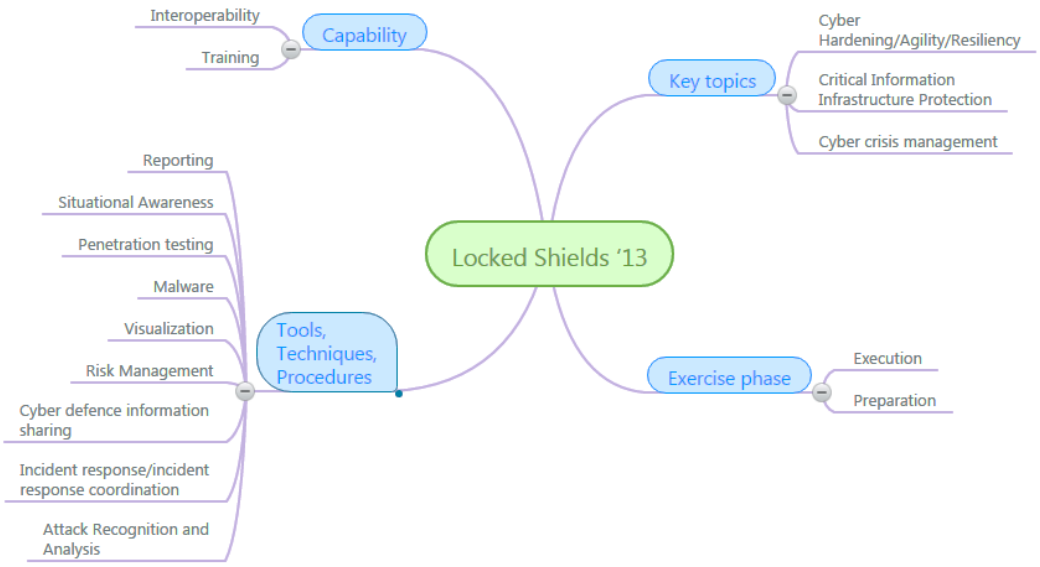


Figure 11. LS'13 extended model.

The LS' 13 exercise was a multinational technical exercise executed on 23-26 April 2013, including 10 blue teams. The teams were acting as a rapid reaction teams who had to defend virtual networks against the red team attack. The extended model shows the key topics, tools, techniques and procedures had been exercised during LS '13.

The next selected exercise is Cyber Storm IV exercise as presented in Figure 12. Cyber Storm IV exercise series began in late 2011 and concluded in early 2014, having 15 table-top and distributed exercises. It had the focus areas of information sharing, international and domestic (federal, state, private-sector) coordination, plans & procedures, public affairs, cyber resources. It had involved 11 countries 14 federal agencies 24 cyber coordination bodies & cyber centres.

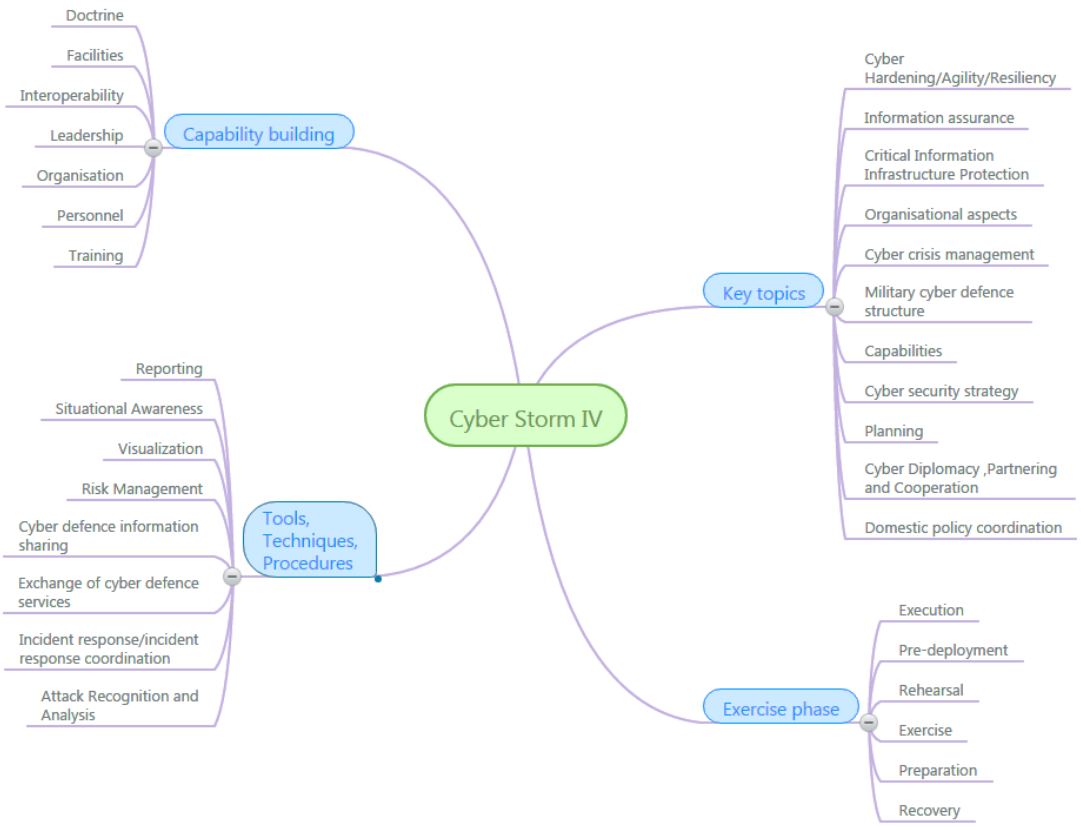


Figure 12. Cyber Storm IV extended model.

Applying the extended exercise profiling model on after action reports created a richer characteristic of the exercise. With the more detailed understanding of the exercise the information sharing can be better developed.

3.5. Result

The overview of exercises provided an understanding of types of exercises, building considerations and the statistical analysis, including extended exercise profiling. The main identifiable patterns were the increase in the number of exercises, the increase of complexity, cooperation and private sector involvement.

There are different reasons behind the growth of cyber security exercises. One is the spread of knowledge. There are new national exercises that are using the shared knowledge and expertise of large international exercises and developed by those who had previously participated in the international exercise. The other impact is the increase of awareness in cyber security issues, including latest cyber security breaches, the importance of collective training and international cybersecurity exercises.

The other identified trend was the increase of complexity. More participants were willing to join to exercise series year by year that will increase the variety of organisations, experts and stakeholders. This makes exercise planning more complex and time consuming and can affect the exercise objective. It can result in a shift of previous exercise scope and can change the exercise to be too general. This can be avoided by developing side events for the exercise that use the exercise data, but not affecting the primary scope of the exercise.

The examples showed also that the exercise scenarios are shifting from aiming only one training audience rather to exercise cross sector dependencies and become more interdisciplinary. It is more common to have less independent scenarios during the exercises but rather there were more complex ones including more technical, legal injects. This would require more precise exercise planning, but the interdependencies can be better explained to the training audience through these scenarios.

There is no common information sharing platform for cyber security exercises. There were only a few numbers of exercises that share exercise lessons learned. The lessons learned are shared in many different channels, depending on the involved community of interest. The top-down information sharing approach can work only in those organisations where there is a strong culture of sharing lessons learned. The bottom-up approach is used throughout communities. There are examples of building cyber security communities around a certain cyber security area. One example is the military operational planners, who got an access to a community portal after participating in a training course. This virtual environment was used as a tool of information sharing and providing place for discussions. Using this bottom-up approach together with the top-down can result better and faster information sharing.

The top down information sharing approach can work only in those organisations where there is a strong culture of sharing lessons learned. The bottom up approach is used through communities. There are examples of building cyber security communities around a certain cyber security area. One example is the military operational planners, who got an access to a community portal after participating in a training course. This virtual environment was used as a tool of information sharing and providing place for discussions. Using this bottom up approach together with the top down can result better and faster information sharing.

4. Effectiveness of exercise information sharing

Exercise information sharing has been analysed from a technical exercises training audience perspective, military exercise training audience perspective and the exercise planner's perspective.

4.1. Military operational planners

The NATO CCD COE provides a course for operational planners, including topics such as: cyberspace as a military operational domain, definitions and taxonomy, military capabilities in the cyberspace, principles of warfare applicable to cyberspace, cyber operations tenets, international law applicable to cyber operations, rules of engagement in the cyberspace, cyber intelligence, cyber defence in the operational planning process, cyberattacks and their effects, defensive cyber defence, offensive cyber defence, and NATO cyber capabilities. The course was designed for operational planners, non-experts in cyber topics.

4.1.1. Method - operational planners

The course training audience was used to draw the conclusion on identifying the best channels of post-exercise information sharing to facilitate future exercise development and exercise execution, with no generalising the results of the exercises to real-life situations. The training audience was also used to identify the main information sources of learning and to rank the sources based on importance.

My contribution is the identification of key information sources for exercise preparation and analysis of survey answers that rated the importance of information sources for non-technical exercise planners. The collected data includes: individual experience, identification of exercise roles, identification and ranking of information sources used for exercise preparation.

4.1.2. Execution

The Cyber Defence at Operational Level course is a five day course provided by NATO CCD COE. The training audience of the course was operational planners without deep cyber knowledge.

The exercise survey is designed to collect exercise information sharing data. The survey is used on the last two days of the course. Statistical analysis was performed on the survey data, investigating the personnel experience, resources of the personnel development and usefulness of the information sources using Likert scale analysis. Twelve (38%) of the thirty-two course participants answered the exercise survey. Detailed survey data is provided in Appendix 4.

4.1.3. Result

In total 13 responses were received. There was one answer, stating that the questionnaire was not closely related to the course, and so did not answer the questions. This answer was not taken into account. The results in Table 1shows that operational planners found exercise lessons learned extremely important.

Table 1. Importance of information sources (CDOLC).

Questions		Not important	Slightly important	Moderately important	Important	Extremly important
Importance of	Exercise planning information portal	0%	8%	8%	33%	50%
Importance of	Exercise observations	0%	0%	25%	42%	33%
Importance of	Exercise lessons learned	0%	8%	17%	8%	67%
Importance of	Exercise after action report	0%	17%	8%	33%	42%
Importance of	Information about used processes	0%	0%	36%	36%	27%
Importance of	Information about used tools	8%	0%	33%	25%	33%
Importance of	Sharing technical exercise environment (virtual machines)	0%	9%	36%	45%	9%
Importance of	Participating exercises	0%	8%	0%	42%	50%

There are processes, tools and personnel dedicated in military organisations to collect observations during exercises and share lessons learned after analysis. The mind-set and the strong culture support information sharing.

The answers for the open question about main information sources of developing the skills ranked by importance are:

1. training courses
2. directives, policies
3. participation in exercises
4. exercise documentation
5. work experience
6. exercise observations
7. exercise lessons learned
8. information and knowledge sharing with colleagues

It is important to notice that even if there is a strong culture of collecting and sharing exercise lessons, the exercise planners did not find it the best source to develop their skills. The primary source of skill development is still courses, which leads back the importance of using lessons to future develop courses.

4.2. Crossed Swords 2016

The Crossed Swords (XS)'16 cyber defence technical exercise is a multi-national exercise organised by NATO CCD COE first time in 2016. The exercise focuses on vulnerability scanning. The exercise scenario is based on a fictional state. The players are members of a rapid reaction team (RRT) of IT security personnel has been mobilized to determine the security status of the infrastructure detecting the weaknesses and vulnerabilities in the system. The scenario is based on responsive cyber defence scenario.

4.2.1. Method- Crossed Swords 2016

The XS'16 exercise training audience were used to draw the conclusion on learning through exercises is more effective way of learning in technical exercises, with no generalising the performance results of the exercises to real-life situations. The training audience were also used to identify the main information sources of learning and to rank the sources based on importance. My contribution is the identification of key information sources for exercise preparation and analysis of survey answers that rated the importance of information sources for technical personnel, weighted by their performance during the exercise.

The case study [60] was conducted as a cross-disciplinary study. The case study approach supports the use of multiply methods and sources. The collected data included: individual experience, team experience, team organisation, teamwork, team spirit, mostly gathered through surveys. The full data contained quantitative and qualitative, subjective and objective parameters.

It was recognised that multiply data sources are necessary for verification to avoid subjectivity and it was also recognised that the scope will not cover the identification

where learning happens, only the identification and ranking of post-exercise information sharing or lessons learned sharing.

4.2.2. Execution

The exercise participants' tasks included, but were not limited to, collect evidences gather information and analyse technical attribution to solve the cyber incident. The game control (white team) and the situational awareness (yellow team) were provided by NATO CCD COE just like the technical environment (green team). A virtual pre-configured environment was provided for the exercise training audience. The exercise had a test run, with the same number of participants. There is no data from the XS test run.

The exercise took two days and was executed only during working hours. The exercise's participants were from NATO CCD COE Sponsoring Nations and Contributing Participants. All the teams were in a same location. A total of fifty-two people participated in the exercise.

Exercise survey was designed to collect detailed exercise feedback. The survey was delivered and used only after the execution. Statistical analysis was performed on the survey data, investigating the personnel experience, performance, resources of the personnel development and usefulness of the information sources using Likert scale analysis. Fifteen (78%) of the nineteen red team members answered the post exercise survey. The average age of the survey participants is 33.8. Detailed survey data is provided in Appendix 1.

4.2.3. Result

In total sixteen responses were received. One yellow team member who accidentally answered the survey designed for red team. Consequently this participant did not answer the number of successful attacks and only focused on the information sources used for exercise preparation. This answer was not used for the analysis. There were red team members who did not submit numeric answers to the number of successful attacks; instead they just stated that they did not count them. In order to be able to perform the analysis, these gaps were filled with zero for that particular question. With this manipulation, the complete dataset can be used. As the objective of this study is to evaluate the information sources rather than measuring individual effectiveness or

identifying all the sources, the above introduced errors do not affect the validity of this study.

The results in Table 2 show that the responders found extremely important to participate in exercises.

Table 2. Importance of information sources (XS).

Questions		Not important	Slightly important	Moderately important	Important	Extremly important
Importance of	Exercise observations«»	6%	0%	6%	69%	19%
Importance of	Exercise lessons learned«»	0%	6%	13%	56%	25%
Importance of	Exercise after action report«»	0%	7%	20%	40%	33%
Importance of	Information about used tools«»	0%	0%	31%	38%	31%
Importance of	Sharing exercise technical environment«»	0%	6%	6%	56%	31%
Importance of	Online forums«»	0%	13%	20%	40%	27%
Importance of	Participating exercises«»	0%	0%	0%	38%	63%

One answer pointed out one unimportant field: exercise observation. However if we see the rest of the answers the observations got the highest score of important source of information to their preparation. This contradiction may come from the understanding of the term ‘exercise observations’.

There were 5 people who has previously participated 3 or more exercises. These people executed the average of 12.2 successful attacks while the rest of the participants executed the average of 3.73 successful attacks during the exercise. This pattern shows clearly that those who participated in more exercises perform better during the next exercise. The answers for the open question about main information sources of developing the skills ranked by importance are:

1. self-learning
2. courses and trainings attendance
3. Internet
4. exercise team members
5. exercises
6. everyday work
7. information and knowledge sharing with colleagues
8. learning by doing

The results show the added value of participating exercises. Different types of data were useful for analysing different aspects of individual effectiveness. In the case study, the

survey served the purpose of improving understanding regarding how the individual prepares for the exercise. It helped to understand the importance of participating in exercises and also highlighted the performance differences among those who had participated in previous exercises. Exercise participation is a very important step in the learning experience, but not a unique source of the best performance. The participants highlighted the importance of individual preparations that leads to good performance. Individual preparation and courses as primary sources of information can be used as an input to inject exercise outcomes from exercises: observations and lessons learned. In that way the pre-exercise preparation can be more effective.

4.3. Locked Shields 2016 test run

The second selected technical exercise is the LS 2016 cyber defence technical exercise test run, which took place on 9-10 March 2010. It was also a multi-national exercise organised by the same organisation since 2010. However, the exercise's focus was different; it focuses on defending IT infrastructure. The training audience of the LS exercise was blue teams: computer emergency response teams. The LS exercise had a test run with a limited number of blue teams, mostly from universities testing the gaming environment.

4.3.1. Method- Locked Shields 2016 test run

The LS 2016 test run exercise training audience is used to verify the result of XS 2016 exercise study outcome. The case study outcome was that the red team members who participate in more exercises could perform more successful attacks during the exercise. The LS 2016 test run exercise training audience was used to draw the conclusion that teams which learn more through exercises are more effective defending their networks during exercises, with no generalising about the performance result to real-life situations. Although, the red team members' performance can be easily measured through successful attacks, the blue teams' performance measurement is as difficult as measuring cyber security within the infrastructure [61]. The individual blue team performance is highly dependent on each member performance and the cooperation of team members.

My contribution is the identification of indicators that reflect team preparation performance. Using the indications the better prepared team can be selected and future

more the exercise winner can be predicted. The test run provided an opportunity to test the created methodology.

The collected data includes: individual experience, team experience, team organisation, teamwork and team spirit, mostly gathered through surveys. The full data contained quantitative and qualitative, subjective and objective parameters. The survey was shared with the test run blue team before the exercise, and analysed before the exercise predicting the winning team. The exercise outcome prediction was carried out one day before the exercise execution.

4.3.2. Execution

The main objectives of the test run is to test the game infrastructure of LS, test the preparedness of Red Team members, test the game injects and train the participating students. The main difference between the actual run and the test run is that the test run lasts two days: one day for preparations and one day for game play. The actual run lasts three days: one day for preparation and two days for game play.

The exercise scenario for the students is based on a conflict between fictional states. The players are members of a rapid reaction team (RRT) of IT security personnel that have been mobilised to determine the security status of the infrastructure. They must detect the weaknesses and vulnerabilities in the system, take measures to harden them, determine what, if any, data has been compromised, and keep the system operational and connected. The game control (white team) and the situational awareness (yellow team) were provided by NATO CCD COE just like the technical environment (green team). The exercise training audience were provided a virtual pre-configured environment. No offensive operations were allowed.

The exercise was executed only during working hours. The test run blue teams are assembled from the students of Tallinn University of Technology, Hungarian National University of Public Services, Budapest University of Technology with CrySyS Lab and members from Finnish non-profit Internet Users Association (KAPSI).All teams had access to the game-net from their location. A total of fifty-four people participated in the exercise as test run blue teams.

The exercise survey was only designed to collect pre-exercise information before the exercise. The questionnaire data collection included human factors like personnel

experience, performance and also team aspects, such as team organisation, teamwork, team spirit, readiness level and team performance expectations. The data collection during the exercise included: exercise environment automatic performance scoring, red team attack scoring, cooperation scoring, white team scorings, which put together the test run final scores. The aim of the scoring is to provide a gamified environment and immediate feedback for the blue teams.

4.3.3. Result

The aim of the proof of concept is to measure the preparedness of the teams before the exercise in order to predict the winner of the exercise.

My prediction was the following, before the exercise: „Taking into account the experience working in a team, and working with the tools, additionally the second positions in real life and exercise experience I assume that blue team 3 will win the test run however blue team 4 is also very strong.'

The final result in Figure 13 shows that blue team 4 won the test run, blue team 2 got the second place and blue team 3 got the third place.

Figure 13. LS 16 test run final scores.

The survey prepared for the exercise received 28 (51%) answers of the 54 blue team members. In detail Table 3. Pre exercise survey: number of ***answers*** shows the dispersion of the received answers. Blue team 1 and blue team 5 submitted only one answer. In order to be able to perform the analysis the answers from these two teams were not taken into account.

Table 3. Pre exercise survey: number of answers.

	Team size	Number of answers	
B1	12	1	8%
B2	11	10	91%
B3	10	6	60%
B4	11	10	91%
B5	10	1	10%

The data collection included pre-exercise questionnaires before the exercise. The analysis of pre-exercise questionnaire in Table 4 shows significant differences in competences between blue team 3 and 4. The first question was about the number of exercises that team members had participated in. In blue team 3, four people had participated 2 or more than 2 exercises, while in blue team 4, there were five people with the same or better experience. In blue team 4 there were three people who have participated in 6 or more exercises. The team average was better in blue team 4.

Table 4. LS test run pre exercise survey answers.

	Number of Answers	1	10	6	10	1
	Answers	8%	91%	60%	91%	10%
	Teams	**B1**	**B2**	**B3**	**B4**	**B5**
1	How many exercises have you participated? (avg)	0	0,8	2,33333333	3	0
2	How many years operational/real life experience do you have? (avg)	2	1	2,83333333	2,6	5
3	How many hours experience do you have with your tools you going to use in the exercise? (avg)	0	9,3	30,8333333	16,7	10
4	How many hours have you spent for team preparation?	10	16,4	10	12,8	5
5	How many people in your team are keeping the team together? (avg)	2	3,1	1,33333333	2,7	10
6	Do you have an experience of working in ad hoc teams (like Rapid Reaction Team)?	No	No (80%)	Yes (66%)	N/A (50%)	No
7	Do you have all the areas covered by appropriate personnel (e.g. media, legal, situational reporting, etc.)?	No	Yes (60%)	Yes (84%)	Yes (70%)	Yes (70%)
8	Do you have functions and duties clearly assigned to the team members?	Yes	Yes (100%)	Yes (100%)	Yes (70%)	Yes
9	Does your team members know their functions and duties?	Yes	Yes	Yes	Yes	Yes
10	What is the percentage of new tools in this exercise which you don't use in your daily job (0% - it's the same tools in LS, 100% - all the tools are new for us)? Think about monitoring, reporting, etc. tools.	90%	80%	45%	46%	20%
11	Do you expect to win?	Yes	No (80%)	No (66%)	Yes (90%)	Yes
12	Do you feel ready for game, or are you confused?	confused	N/A (50%)	ready (84%)	ready (90%)	ready

The following question was about operational or real life experience. The question reflects the team working and problem solving knowledge. The answer received from blue team 5 was not taken into account. The next, most experienced average came from blue team 3.The next question wanted to identify the experience and knowledge the team had with their tools. It sometimes happens that the team uses different tools for exercises and for real operations. The highest average had been given by blue team 3, although there was one person in blue team 4 who had the highest (100 hours) experience with the tool. There were significant differences within each team: some had quite few, less than 6 hours experience with the chosen tool.

The following question reflected the team preparation. It was interesting that the provided numbers had large variance even within a team, where they were preparing together for the challenge. Blue team 2 had the highest average, although there were no significant differences among the teams.

The next question was about the team management and team roles. The question could be interpreted in different ways, as blue team 5 did. They answered that all of them keeping the team together. The following question was about the experience. The ad-hoc teams and rapid reaction teams have different information flow and easy adaptation is important. Blue team 3 members had the most experience working in ad-hoc teams, blue team 4 had the second. Most of the teams had all the areas covered by appropriate personnel, with only slight differences among the provided answers.

The next question was about the duty assignment within the team. Only blue team 4 provided some negative answers due to not all the roles played during the test run (legal). The entire team within all blue teams knew their roles and duties before the test run. There was no difference among the teams regarding this question. The following question asked about the new tools in the team, and blue team 3, 4 and 5 wanted to keep the level below 50%.

The rest of the questions were about team spirit and readiness level. Blue team 4 was very positive in that sense most of them felt ready for the game and expected to win it. It was interesting to see that blue team 3 did not have a good team spirit even if all the other answer showed their prepared for the game.

The survey evaluation and prediction was done a day before the execution. The prediction is available in Appendix 3 and also attached as a separate signed e-document.

Blue team 1 and 5 were not taken into account during the final evaluation. Blue team 3 scored most of the highest scores, but there was very little difference between blue team 3 and blue team 4.

During the exercise the data collection included: exercise environment automatic availability scoring, red team attack scoring, cooperation scoring, inject scoring, revert, which put together the test run final scores, as seen in Figure 14.

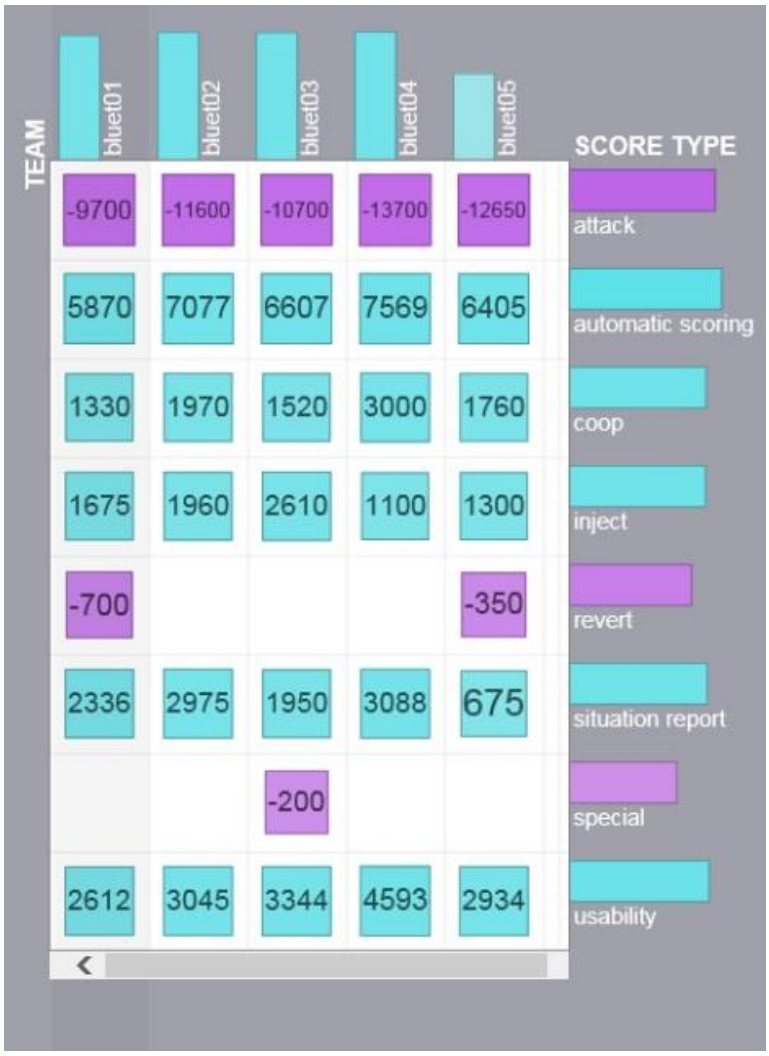


Figure 14. LS 16 test run scores by types.

The blue team performance is scored, in light of the red team actions. Red teams have no score for themselves as there is no competition between red teams.

All blue teams were equally challenged based on a pre-defined list of injects or attacks. Blue teams had the continuous task to maintain a running set of services where availability is measured automatically and, where needed, verified manually by the white team.

There were eight categories of scores, one measured automatically. The percentage represents number of points blue team can gain or lose in overall score.

Availability of Services was calculated independently for the game-day (8 hours), scoring was exponential, any availability got some points but every additional minute of uptime was very valuable. Usability was simulating normal work of the users - reading

email, opening attachments, browsing Internet, etc. If users could not access required services, this was penalised. Successful red team attacks gave negative scores. Red team had a specific list of objectives they had to achieve. Every time they were successful with one of these, blue team lost a certain amount of points. If they weren't successful, blue team did not just lose points but they could gain points when the attack attempt was detected and reported. During situation reporting (SITREPs) the quality of reports was scored. Cooperation quality and relevance of information sharing between teams were also scored. Responding to injects was also scored by the quality and completeness.

During the test run there was no legal play, forensics challenge and there was no score for them.

Green Team (GT) gave negative scores for requesting assistance and reverting virtual machines. Green team assistance in cases of infrastructure problems was not scored. Special scoring included penalties for breaking the in-game and out-game rules or bonus points for blue teams for outstanding performance e.g. info sharing.

Consistency of scoring was checked at a central point in the white team. Given scores were made visible to the blue teams after a short delay, depending of the type of score.

Blue team 4 won the exercise; they got high number for availability scores, cooperation scores, situation report and usability scores. Even if the red team executed most of the successful attacks against blue team 4, they could keep the systems up, provide services to the users and inform the higher management in the understandable way about the situation in their network. Blue team 2 got the second place, with the second highest availability cooperation and situation report scores. Blue team 3, which was predicted to win, got third place during the execution. They lost many points in availability, cooperation and situation report and got special scores due to not answering the game management on time. All the other fields were quite balanced with the other teams.

4.4. Locked Shields 2016

The third selected technical exercise is LS 2016 cyber defence technical exercise. It is the biggest and most advanced international live-fire cyber defence exercise in the world and took place on 18-22 April 2016. The annual scenario-based real-time network

defence exercise focuses on training the security experts who protect national IT systems on a daily basis. Over 550 people and a total of 26 nations were involved in LS 2016, organised since 2010 by also the NATO CCD COE. Twenty blue teams were representing by nineteen nations and NATO Computer Incident Response Capability (NCIRC). The exercise followed the test run which was held in March.

4.4.1. Method- Locked Shields 2016

The LS 2016 exercise training audience was also used to verify the result of XS 2016 exercise study outcome. The case study outcome was that the red team members who participated in more exercises performed more successful attacks during the exercise.

My contribution is the identification of key preparation indicators for technical exercise preparation. Using the indications the team can prepare better for defending their networks during technical exercises. Furthermore, the exercise winner can be predicted.

The collected data included individual experience, team experience, team organisation, teamwork, team spirit, mostly gathered through surveys. The survey used during the LS 2016 test run had been slightly modified to allow for better measurements. The survey also included new questions reflecting the learning experience before the exercise.

The full data contained quantitative and qualitative, subjective and objective parameters. The survey was shared with the blue teams before the exercise, and analysed before the exercise predicting the winning team. The exercise outcome prediction was done one day before the exercise execution.

4.4.2. Execution

The main objective of the LS 2016 exercise was to train the national blue teams. The teams were tasked to maintain the networks and services of a fictional country, Berylia under intense pressure. This included handling and reporting incidents, solving forensic challenges as well as responding to legal, media and scenario injects.

The exercise scenario for the blue teams was the same for LS test run. The difference from LS test run was that all the scenarios and all the elements were played during the exercise. These were media play, forensics challenge, legal play also - that was not played during the test run.

The participating blue teams had online access to the exercise networks and typically worked from their home countries. The virtualized blue team networks were custom-built and included a variety of services and platforms. For example, the blue teams had to maintain a number of servers, online services and an industrial control system. Realistic technologies, networks and attack methods formed the backbone of LS 2016 to stay abreast with market developments. The exercise was organised in cooperation with the Estonian Defence Forces, the Finnish Defence Forces, the Swedish Defence College, the British Army, the United States European Command, Tallinn University of Technology and numerous other partners.

The training objectives for the blue teams included[56]:

- Learning the network.
- System administration and prevention of attacks.
- Monitoring networks, detecting and responding to attacks.
- Handling cyber incidents.
- Conducting forensic investigation.
- Teamwork: delegation, dividing and assigning roles, leadership.
- Cooperation and information sharing.
- Ability to convey the big picture.
- Reporting.
- Crisis communication.
- Time management and prioritisation.

4.4.3. Result

The aim of the proof of concept was to measure the preparedness of the team before the exercise to predict the winner of the exercise.

My prediction was the following, before the exercise: ‘Taking account the exercise experience, the specific Locked Shield exercise experience working in a team, and working with the tools, I assume that blue team 17 will win the test run however blue team 9 is also very strong.’

The final result in Figure 15 shows that blue team 17 won the exercise as predicted using the developed methodology.

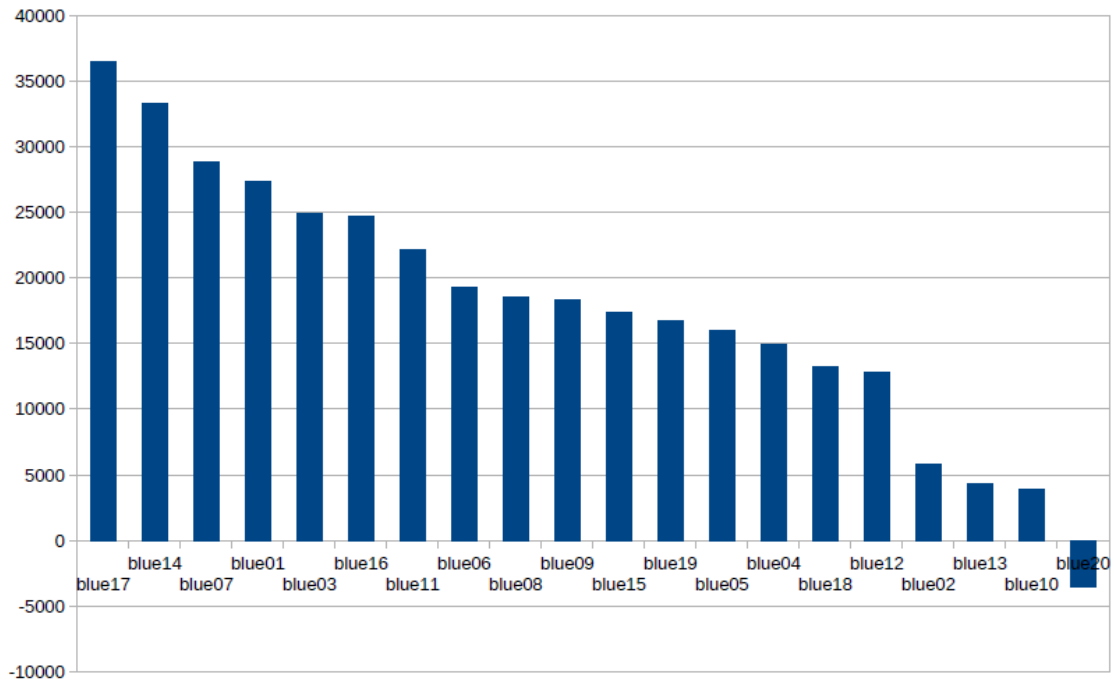


Figure 15. LS 16 exercise final scores.

The survey for the exercise got 119 answers (44%) of the 268 blue team members. The required sample size would have been 159 if the confidences level 95% and the margin error 5%. The data sample was too small to confirm the hypotheses; however the online survey responses rate it was above average. Blue team 5 had not submitted any answer and blue team 3 and 6 submitted only one answer. In order to be able to perform the analysis the answers from these three teams were not taken into account.

The data collection included the pre-exercise questionnaire before the execution. The full analysis of the questionnaire is available in Appendix5. Table 5 shows the competence differences between blue teams 9-10 and 16-17.

Table 5. LS '16 pre exercise survey blue team 9-10 and 16-17.

	Team size	14	14	14	14
	Number of answers	3	7	4	2
	Avg	21%	50%	29%	14%
	Teams	**B9**	**B10**	**B16**	**B17**
1	How many technical exercises have you participated? (avg)	5,666666667	2,857142857	3,25	9,5
2	How many Locked Shields have you participated? (avg)	1,333333333	1,142857143	1,5	2,5
3	How many years operational/real life experience do you have? (avg)	5	7,857142857	10	18,5
4	How many hours have you spent for team preparation? (avg)	61,66666667	33,57142857	13,75	22,5
5	How many hours experience do you have with your tools you going to use in the exercise?	more than 100 (33,33%)	3--10 (42,86%)	10-50 (50%)	10-50 (50%)
6	What is your team's organisational structure (decision making)?	hiearchical (100%)	functional (71,43%)	functional (75%)	matrix (100%)
7	How long have you known each other as a team?	1 year (33,33%)	2 days (14,29%)	1 month (25%)	20 (50%)
8	Do you have an experience of working in ad hoc teams (like Rapid Reaction Team)?	No (100%)	No (57,14%)	No (75%)	Yes (100%)
	Media	No (66,67%)	No (57,14%)	Yes (50%)	Yes (100%)
	Routing	Yes (100%)	Yes (71,43%)	Yes (50%)	Yes (100%)
	Forensics	Yes (100%)	Yes (57,14%)	Yes (50%)	Yes (100%)
	Legal	Yes (100%)	Yes (71,43%)	Yes (50%)	Yes (100%)
	PLC	No (100%)	No (71,43%)	Yes (50%)	No (100%)
	Admins	Yes (100%)	Yes (100%)	Yes (100%)	Yes (100%)
	Reporting	No (66,67%)	No (57,14%)	Yes (50%)	Yes (100%)
	Monitoring	Yes (100%)	Yes (71,43%)	Yes (100%)	Yes (100%)
9	Drone	No (66,67%)	No (100%)	Yes (50%)	Yes (50%)
10	Do you have functions and duties clearly assigned to the team members?	Yes (100%)	Yes (85,71%)	Yes (100%)	Yes (100%)
11	What is the percentage of new tools in this exercise which you don't use in your daily job (0% - it's the same tools in LS, 100% - all the tools are new for me)? Think about monitoring, reporting, etc. tools.	10% (33,33%)	70% (42,86%)	30% (50%)	30% (100%)
12	Do you expect to win?	Yes (100%)	No (71,43%)	Yes (100%)	No (50%)
13	Do you feel ready for game, or are you confused?	Ready (100%)	Ready (71,43%)	Ready (100%)	Ready (100%)

The first question was about the number of exercises that the team members participated in and the following question focused on the Locked Shield exercise participation. Team members from blue team 17 had participated in an average of 9.5 exercises already, while they participated in 2.5LS exercises on average. The other top team in exercise participation was blue team 9, however this team did not have that much experience with this specific technical exercise.

The third question was about the real life experience. With that it was measured that the experience stayed in the game or exercise environment or the players also had every day, operational experience. As the feedback showed the answering blue team 17 members had more than a decade of real life experience and only blue team 15 had more than 10 years average experience. Regarding the team experience in exercises and real life, blue team 17 scored the highest average.

The following question was about the exercise preparation. Blue team 9 spent more than 60 hours preparing for the exercise, which was double the time for following team. The significant difference here comes from the blue team 9 members who answered 160 hours of preparation. The rest of the teams stated the average number, which is around 20 hours also in other teams.

The next question is about the tools that the team decided to use during the exercise. There were team members in each predicted winning team that has more than 100 hours experience with the assigned tool. However, blue team 8 had the best understanding of the chosen tools.

The next question was about the tools that the team decided to use during the exercise. There were team members in each predicted winning team that had more than 100 hours experience with the assigned tool. However, blue team 8 had the best understanding of the chosen tools.

The next question was about the team structure to identify the decision-making process within the team. During the previous survey the question was asked the same when asking: ‘how many people in your team are keeping the team together’, although it could be easily misunderstood. The question provided four possible choices for the teams, and it was very clear that the decision making was centralised in blue team 9. Blue team 17 used matrix structure for team setup.

Questions 7 and 8 also reflected the team's experience. Blue team 17 and 12 had the most experience working in ad-hoc teams which was important when not all the team members worked together before the exercise. Even if some of them knew each other, it was a different experience to learn how to work together as a new ad-hoc team.

During the exercise all the scenario elements were played - above the test run additionally included media play, forensics challenge and legal game. The following questions were about assignment of skilled personnel to each area played during the exercise. Most of the teams had difficulties covering every area with skilled personnel. Blue team 9 and 17 managed to cover most of the areas and clearly assign duties to team members. Blue team 17 indicated that the team had no skilled personnel for the critical information infrastructure play, which was an air conditioning system with programmable logic controller (PLC). During the game, blue team 17 lost the control

over the PLC and the air conditioning system blown up. Consequently they lost some of the services that were assigned virtually in that server room. However the team managed to overcome the loss and ensure continuity. They transferred the affected services to other environment and it did not affect the availability and usability scores.

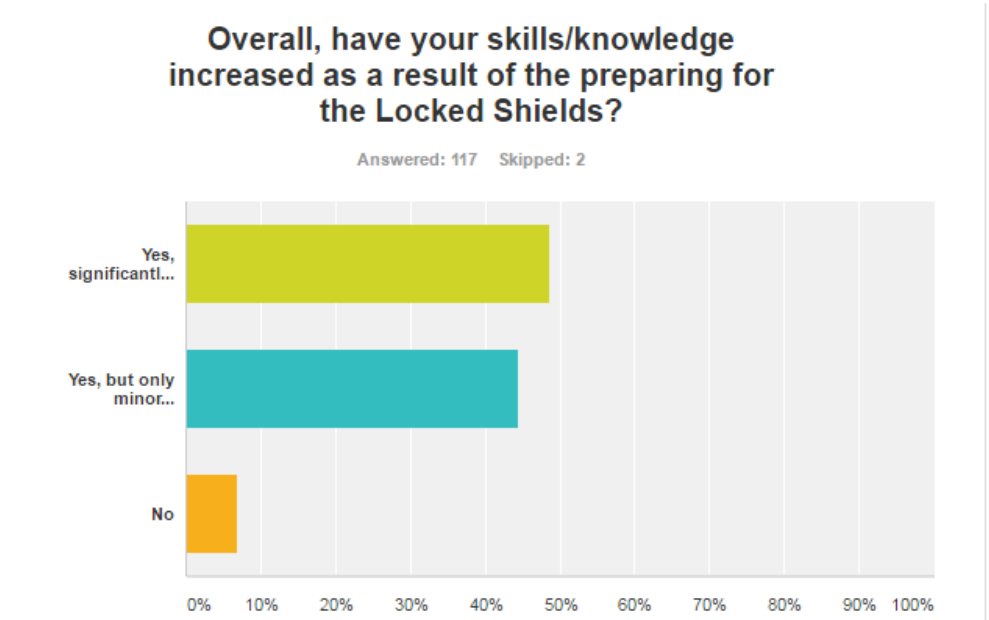
The next question was about the tools the teams wanted to use during the exercise. Blue team 15 had not introduced any new tool for the game and blue team 9 also wanted to keep the level of new tools below.

The following questions were about the team spirit and readiness where only three teams said yes 100% that they expected to win including blue team 9 and 17. Six teams of twenty felt ready for the game. Future analysis needed through interview to identify the root cause of confusion. 28% of the answerer felt confused before the execution. In new team the confusion was bigger, in blue team 2 it was 80% and in blue team 20 it was 42%. The root cause could be the complexity of the game and scoring and the information overload. Participants might need more informative collaboration environment to support preparation and reduce confusion.

The survey evaluation and winner prediction were done a day before the exercise. The winner prediction is available in Appendix 6 and also attached as a separate signed e-document.

Blue team 17 scored most of the highest scores overall, particularly in preparation, but there were no significant difference between blue teams 9 and 17.

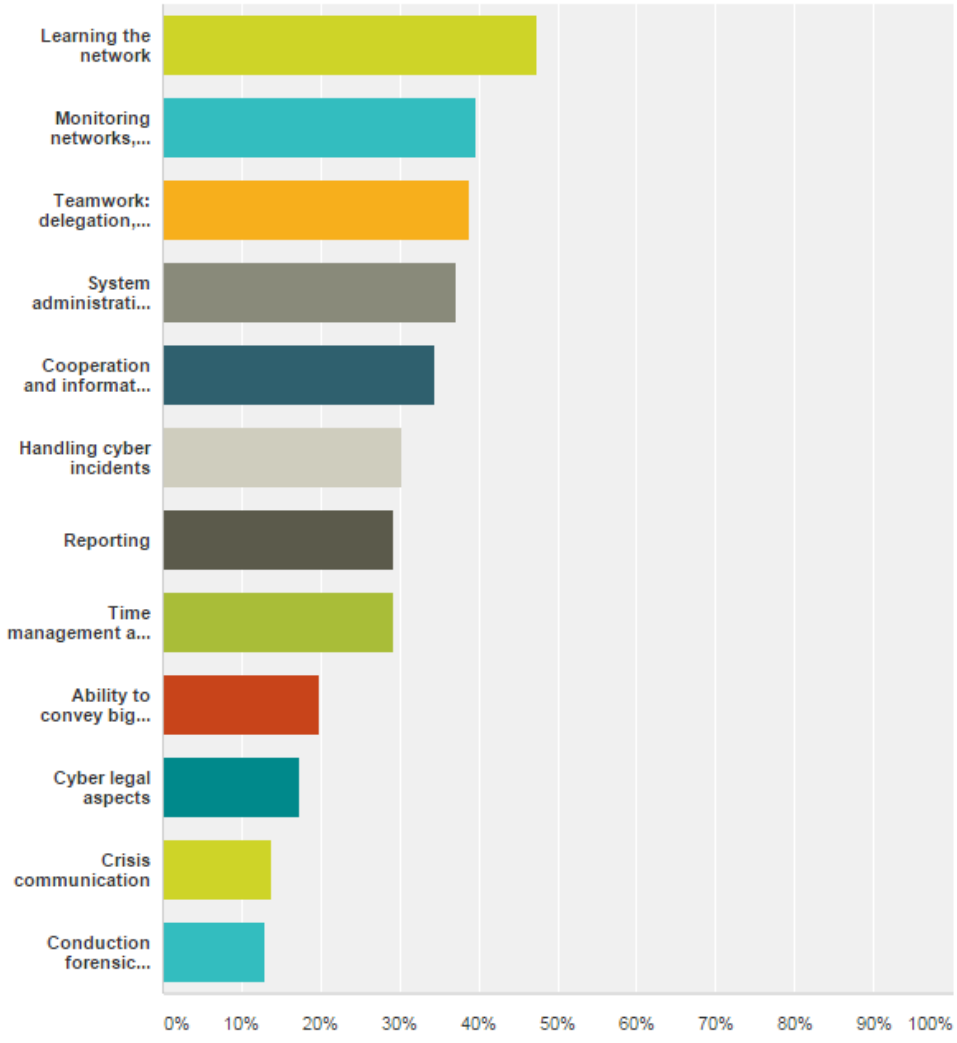
There were three additional questions that wanted to highlight the learning perspective in the exercise preparation phase. Figure 16 shows that 93% of the participants felt that their skills improved to some extent as a result of the exercise preparation.



Answer Choices	Responses	
Yes, significantly increased	48.72%	57
Yes, but only minor improvement	44.44%	52
No	6.84%	8
Total		117

Figure 16. Skills and knowledge improvement as a result of preparing for Locked Shields.

The next question wanted to identify the top three skills that exercise participants had learned in the preparation process. The learning network was the skill that improved most of the exercise participants, as shown in Figure 16.

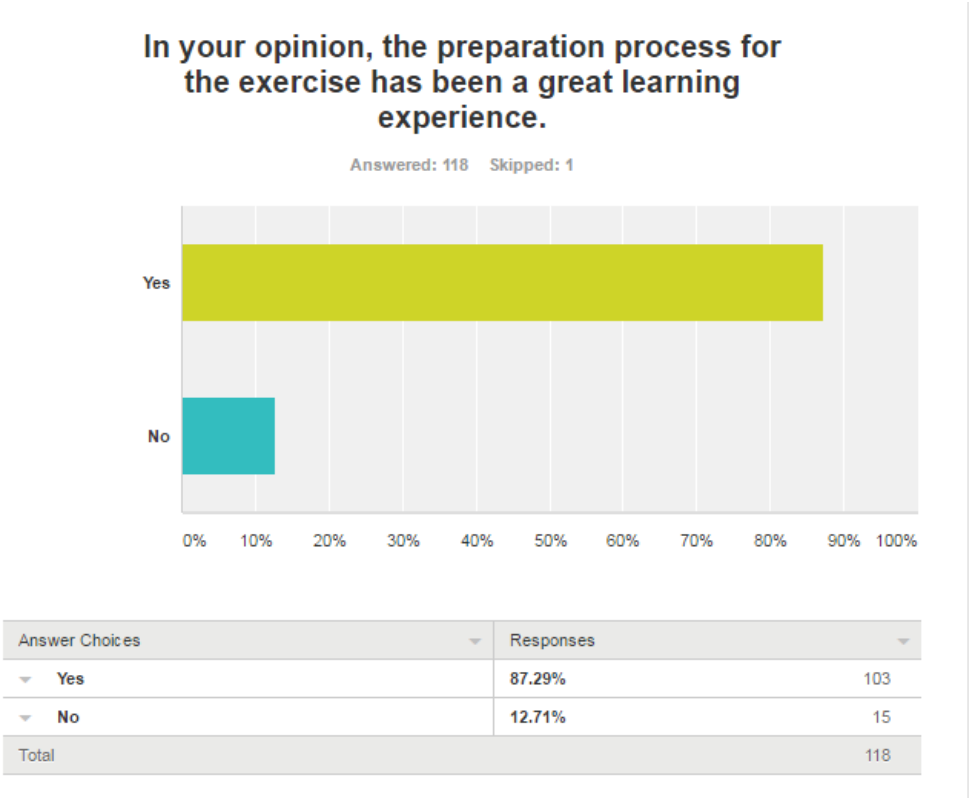


Answer Choices	Responses	
Learning the network	47.41%	55
Monitoring networks, detecting and responding to attacks	39.66%	46
Teamwork: delegation, dividing and assigning roles, assignment	38.79%	45
System administration and prevention of attacks	37.07%	43
Cooperation and information sharing	34.48%	40
Handling cyber incidents	30.17%	35
Reporting	29.31%	34
Time management and prioritization	29.31%	34
Ability to convey big picture	19.83%	23

Figure 17. Top 3 new sills/knowledge had been learned in the preparation process.

Although LS was a highly technical exercise, there was a non-technical skill development in the top three as listed in Figure 17. Learning teamwork was one of the most important skills learned by the exercise participants.

The technical exercise provided an effective environment to put the learned theoretical knowledge into practice. The exercise preparation phase was already a learning experience, as shown in Figure 18. The exercise training audience clearly saw the usefulness of exercise preparation.



Answer Choices	Responses	
Yes	87.29%	103
No	12.71%	15
Total		118

Figure 18. Preparation process is a learning experience.

The exercise participants were questioned also about their view about the exercise that is a game or a learning event for them. The feedback clearly showed in Figure 19, that only 2 out of 17 responses saw it as a competition, everyone else as learning.

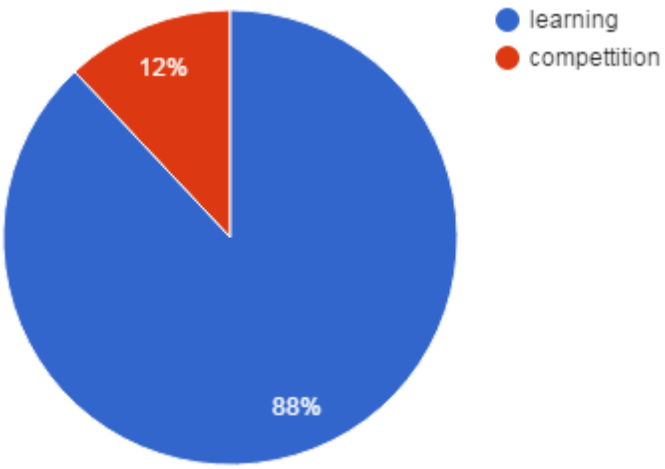


Figure 19. Learning or competition.

For the scoring the data collection included: exercise environment automatic performance scoring, red team attack scoring, cooperation scoring, white team scorings, which put together the final scores, as seen in Figure ***20***.

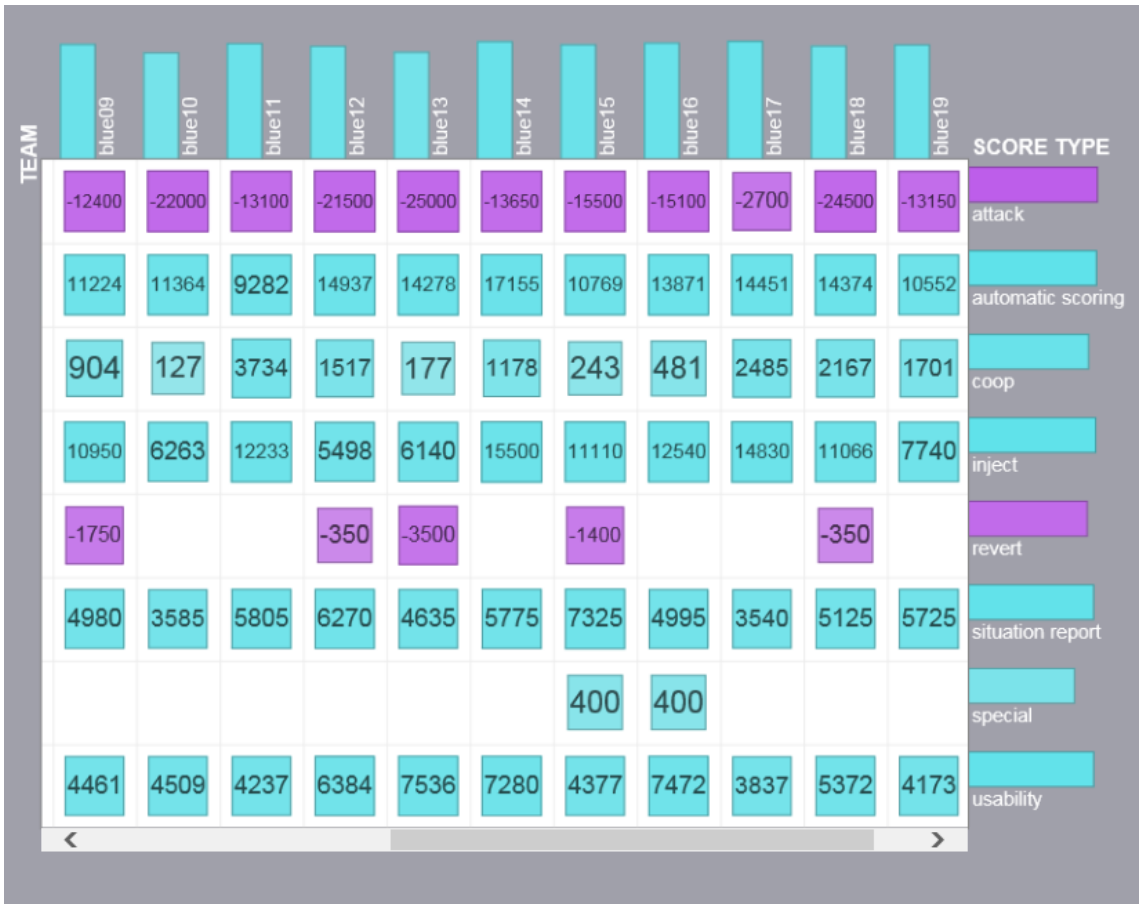


Figure 20. LS 16 scores by types.

During the execution, the same scoring was applied as during the test run. There were eight categories of scores. The difference of actual run scoring was in the availability scoring. The availability of services is calculated independently for each game-day (8hours) and scoring was exponential. The test run was only one day the execution was a two day long exercise. The teams got 40 injects during the execution, which included forensics challenge, legal play and also more injects in scenario and media.

The winning team was blue team 17, as predicted using the developed methodology.

The winning team applied a highly defensive strategy and got the best score for defending successful red team attacks. The difference was 8300 points compared with the next best team. Blue team 17 also got the second place in injects scoring. The team was also creative when the simulated air conditioning exploded. In the pre-exercise survey the team stated that they have no experience with industrial systems, which in this case the air conditioning programmable logic controller. However, when the air

conditioning exploded the team migrated all of the virtual services to different location and provided the services. The weak side of blue team 17 was the usability, which was measured by simulated users and situational reports. In these areas the team came in last place.

5. Conclusion

As a result of this thesis an overview of cyber security exercises and their information sharing was provided along with the identification of pre-exercise performance objectives. The thesis addressed the problem of effective information sharing.

The thesis hypotheses were tested:

1) The number and complexity of cyber exercises are growing.
2) The existing information sharing patterns are used only to share pieces of information.
3) There are key indicators to prepare for technical exercises.

The analysis of the dataset – consisting of over 120 exercises and reviewing literatures such as studies on cyber exercises and cyber exercise after action reports – identified the following patterns: increase the number of exercises, increase the number of cooperation exercises and private sector involvement. The increase was partly driven by policy demand and also awareness of exercise planners, participants and stake holders. The other identified pattern was the growth of complexity in the large scale exercises. They became more complex due to involving more Nations, more organisations and more participants consequently the planning was more complex, which could take a whole year. The growth of complexity of the large scale exercises could cause confusion, the exercise members desired more user-friendly collaboration environment to have easier access to exercise's information which supports better preparation and reduces confusion.

There is no common information sharing pattern identifiable that was used to share exercise information. There were only a few numbers of exercises that share exercise lessons learned. The lessons were shared in many different channels, depending on the involved community of interest. The top-down information sharing approach can only work in those organisations where there is a strong culture of sharing lessons learned. The bottom-up approach is used in communities that are built around a certain cyber security topic. The combination of a top-down and bottom-up, a community of interest grouping, approach can result in better and faster information sharing. The exercise

outcome and information need to feed the information sharing network from these two directions. One is the top-down approach, where the complex after action report is shared, using the exercise classification model introduced in this thesis. It provides richer meta data, that supports easier search and identification. The other is tailored input, once to feed the bottom-up sharing in communities and second to insert directly into courses, which is one of the best preparation sources as questionnaire results showed.

The analysis of XS ‘16 exercise participants’ survey showed the added value of participating technical exercises and also highlighted the performance differences among those who had more exercise experience previously. The ones who participated in more exercises performed better and had more successful attacks during XS. Participating exercises was a very important step of the learning experience, but not a unique source of the best performance. The participants highlighted the importance of the individual preparation that leads to good performance. The individual preparation and courses as primary sources of information can be used as an input to exercise outcomes from cyber exercises: observations and lessons learned. In that way the pre-exercise preparation can be more effective.

The LS ‘16 exercise test run and the execution were used to test the concept that there are key exercise preparation indicators. Using the indicators the participants can better focus their preparation, furthermore the team preparedness can be measured before the exercise and the winner can be predicted. The indicators were tested using a pre-exercise questionnaire. The collected data included individual experience, team experience, team organisation, teamwork and team spirit. The survey used during LS ‘16 test run was slightly modified for the execution to allow better measurement. There were 20 blue teams during the exercise and 119 blue team members answered the pre-exercise questionnaire. The exercise outcome prediction was carried out one day before the exercise execution and the winner was predicted correctly, however the second was different as expected. The identified and tested key indicators allowed predicting the winner, but future study and test required to identify the final set of key indicators. They need to be tested through number of exercises and on the required sample size to proof hypothesis 3. The results showed that indicators can be identified and highlighted the importance and complexity of exercise preparation.

Participation in technical exercises provides a great opportunity to learn through practice; 93% of participants felt that their skills improved to some extent as a result of exercise preparation and 88% saw it as a learning event. Exercises and competitions can be made more equal for all participants by applying pre-exercise survey and integrating the measurement of learning experience into the scoring. It has been not identified to what extent the exercise participants have learned; therefore the effectiveness of learning during technical exercises is a potential direction for future research.

References

[1] Eurostat, “Analyses data on high-technology or ‘high-tech’ sectors in the European Union (EU) and in some EFTA and candidate countries,” 2015. [Online]. Available: http://ec.europa.eu/eurostat/statistics-explained/index.php/High-tech_statistics. [Accessed: 21-Feb-2015].

[2] J. Dunlosky, K. A. Rawson, E. J. Marsh, M. J. Nathan, and D. T. Willingham, “Improving Students’ Learning With Effective Learning Techniques: Promising Directions From Cognitive and Educational Psychology,” *Psychol. Sci. Public Interes.*, vol. 14, no. 1, pp. 4–58, 2013.

[3] S. Deterding, D. Dixon, R. Khaled, and L. Nacke, “From game design elements to gamefulness,” *Proc. 15th Int. Acad. MindTrek Conf. Envisioning Futur. Media Environ. - MindTrek ’11*, pp. 9–11, 2011.

[4] K. Werbach, “(Re)defining gamification: A process approach,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014, vol. 8462 LNCS, pp. 266–272.

[5] a. T. Sherman, B. O. Roberts, W. E. Byrd, M. R. Baker, and J. Simmons, “Developing and delivering hands-on information assurance exercises: experiences with the cyber defense lab at UMBC,” *Proc. from Fifth Annu. IEEE SMC Inf. Assur. Work. 2004.*, no. June, pp. 10–11, 2004.

[6] M. Ernits and J. Tammekänd, “i-tee : A fully automated Cyber Defense Competition for Students Categories and Subject Descriptors,” *Proc. ACM SIGCOMM (Poster/demo Sess.*, pp. 113–114, 2015.

[7] T. Sommestad and J. Hallberg, “Cyber security exercises and competitions as a platform for cyber security experiments,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7617 LNCS, pp. 47–60, 2012.

[8] A. G. Kotulic and J. G. Clark, “Why there aren’t more information security

research studies," *Inf. Manag.*, vol. 41, no. 5, pp. 597–607, May 2004.

[9] L. A. Gordon, M. P. Loeb, and W. Lucyshyn, "Sharing information on computer systems security: An economic analysis," *J. Account. Public Policy*, vol. 22, no. 6, pp. 461–485, 2003.

[10] "UNESCO International Bureau of Education." [Online]. Available: http://www.ibe.unesco.org/en. [Accessed: 23-Feb-2016].

[11] "OECD, PISA results." [Online]. Available: http://www.oecd.org/pisa/keyfindings/pisa-2012-results.htm.

[12] P. Trimintzios and R. Gavrila, "On National and International Cyber Security Exercises Survey, Analysis and Recommendations," 2012.

[13] ENISA, "The 2015 Report on National and International Cyber Security Exercises," 2015.

[14] NATO CCD COE, "Cyber Security Strategy Documents, NATO Cooperative Cyber Defence Centre of Excellence," 2015. [Online]. Available: https://ccdcoe.org/cyber-security-strategy-documents.html. [Accessed: 22-Feb-2016].

[15] European Union, "Europian Union: Network and Information Security Directive," *2015*. [Online]. Available: https://ec.europa.eu/digital-agenda/en/news/network-and-information-security-directive-co-legislators-agree-first-eu-wide-legislation. [Accessed: 22-Feb-2016].

[16] European Union, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final - 7/2/2013 (2013)." European Union, Brussels, p. 20, 2013.

[17] R. Ottis, "Light weight tabletop exercise for cybersecurity education," *J. Homel. Secur. Emerg. Manag.*, vol. 11, no. 4, pp. 579–592, 2014.

[18] Spanish National Cybersecurity Institute, "Cyber Exercises taxonomy," Madrid, 2015.

[19] J. Marshall, “The cyber scenario modeling and reporting tool(CyberSMART),” *Proc. - Cybersecurity Appl. Technol. Conf. Homel. Secur. CATCH 2009*, pp. 305–309, 2009.

[20] R. Gurnani, K. Pandey, and S. K. Rai, “A scalable model for implementing cyber security exercises,” *2014 Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2014*, pp. 680–684, 2014.

[21] Homeland Security, “Informing Cyber Storm V: Lessons Learned from Cyber Storm IV,” no. June, 2015.

[22] D. Hoffman, Lance , Ragsdale, “Exploring a National Cyber Security Exercise for Colleges and Universities,” 2004.

[23] L. J. Hoffman, T. Rosenberg, R. Dodge, and D. Ragsdale, “Exploring a national cybersecurity exercise for universities,” *IEEE Secur. Priv.*, vol. 3, no. 5, pp. 27–33, 2005.

[24] G. Vigna, “Teaching Network Security through Live Exercises,” in *Security Education and Critical Infrastructures SE - 2*, vol. 125, C. Irvine and H. Armstrong, Eds. Springer US, 2003, pp. 3–18.

[25] A. Conklin, “Cyber defense competitions and information security education: An active learning solution for a capstone course,” *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 9, no. C, pp. 1–6, 2006.

[26] A. L. M. Luigi Ferrara, Christian Mårtenson, Pontus Svenson, Per Svensson, Justo Hidalgo, Anastasio Molano, “Integrating Data Sources and Network Analysis Tools to Support the Fight Against Organized Crime,” *Intell. Secur. Informatics Work.*, vol. 5075, pp. 171–182, 2008.

[27] C. Chiu, M. Hsu, and E. Wang, “Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories,” *Decis. Support Syst.*, vol. 42, no. 3, pp. 1872–1888, 2006.

[28] “EISAS (enhanced) report on implementation.” [Online]. Available: https://www.enisa.europa.eu/publications/eisas-report-on-implementation-

enhanced. [Accessed: 18-May-2016].

[29] C. Infrastructure, L. Dandurand, and O. S. Serrano, “Towards Improved Cyber Security Information Sharing,” *5th Int. Conf. Cyber Confl.*, 2013.

[30] “ITU Study Group 17.” [Online]. Available: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybex.aspx. [Accessed: 17-May-2016].

[31] A. Rutkowski, Y. Kadobayashi, I. Furey, D. Rajnoivc, R. Martin, and T. Takahashi, “CYBEX: the cybersecurity information exchange framework (x. 1500),” *Acm Sigcomm*, vol. 40, no. 5, pp. 59–64, 2010.

[32] “PDD 63.” [Online]. Available: http://fas.org/irp/offdocs/pdd/pdd-63.htm. [Accessed: 18-May-2016].

[33] “Capture The Flag exercise write ups (GitHub),” 2013. [Online]. Available: https://github.com/ctfs. [Accessed: 28-Mar-2016].

[34] International Organization of Standardization (ISO), *International Standard, Societal Security - Guidelines for exercises ISO-22398-2013*. ISO, 2013.

[35] B. E. Mullins, T. H. Lacey, R. F. Mills, J. M. Trechter, and S. D. Bass, “The impact of the NSA cyber defense exercise on the curriculum at the air force institute of technology,” *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 1–9, 2007.

[36] “Cyber Defence Exercise, Cyber Research Centre Unitied States Military Academy, West Point.” [Online]. Available: http://www.usma.edu/crc/SitePages/CDX.aspx. [Accessed: 29-Mar-2016].

[37] W.J. Schepens, D.J. Ragsdale, J.R. Surdu, J. Schafer and R.I. New Port “The Cyber Defense Exercise: An evaluation of the effectiveness of information assurance education,” *J.of Inf.Sec., vol.1,* pp. 1–14, 2002.

[38] NATO CCD COE, “Locked Shields 2015 exercise.” [Online]. Available: https://ccdcoe.org/locked-shields-2015.html. [Accessed: 16-Mar-2016].

[39] “The University of California, Santa Barbara, iCapture The Flag Competition.” [Online]. Available: https://ictf.cs.ucsb.edu/. [Accessed: 15-Mar-2016].

[40] “Ghost in the Shellcode.” [Online]. Available: http://ghostintheshellcode.com/. [Accessed: 15-Mar-2016].

[41] “RuCTFE - Online international challenge of information security.” [Online]. Available: https://ructf.org/e/2015/index.html. [Accessed: 15-Mar-2016].

[42] “Nuit Du Hack.” [Online]. Available: https://nuitduhack.com/en/. [Accessed: 15-Mar-2016].

[43] “Chaos Computer Club Aachen.” [Online]. Available: https://aachen.ccc.de/. [Accessed: 15-Mar-2016].

[44] “Insomni’hack Swiss security conference and ethical hacking contest.” [Online]. Available: http://insomnihack.ch/. [Accessed: 15-Mar-2016].

[45] “DEFCON.” [Online]. Available: https://defcon.org/. [Accessed: 15-Mar-2016].

[46] “Codgate - International Hacking Competition & IT Security Conference.” [Online]. Available: http://codegate.org/. [Accessed: 15-Mar-2016].

[47] “Hack Lu.” [Online]. Available: http://2015.hack.lu/. [Accessed: 15-Mar-2016].

[48] “Plaid CTF.” [Online]. Available: http://plaidctf.com/. [Accessed: 15-Mar-2016].

[49] “Positive Hack Days.” [Online]. Available: http://www.phdays.com/. [Accessed: 15-Mar-2016].

[50] “HackIM.” [Online]. Available: http://ctf.nullcon.net/. [Accessed: 15-Mar-2016].

[51] “Seccon.” [Online]. Available: http://ctf.seccon.jp/. [Accessed: 15-Mar-2016].

[52] “CTF Time.” [Online]. Available: https://ctftime.org/ctfs. [Accessed: 15-Mar-2016].

[53] G. Vigna, K. Borgolte, J. Corbetta, A. Doupe, Y. Fratantonio, L. Invernizzi, D. Kirat, and Y. Shoshitaishvili, “Ten Years of iCTF: The Good, The Bad, and The Ugly,” in *USENIX*, 2014.

[54] M. Granåsen and D. Andersson, “Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study,” *Cogn. Technol. Work*, pp. 121–143,

2015.

[55] “NATO Cyber Range.” [Online]. Available: http://www.act.nato.int/sact-and-the-estonian-minister-of-defence-sign-an-agreement-to-establish-the-nato-cyber-range-capability. [Accessed: 02-Apr-2016].

[56] “Cyber Defence Exercise Locked Shields 2013 After Action Report,” 2013.

[57] “NATO CCD COE Locked Shields forensics challange workshop.” [Online]. Available: https://ccdcoe.org/locked-shields-forensics-challenge-workshop.html. [Accessed: 01-Apr-2016].

[58] “NATO CCD COE Cyber Defence Monitoring Course Suite - Module 3, Large Scale Packet Capture and Analysis Course.” [Online]. Available: https://ccdcoe.org/cyber-defence-monitoring-course-suite-module-3.html. [Accessed: 01-Apr-2016].

[59] G. Fink, D. Best, D. Manz, V. Popovsky, and B. Endicott-Popovsky, “Gamification for measuring cyber security situational awareness,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8027 LNAI, pp. 656–665, 2013.

[60] R. K. Yin, *Case Study Research: Design and Methods*, vol. 5, no. 5. Sage Publications, 2009.

[61] J. L. Bayuk and A. Mostashari, “Measuring cyber security in intelligent urban infrastructure systems,” in *2011 8th International Conference and Expo on Emerging Technologies for a Smarter World, CEWIT 2011*, 2011.

Appendix 1 – Data of XS exercise survey

List your main or primary information sources of developing your skills« »	Exercise observations« »	Exercise lessons learned« »	Exercise after action report« »	Information about used tools« »	Sharing exercise technical environment« »	Online forums« »	Participating exercises« »
self learning	4	4	5	4	2	2	5
	5	5	5	5	5	5	5
Self & Team members	4	4	5	3	4	3	4
Internet	4	4	5	5	4	4	4
exercises and attending schools	5	5		4	4	5	5
Everyday work, courses and trainings atte	4	4	4	3	5		5
internet	4	5	4	4	4	4	5
learning by doing	4	4	3	4	5	5	5
self learning	3	4	2	4	3	4	4
internet	4	3	3	5	5	2	4
during the game it is faster to get info from	5	3	3	3	4	5	5
self learning	4	4	5	5	4	3	5
google	4	5	4	3	5	4	4
All 3 teams via team leads translation obj	4	4	4	3	4	4	4
personal interest, work projects, locked st	1	2	4	4	4	3	5
Technical courses + workshops, self stud	4	4	4	5	4	4	5
N (counta)	16	16	15	16	16	15	16
Blanks	0	0	1	0	0	1	0
Total	16	16	16	16	16	16	16
Counts (countif)							
Not important (1)	1	0	0	0	0	0	0
Slightly important (2)	0	1	1	0	1	2	0
Moderately important (3)	1	2	3	5	1	3	0
Important (4)	11	9	6	6	9	6	6
Extremly important (5)	3	4	5	5	5	4	10
Total	16	16	15	16	16	15	16
Valid percents							
Not important (1)	6%	0%	0%	0%	0%	0%	0%
Slightly important (2)	0%	6%	7%	0%	6%	13%	0%
Moderately important (3)	6%	13%	20%	31%	6%	20%	0%
Important (4)	69%	56%	40%	38%	56%	40%	38%
Extremly important (5)	19%	25%	33%	31%	31%	27%	63%
Total	100%	100%	100%	100%	100%	100%	100%

« »	What was you IP in Crossed Swords« »	How old are you« »	How many exercises have you participated« »	What was your role in those exercises« »	How many successful attacks have you done during the exercise« »	List your main or primary information sources of developing your skills« »	Exercise observations« »	Exercise lessons learned« »	Exercise after action report« »	Information about used tools« »	Sharing exercise technical environment« »	Online forums« »	Participating exercises« »
Feedback-0211100500	0	29	5	RT CS member	10 unique and 30	self learning	4	4	5	4	2	2	5
Feedback-0211133912		29	1	NET_RT	15		5	5	5	5	5	5	5
Feedback-0211134030	10.242.0.1xx	29	1	Red Team	03/02/2016	Self & Team members	4	4	5	3	4	3	4
Feedback-0211134129	10.242.0.105	40	3	blue, red_cs, red	4 phishing campa	Internet	4	4	5	5	4	4	4
Feedback-0211134204	10.242.0.108	46	3	Client side attack	6	exercises and attending schools	5	5		4	4	5	5
Feedback-0211134244	10.242.0.123,10.	24	1 - this was the first	RT-WEB	1 (other ones not	Everyday work, courses and trainings atte	4	4	4	3	5		5
Feedback-0211134323	10.242.0.104	25	1	RT_CS	2	internet	4	5	4	4	4	4	5
Feedback-0211134334	10.242.0.10x	36	0	RT_CS	didn't count	learning by doing	4	4	3	4	5	5	5
Feedback-0211134357	10.242.0.1XX	36	2	CS	8 succesful	self learning	3	4	2	4	3	4	4
Feedback-0211134429	10.242.0.116	31	2	RT_NET	5	internet	4	3	3	5	5	2	4
Feedback-0211134508	10.242.0.135,10.	39	2	NET	3	during the game it is faster to get info from	5	3	3	3	4	5	5
Feedback-0211134537	10.242.0.157	40	1	RT_NET	At least 1	self learning	4	4	5	5	4	3	5
Feedback-0211134646	10.242.0.122	32	1	RED TEAM	4	google	4	5	4	3	5	4	4
Feedback-0211135212	8.8.8.8	33	2	RT Lead	0	All 3 teams via team leads translation obj	4	4	4	3	4	4	4
Feedback-0212115027		29	4	Network	3	personal interest, work projects, locked st	1	2	4	4	4	3	5
Feedback-0216155625		44	4	3x Blueteam, 1x	YT-none	Technical courses + workshops, self stud	4	4	4	5	4	4	5

Appendix 2 – Data of LS test run exercise survey

Respon	Collecto	StartDate	EndDate	IP Addr	Email A	Please sele	How ma	How many	How ma	How many	How many	ople in t	How lo	Do you	ve an ex	Do you	ve all th	Do you	ve functi	Does yo	team m	What is	Do you	pect to v	Do you	I ready for game, or are you confused?
4,55E+09	81714533	03/02/2016	03/02/2016	193.40.250.232		Blue 1	0	2	0	10	2		4 months	No		No		Yes		Yes		90%	Yes		Confused	
4,55E+09	81714533	03/03/2016	03/03/2016	85.253.201.107		Blue 2	2	2	3	5	2		Beginning	No		Yes		Yes		Yes		70%	No		Ready	
4,55E+09	81714533	03/02/2016	03/02/2016	90.190.170.196		Blue 2	1	0	20	12	0	At the mor	As a team	No	Not really,	Yes		Yes	I do think \	Yes		80%	No	No real ex	Ready	
4,55E+09	81714533	03/02/2016	03/02/2016	89.235.249.163		Blue 2	0	0	3	10	3		about 6 m	No		No		Yes		Yes		80%	No		Confused	I am not very proficient with the tools I will have to use, and I am not sure to be able to handle a live situation
4,55E+09	81714533	03/02/2016	03/02/2016	82.147.163.104		Blue 2	0	2	4	12	2		As individu	Yes		Yes		Yes		Yes		80%	No		Confused	
4,55E+09	81714533	03/02/2016	03/02/2016	90.191.23.167		Blue 2	0	1	0	15	4		not more t	Yes		Yes		Yes		Yes		60%	No		Confused	
4,55E+09	81714533	03/02/2016	03/02/2016	85.253.75.40		Blue 2	0	0	50	30	5		6 months	No		Yes		Yes		Yes		80%	No		Ready	
4,55E+09	81714533	03/02/2016	03/02/2016	193.40.250.236		Blue 2	1	1	7	12	3		About one	No	In a busine	No	SCADA skil	Yes	Each Blue t	Yes	Our group	70%	No	We expect	Ready	I know what I know, and I know what I dont know. As students with no previous experience, one month is not enough close all the gaps in knowledge that have been identified. I chose the "ready" option because we have done as much as we can..
4,55E+09	81714533	03/02/2016	03/02/2016	88.196.244.129		Blue 2	0	0	0	50	2	1 team lea	We know e	No	-	No	No, we are	Yes	-	Yes	-	100%	No	I miss the (	Confused	Ready is a too big word, so is confused. It is simpy difficult to imagine how the real game will go. So we dive into the deep, and prepare as good as we can.
4,55E+09	81714533	03/02/2016	03/02/2016	192.40.88.13		Blue 2	3	3	2	3	5		a month	No		No	No membe	Yes		Yes		100%	Yes		Confused	
4,55E+09	81714533	03/02/2016	03/02/2016	193.40.250.233		Blue 2	1	1	4	15	5		1 semester	No		Yes		Yes		Yes		80%	Yes	I will do m	Ready	Something between those 2 options
4,56E+09	81714533	03/05/2016	03/05/2016	46.107.206.159		Blue 3	1	3	50	10	2		2 weeks	Yes		Yes		Yes		Yes		50%	No		Ready	
4,56E+09	81714533	03/04/2016	03/04/2016	89.133.121.187		Blue 3	1	1	50	5	1		Met half th	No		No	We have n	Yes		Yes		30%	No	Dont know	Ready	
4,55E+09	81714533	03/02/2016	03/02/2016	80.98.110.63		Blue 3	2	2	25	10	1		From 2 we	Yes	As a mem	Yes		Yes		Yes		50%	Yes	Maybe	Ready	
4,55E+09	81714533	03/02/2016	03/02/2016	80.98.110.63		Blue 3	4	2	50	5	1		I know the	Yes		Yes	hopefully	Yes		Yes		40%	No	but will do	Ready	
4,55E+09	81714533	03/02/2016	03/02/2016	80.98.110.63		Blue 3	4	5	5	25	1		Long enou	Yes		Yes		Yes		Yes		50%	No	But we wo	Ready	
4,55E+09	81714533	03/02/2016	03/02/2016	193.224.76.134		Blue 3	2	4	5	5	2		3 weeks	No		Yes		Yes		Yes		50%	Yes		Confused	we send some questions about the Test Run, and waiting for answers....
4,56E+09	81714533	03/06/2016	03/06/2016	84.248.124.245		Blue 4	3	5	0	2	2		First meeti	Yes		Yes		Yes		Yes		60%	Yes		Ready	
4,56E+09	81714533	03/06/2016	03/06/2016	84.248.118.178		Blue 4	1	1	2	5	1		One day.	No		Yes		Yes		Yes		40%	Yes		Confused	It will somehow unknown challenge for me, for I have not participated this kind of exercise before.
4,56E+09	81714533	03/06/2016	03/06/2016	85.23.95.98		Blue 4	1	2	10	20	2		2 years	No		Yes		Yes		Yes		30%	Yes		Ready	
4,56E+09	81714533	03/06/2016	03/06/2016	84.250.119.251		Blue 4	6	10	0	5	2		Several yea	Yes	LS12 Pre r	No		Yes		Yes		10%	Yes	Kapsi alwa	Ready	
4,56E+09	81714533	03/06/2016	03/06/2016	84.248.118.178		Blue 4	4	0	1	24	2		There are	Yes	Kapsi has	No	Media / Le	No	There are	Yes	Get Shit Dc	60%	Yes	Our main t	Ready	"Ready" as in expect everything, assume nothing. Thus always ready.
4,56E+09	81714533	03/06/2016	03/06/2016	84.248.118.178		Blue 4	1	0	10	24	2		multiple ye	No		No		No	mostly	Yes		60%	Yes		Ready	
4,56E+09	81714533	03/06/2016	03/06/2016	84.248.118.178		Blue 4	0	0	100	36	2		Several yea	No		Yes		No		Yes		70%	Yes		Ready	
4,56E+09	81714533	03/06/2016	03/06/2016	84.248.118.178		Blue 4	7	4	20	5	2		Many year	No		Yes		Yes		Yes		50%	Yes		Ready	
4,56E+09	81714533	03/06/2016	03/06/2016	84.248.118.178		Blue 4	7	4	20	5	10	everyone!	Several yea	Yes	Other exer	Yes		Yes	However, (	Yes		50%	No	But we will	Ready	Ready but never know what's coming up... :)
4,56E+09	81714533	03/05/2016	03/05/2016	84.248.118.178		Blue 4	0	0	4	2	2		Few weeks	Yes		Yes		Yes		Yes		30%	Yes		Ready	
4,55E+09	81714533	03/03/2016	03/03/2016	193.40.244.197		Blue 5	0	5	10	5	10	about 10	It varies. B	No	some of us	No	More or le	Yes	working or	Yes	More like y	20%	Yes	Absolutely!	Ready	Ready as hell!

Appendix 3 – LS test run winner prediction

LS 16 test run pre-survey outcome

Date/time: 09-03-2016, 22:10

The test run blue team 1 and 5 has provided only one-one answer for the survey. Consequently the sample size is too small for analysis.

The average has been taken for the first 5 questions.

Taking account the experience working in a team, and working with the tools, additionally the second positions in real life and exercise experience I assume that blue team 3 will win the test run however blue team 4 is also very strong.

	Number of Answers	1	10	6	10	1
	Teams	**B1**	**B2**	**B3**	**B4**	**B5**
1	How many exercises have you participated? (avg)	0	0,8	2,33333333	3	0
2	How many years operational/real life experience do you have? (avg)	2	1	2,83333333	2,6	5
3	How many hours experience do you have with your tools you going to use in the exercise? (avg)	0	9,3	30,8333333	16,7	10
4	How many hours have you spent for team preparation?	10	16,4	10	12,8	5
5	How many people in your team are keeping the team together? (avg)	2	3,1	1,33333333	2,7	10
6	Do you have an experience of working in ad hoc teams (like Rapid Reaction Team)?	No	No (80%)	Yes (66%)	N/A (50%)	No
7	Do you have all the areas covered by appropriate personnel (e.g. media, legal, situational reporting, etc.)?	No	Yes (60%)	Yes (84%)	Yes (70%)	Yes (70%)
8	Do you have functions and duties clearly assigned to the team members?	Yes	Yes (100%)	Yes (100%)	Yes (70%)	Yes
9	Does your team members know their functions and duties?	Yes	Yes	Yes	Yes	Yes
10	What is the percentage of new tools in this exercise which you don't use in your daily job (0% - it's the same tools in LS, 100% - all the tools are new for us)? Think about monitoring, reporting, etc. tools.	90%	80%	45%	46%	20%
11	Do you expect to win?	Yes	No (80%)	No (66%)	Yes (90%)	Yes
12	Do you feel ready for game, or are you confused?	confused	N/A (50%)	ready (84%)	ready (90%)	ready

Appendix 4 – Data of operational planner's survey

Please list your main or primary information sources of developing your skills	Exercise planning information portal	Exercise observations	Exercise lessons learned	Exercise after action report	Information about used processes	Information about used tools	Sharing technical exercise environment (virtual machines)	Participating exercises
0	5	5	5	5	4	5	5	5
NATO sources	5	5	5	5	5	5	3	4
US mil training, US commercial training	2	4	5	4	5	4	2	5
staff training, doctrine, nato sources	5	4	5	4	3	4	3	5
policy, strategy, oplans,	5	3	3	2	0	1	4	4
exercise documentation, nato references	5	3	2	2	3	3	3	2
work experience, workin in different aras, exercises, courses	5	4	3	5	3	3	4	4
cyber security coursess, learning team leader, cyber defence courses	4	4	5	5	4	4	4	4
working groups, participants in exercises, II meetings	4	4	5	5	5	5	0	4
Exercise observations, Exercise LL, participating exercises	3	5	5	4	3	3	3	5
Exercise participation, exercise planning	4	5	5	4	4	5	4	5
info sharing same assingments, doctrines	4	3	4	3	4	3	4	5

N (counta)

Cunts (countif)								
Not important (1)	0	0	0	0	0	1	0	0
Slightly important (2)	1	0	1	2	0	0	1	1
Moderately important (3)	1	3	2	1	4	4	4	0
Important (4)	4	5	1	4	4	3	5	5
Extremly important (5)	6	4	8	5	3	4	1	6
Total	12	12	12	12	11	12	11	12

Valid percents								
Not important (1)	0%	0%	0%	0%	0%	8%	0%	0%
Slightly important (2)	8%	0%	8%	17%	0%	0%	9%	8%
Moderately important (3)	8%	25%	17%	8%	36%	33%	36%	0%
Important (4)	33%	42%	8%	33%	36%	25%	45%	42%
Extremly important (5)	50%	33%	67%	42%	27%	33%	9%	50%
Total	100%	100%	100%	100%	100%	100%	100%	100%

How many exercises have you participated?	What was your role in the exercises?	Please list your main or primary information sources of developing your skills	Exercise planning information portal	Exercise observations	Exercise lessons learned	Exercise after action report	Information about used processes	Information about used tools	Sharing technical exercise environment (virtual machines)	Participating exercises	If you can make changes that can dramatically improve sharing, what would they be?
0	0	0	5	5	5	5	4	5	5	5	0
5	cyber/excon/J6	NATO sources	5	5	5	5	5	5	3	4	NATO LL process, just use the tools exists. The issue is time and manning
30	blue-red-white	US mil training, US commercial trainng	2	4	5	4	5	4	2	5	Common TP for sharing between partners
30	g5, g6	staff training, doctrine, nato sources	5	4	5	4	3	4	3	5	stronger culture of LL
30	observer	policy, strategy, oplans,	5	3	3	2	0	1	4	4	practical will
0	j6	exercise documentation, nato references	5	3	2	2	3	3	3	2	
7	j6	work experience, workin in different aras, exercises, courses	5	4	3	5	3	3	4	4	changing mind set of staff officers, making tools easier to share and share
0	cis, cyber ws	cyber security coursess, learning team leader, cyber defence courses	4	4	5	5	4	4	4	4	
2	cd cell	working groups, participants in exercises, ll meetings	4	4	5	5	5	5	0	4	crate a portal where all countries can particiate, and share incident data.
2	CIED Staff officer, Czber Staff offier	Exercise observations, Exercise LL, participating exercises	3	5	5	4	3	3	3	5	
1	CIS securty officer, Mil cert	Exercise participation, exercise planning	4	5	5	4	4	5	4	5	
20	s6,	info sharing same assingments, doctrines	4	3	4	3	4	3	4	5	sharepoint

Appendix 5 – Data of LS exercise survey

Team size	14	13	12	13	12	16	14	12	14	14
Number of answers	4	9	1	12	0	1	7	8	3	7
Avg	29%	69%	8%	92%	0%	6%	50%	67%	21%	50%
Teams	**B1**	**B2**	**B3**	**B4**	**B5**	**B6**	**B7**	**B8**	**B9**	**B10**
How many technical exercises have you participated? (avg)	2,5	1,222222222	5	1,666666667		2,5	2,142857143	0,875	5,666666667	2,857142857
How many Locked Shields have you participated? (avg)	1,25	0,333333333	2	0,916666667		2,5	1,285714286	0,625	1,333333333	1,142857143
How many years operational/real life experience do you have? (avg)	6,25	4	5	8,583333333		2,5	3,571428571	5,25	5	7,857142857
How many hours have you spent for team preparation? (avg)	14,75	2,333333333	10	18,83333333		2,5	9,714285714	10,25	61,66666667	33,57142857
How many hours experience do you have with your tools you going to use in the exercise?	more than 100 (50%)	more than 100 (33,33%)		3--10 (25%)			10-50 (57,14%)	more than 100 (62,5%)	more than 100 (33,33%)	3--10 (42,86%)
What is your team's organisational structure (decision making)?	functional (50%)	functional (55,56%)		functional (66,67%)			hiearchical (57,14%)	mix (37,5%)	hiearchical (100%)	functional (71,43%)
How long have you known each other as a team?	1 year (25%)	2y (11,11%)		1 week before (8,33%)			LS16 only (14,29%)	I hadn't ever seen the other team members before the exercise started, except for two of my colleagues. (12,5%)	1 year (33,33%)	2 days (14,29%)
Do you have an experience of working in ad hoc teams (like Rapid Reaction Team)?	No (75%)	No (88,89%)		No (75%)			No (100%)	No (75%)	No (100%)	No (57,14%)
Media	Yes (75%)	Yes (55,56%)		No (66,67%)			Yes (100%)	Yes (62,5%)	No (66,67%)	No (57,14%)
Routing	No (75%)	Yes (55,56%)		Yes (75%)			Yes (100%)	Yes (62,5%)	Yes (100%)	Yes (71,43%)
Forensics	No (75%)	Yes (66,67%)		Yes (66,67%)			Yes (85,71%)	Yes (50%)	Yes (100%)	Yes (57,14%)
Legal	Yes (100%)	Yes (66,67%)		Yes (66,67%)			Yes (100%)	Yes (50%)	Yes (100%)	Yes (71,43%)
PLC	No (100%)	No (88,89%)		No (83,33%)			Yes (85,71%)	No (87,5%)	No (100%)	No (71,43%)
Admins	Yes (75%)	No (66,67%)		Yes (83,33%)			Yes (85,71%)	Yes (50%)	Yes (100%)	Yes (100%)
Reporting	No (50%)	Yes (66,67%)		Yes (58,33%)			Yes (85,71%)	Yes (50%)	No (66,67%)	No (57,14%)
Monitoring	Yes (75%)	No (55,56%)		No (50%)			Yes (100%)	Yes (62,5%)	Yes (100%)	Yes (71,43%)
Drone	No (100%)	No (88,89%)		No (75%)			Yes (71,43%)	Yes (50%)	No (66,67%)	No (100%)
Do you have functions and duties clearly assigned to the team members?	Yes (50%)	Yes (77,78%)		Yes (100%)			Yes (100%)	Yes (87,5%)	Yes (100%)	Yes (85,71%)
What is the percentage of new tools in this exercise which you don't use in your daily job (0% - it's the same tools in LS, 100% - all the tools are new for me)? Think about monitoring, reporting, etc. tools.	60% (25%)	90% (33,33%)		70% (16,67%)			20% (28,57%)	40% (25%)	10% (33,33%)	70% (42,86%)
Do you expect to win?	No (100%)	No (100%)		No (83,33%)			No (57,14%)	Yes (62,5%)	Yes (100%)	No (71,43%)
Do you feel ready for game, or are you confused?	Ready (75%)	Confused (77,78%)		Ready (58,33%)			Ready (57,14%)	Ready (87,5%)	Ready (100%)	Ready (71,43%)

Team size	12	13	14	14	12	14	14	14	15	12
Number of answers	7	2	4	11	5	4	2	9	15	7
Avg	58%	15%	29%	79%	42%	29%	14%	64%	100%	58%
Teams	**B11**	**B12**	**B13**	**B14**	**B15**	**B16**	**B17**	**B18**	**B19**	**B20**
How many technical exercises have you participated? (avg)	2,285714286	3	2,5	3,727272727	3	3,25	9,5	1,333333333	1,733333333	2,142857143
How many Locked Shields have you participated? (avg)	1,428571429	1	1,5	1,272727273	1,6	1,5	2,5	0,888888889	0,2	0,142857143
How many years operational/real life experience do you have? (avg)	8	4	5,75	9,818181818	15,6	10	18,5	4,555555556	4,066666667	2,428571429
How many hours have you spent for team preparation? (avg)	15,71428571	4	4,5	20,09090909	19,6	13,75	22,5	24,66666667	19,53333333	16,42857143
How many hours experience do you have with your tools you going to use in the exercise?	3--10 (42,86%)	3--10 (50%)	10-50 (75%)	10-50 (45,45%)	3--10 (40%)	10-50 (50%)	10-50 (50%)	more than 100 (44,44%)	more than 100 (46,67%)	more than 100 (28,57%)
What is your team's organisational structure (decision making)?	functional (57,14%)	functional (100%)	functional (50%)	functional (45,45%)	functional (40%)	functional (75%)	matrix (100%)	functional (55,56%)	functional (60%)	hiearchical (71,43%)
How long have you known each other as a team?	2 weeks (14,29%)	I am new to the team only for exercise period (50%)	1 month (25%)	ranging from 1 week to 8 years (9,09%)	never met prior (20%)	1 month (25%)	20 (50%)	For three months. (11,11%)	2 Weeks (20%)	1 year (28,57%)
Do you have an experience of working in ad hoc teams (like Rapid Reaction Team)?	No (85,71%)	Yes (100%)	Yes (75%)	No (54,55%)	Yes (60%)	No (75%)	Yes (100%)	No (66,67%)	No (66,67%)	No (57,14%)
Media	Yes (71,43%)	Yes (100%)	Yes (75%)	Yes (63,64%)	Yes (100%)	Yes (50%)	Yes (100%)	Yes (88,89%)	Yes (66,67%)	No (57,14%)
Routing	Yes (85,71%)	Yes (100%)	Yes (75%)	Yes (81,82%)	Yes (80%)	Yes (50%)	Yes (100%)	Yes (88,89%)	Yes (93,33%)	Yes (85,71%)
Forensics	Yes (57,14%)	Yes (100%)	Yes (100%)	Yes (81,82%)	Yes (80%)	Yes (50%)	Yes (100%)	Yes (88,89%)	Yes (86,67%)	Yes (85,71%)
Legal	Yes (85,71%)	Yes (100%)	Yes (75%)	Yes (72,73%)	Yes (80%)	Yes (50%)	Yes (100%)	Yes (77,78%)	Yes (86,67%)	Yes (71,43%)
PLC	Yes (42,86%)	No (100%)	Yes (50%)	Yes (63,64%)	Yes (80%)	Yes (50%)	No (100%)	Yes (55,56%)	No (80%)	No (71,43%)
Admins	Yes (71,43%)	Yes (100%)	Yes (100%)	Yes (81,82%)	Yes (80%)	Yes (100%)	Yes (100%)	Yes (100%)	Yes (86,67%)	Yes (85,71%)
Reporting	Yes (85,71%)	Yes (100%)	Yes (75%)	Yes (81,82%)	Yes (80%)	Yes (50%)	Yes (100%)	Yes (66,67%)	Yes (86,67%)	Yes (100%)
Monitoring	Yes (71,43%)	Yes (100%)	Yes (75%)	Yes (72,73%)	Yes (80%)	Yes (100%)	Yes (100%)	Yes (77,78%)	Yes (100%)	Yes (85,71%)
Drone	No (57,14%)	No (50%)	No (75%)	Yes (54,55%)	No (60%)	Yes (50%)	Yes (50%)	Yes (55,56%)	No (80%)	No (57,14%)
Do you have functions and duties clearly assigned to the team members?	Yes (100%)	Yes (50%)	Yes (100%)	Yes (90,91%)	Yes (100%)	Yes (100%)	Yes (100%)	Yes (100%)	Yes (93,33%)	Yes (100%)
What is the percentage of new tools in this exercise which you don't use in your daily job (0% - it's the same tools in LS, 100% - all the tools are new for me)? Think about monitoring, reporting, etc. tools.	50% (28,57%)	30% (50%)	30% (50%)	30% (27,27%)	0% (40%)	30% (50%)	30% (100%)	80% (33,33%)	50% (20%)	100% (28,57%)
Do you expect to win?	No (71,43%)	Yes (100%)	Yes (50%)	Yes (72,73%)	Yes (80%)	Yes (100%)	No (50%)	Yes (66,67%)	No (100%)	Yes (57,14%)
Do you feel ready for game, or are you confused?	Ready (100%)	Ready (100%)	Ready (75%)	Ready (81,82%)	Ready (100%)	Ready (100%)	Ready (100%)	Ready (66,67%)	Ready (66,67%)	Ready (57,14%)

Appendix 6 – LS 16 winner prediction

LS 16 pre-survey outcome
Date/time: 20-04-2016, 22:40

The Locked Shields 2016 Blue team 5 has not provided any answer. Blue team 3 and 6 provided only one-one answer.
The average has been taken for the first 5 questions.

Taking account the exercise experience, the specific Locked Shield exercise experience working in a team, and working with the tools, I assume that blue team 17 will win the test run however blue team 9 is also very strong.

Team size	14	14	14	14
Number of answers	3	7	4	2
Avg	21%	50%	29%	14%
Teams	**B9**	**B10**	**B16**	**B17**
How many technical exercises have you participated? (avg)	5,666666667	2,857142857	3,25	9,5
How many Locked Shields have you participated? (avg)	1,333333333	1,142857143	1,5	2,5
How many years operational/real life experience do you have? (avg)	5	7,857142857	10	18,5
How many hours have you spent for team preparation? (avg)	61,66666667	33,57142857	13,75	22,5
How many hours experience do you have with your tools you going to use in the exercise?	more than 100 (33,33%)	3--10 (42,86%)	10-50 (50%)	10-50 (50%)
What is your team's organisational structure (decision making)?	hiearchical (100%)	functional (71,43%)	functional (75%)	matrix (100%)
How long have you known each other as a team?	1 year (33,33%)	2 days (14,29%)	1 month (25%)	20 (50%)
Do you have an experience of working in ad hoc teams (like Rapid Reaction Team)?	No (100%)	No (57,14%)	No (75%)	Yes (100%)
Media	No (66,67%)	No (57,14%)	Yes (50%)	Yes (100%)
Routing	Yes (100%)	Yes (71,43%)	Yes (50%)	Yes (100%)
Forensics	Yes (100%)	Yes (57,14%)	Yes (50%)	Yes (100%)
Legal	Yes (100%)	Yes (71,43%)	Yes (50%)	Yes (100%)
PLC	No (100%)	No (71,43%)	Yes (50%)	No (100%)
Admins	Yes (100%)	Yes (100%)	Yes (100%)	Yes (100%)
Reporting	No (66,67%)	No (57,14%)	Yes (50%)	Yes (100%)
Monitoring	Yes (100%)	Yes (71,43%)	Yes (100%)	Yes (100%)
Drone	No (66,67%)	No (100%)	Yes (50%)	Yes (50%)
Do you have functions and duties clearly assigned to the team members?	Yes (100%)	Yes (85,71%)	Yes (100%)	Yes (100%)
What is the percentage of new tools in this exercise which you don't use in your daily job (0% - it's the same tools in LS, 100% - all the tools are new for me)? Think about monitoring, reporting, etc. tools.	10% (33,33%)	70% (42,86%)	30% (50%)	30% (100%)
Do you expect to win?	Yes (100%)	No (71,43%)	Yes (100%)	No (50%)
Do you feel ready for game, or are you confused?	Ready (100%)	Ready (71,43%)	Ready (100%)	Ready (100%)