Blue Team Communication and Reporting for Enhancing Situational Awareness from White Team Perspective in Cyber Security Exercises

Tero Kokkonen and Samir Puuska

Institute of Information Technology, JAMK University of Applied Sciences,
Jyväskylä, Finland
{tero.kokkonen, samir.puuska}@jamk.fi

Abstract. Cyber security exercises allow individuals and organisations to train and test their skills in complex cyber attack situations. In order to effectively organise and conduct such exercise, the exercise control team must have accurate situational awareness of the exercise teams. In this paper, the communication patterns collected during a large-scale cyber exercise, and their possible use in improving Situational awareness of exercise control team were analysed. Communication patterns were analysed using graph visualisation and time-series based methods. In addition, suitability of a new reporting tool was analysed. The reporting tool was developed for improving situational awareness and exercise control flow. The tool was used for real-time reporting and communication in various exercise related tasks. Based on the results, it can be stated that the communication patterns can be effectively used to infer performance of exercise teams and improve situational awareness of exercise control team in a complex large-scale cyber security exercise. In addition, the developed model and state-of-the-art reporting tool enable real-time analysis for achieving a better situational awareness for the exercise control of the cyber security exercise.

Keywords: Cyber Security · Exercise · Training · Situational Awareness · Communication.

1 Introduction

Cyber security is an ongoing process where both organisations and individuals are training, working, and learning continually. Cyber security exercises are an excellent way to train and simultaneously test an organisation's or individual's capabilities under stressful cyber-attack situations. The exercise can be conducted in both public and private sectors. The cyber security strategy of the European Union notices the importance of national and international cyber security exercises [8]. Finland's security strategy for society states several times the importance of regular exercises for improving the resilience against threats [23], whereas Finland's cyber security strategy states that cyber threats are evolving extremely rapidly, and therefore cyber security exercises should be

conducted regularly for improving preparedness and cyber resilience [22]. Handbook for information technology and cyber security exercises [26] lists following exercise types: unannounced live exercises, initiation exercises, staff exercises, decision exercises, management exercises, cooperation exercises and Red Team - Blue Team exercises. The exercise type indicates the primary function of the exercise.

Cyber security exercises are usually organised using various teams with different tasks or missions. These teams are formed based on exercise type, training goals, and available resources and personnel. Blue Team (BT) is a group of people defending their information technology assets against cyber threats. They also report the observations to (simulated) management, create their own situational awareness and maintain their own security posture under cyber-attack. BT is very often modelled after a real organisation, team, or branch. There can be one or many BTs in the exercise that can represent different aspects of the real world. BTs often aim to role-play their normal organisational practices and procedures. Red Team (RT) is a group of people simulating the threat actors in the exercise by making real cyber-attacks against Blue Teams. White Team (WT) is responsible for controlling the exercise, making observations, collecting the data and handling the situational awareness of the exercise [5, 26, 13, 25].

Sometimes the exercise control team is also called EXCON which has similar functions as WT. In that sense, the situational awareness of the WT is extremely important for controlling the exercise and for making the required decisions during the exercise. The communication patterns of the BTs are an important source for understanding what is happening in the exercises from the BT's perspective, and how they are communicating with the co-operation organisations under cyber-attack.

One of the most classical definitions of situational (or situation) awareness is as follows: *"Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future"* [7]. In this study, the term situational awareness (SA) is used. At the first level of SA there is the perception (observations and sensor information), the second level is the comprehension (understanding the current situation) and the third level is the projection (prediction of future events based on the information of earlier states and decision makers' pre-learned history). It is stated that with erroneous SA even the trained decision makers will make incorrect decisions [7]. In the cyber security the objective of SA is to know what is (and will be) the security level of organisation's assets in the networked systems [9].

Cyber security exercises enable a comprehensive platform for studying situational awareness in cyber security and behaviour or efficiency of individuals and teams under cyber-attack. In the study [6] a methodology is proposed for adjustment of situation awareness measurement experiments within the context of a cyber security exercise. The author of [10] states that cyber security exercises can be used as an empirical study of situation awareness in cyber security. Also, the paper [5] deploys cyber security exercise data for profiling the attacker. Accord-

ing to the authors of the studies [4, 3], training and exercises have an important role for improving the competencies in the defence of the cyber security assets and for achieving the required level of preparedness especially in the resilience of critical infrastructure.

Situational awareness is important for all involved teams in the exercise. However, WT is required to have an understanding of the SA of the BTs in exercise in order to effectively adjust and steer the exercise towards fulfilling the desired learning and testing goals. Traditional monitoring of technical details of the exercise environment supplemented with the analysis of communication patterns provides an extensive view into Blue Team behaviour.

This study presents the study of Blue Team communication patterns and based on that the implementation of the state-of-the–art reporting tool for enhancing the SA of the White Team during the complex and hectic cyber security exercise. First the Finland's national cyber security exercise is introduced, the event timelines are are studied, and analysis is made. In addition, the reporting tool is developed and studied to produce incident reports for enhancing the SA of the White Team. Finally, the conclusions are done, and future research ideas are found and introduced.

2 Finland's National Cyber Security Exercise

Finland's national cyber security exercise has been conducted annually since 2013 and every year, the Cyber Range of Finland's national cyber exercise has been Realistic Global Cyber Environment (RGCE) developed by JAMK University of Applied Sciences Institute of Information Technology [18].

Finland's national cyber security exercise of 2017 was executed from 8th of May to 11th of May and it was commanded by the Ministry of Defence with The Security Committee. The RGCE Cyber Range and the overall implementation was conducted by JAMK University of Applied Sciences. There were more than 100 individuals participating in the exercise forming several co-operating Blue Teams communicating with each other according to their operational tasks. The aim of the exercise was to practice co-operation between security organisations and security network organisations in Finland during cyber-attacks or incidents for verifying the performance of the participant organisations and ensuring their further development [18].

As described in the aim of the exercise, the Blue Teams of the exercise were formed from different security authorities of Finland. All of them were acting, communicating and co-operating according to their real operational tasks during the realistic cyber attacks of several simulated threat actors. Some of the Blue Teams mainly defend their own assets whereas some Blue Teams have highly co-operational role and act and communicate actively in accordance with that role.

2.1 RGCE Cyber Range

RGCE is a fully operational Cyber Range that mimics the structures, services and traffic of the real Internet. It allows the usage of real IP addresses and global GeoIP information with realistic end user traffic patterns automatically generated by botnet based special software. RGCE is a closed environment, which allows usage of real attacks or malware. [14, 12]

3 Event Timelines

Cyber security exercises consist of several components forming the core which the White Team uses to direct the overall flow. A typical exercise contains a background story that sets the general tone and mindset for the trainees. Several threat actors are created to portray real-world counterparts, such as hactivist groups and more advanced organisations. Based on these actors and their modus operandi, various attack scenarios are prepared. The scenarios may include technical exploitations, denial-of-service attacks, social engineering, and advanced directed cyber operations.

3.1 Injects

Injects are pre-prepared actions in the Cyber Range. They are modelled after the threat actor's simulated campaigns. For example, a malicious group may want to use a denial-of-service (DoS) or a distributed denial-of-service (DDoS) attack to mask a more advanced exploit, targeted at one team. This could be achieved by two injects, one for each type of attack. The schedule for injects is drafted at the planning stage. However, due to the live nature of cyber exercises, White Team may choose to adjust their timing, targets or their potential execution, depending on the Blue Team response. Adjusting overlapping incidents and injects to support learning goals and desired stress levels is crucial for a successful exercise.

For the studied exercise, dozens of injects were prepared to simulate the cyber attack campaigns of threat actors. There were several realistic threat actors modelled and simulated in the exercise and the injects were prepared to simulate the behaviour of those threat actors. The attack campaigns varied from volumetric DoS/DDoS campaigns to targeted advanced persistent threat (APT) attacks including for example realistic behaviour of threat actors in social media.

Figure 1 illustrates the duration of the injects during the cyber security exercise. When WT decides to activate an inject, the actual time is recorded, as well as the moment when the inject in question is marked as 'executed', i.e. it does not require any further work from any of the teams. Figure 1 shows, that the approximate workload is relatively evenly distributed inside each exercise day, first and last being less intensive. This was the desired goal in the planning stage.

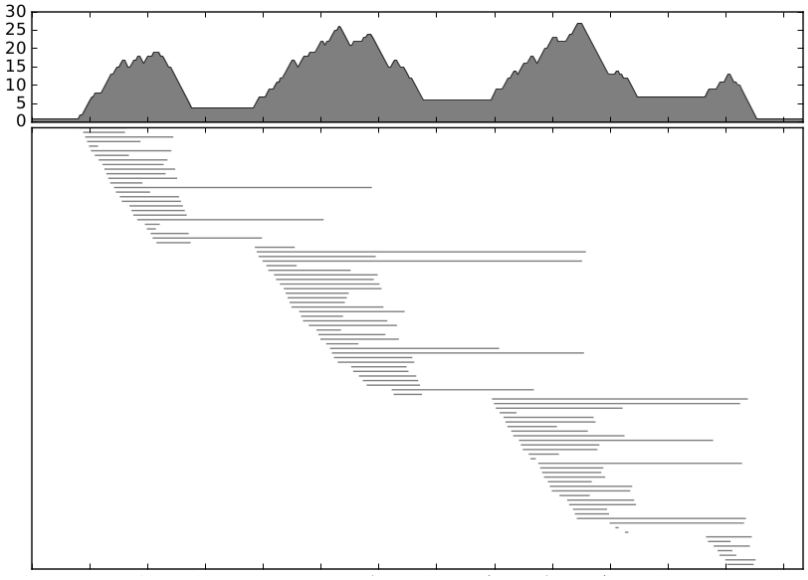


Fig. 1: Inject timing, durations (lower), and cumulative sum (upper) during the Exercise.

3.2 Communication Methods

Blue Teams were given various common methods for communicating between groups and internally. Each team had corporate email-accounts, two kinds of direct messaging options, and VOIP phones. Overall, the teams preferred e-mail over other forms of communication. Therefore, this study focuses on e-mails, and data fusion between other systems is considered as future work.

4 Analysis

Although figure 1 illustrates the approximate amount of desired work, it does not tell how the exercise teams actually react to the injects. In some cases the exercise teams may miss the inject entirely or fail to take appropriate measures. Direct monitoring or questionnaires disturb the flow of the exercise and require extra personnel.

E-mail patterns were analysed to see what communication patterns teams use during incidents. The mail headers were extracted from mail servers and analysed and visualised using Cytoscape software [24].

4.1 Team Communication Patterns

BTs in the exercise played several different roles. For example, one BT formed a common networking and service platform, which includes physical networks, as

well as workstations and intranet services, and another BT was a cyber security service organisation offering services to all other teams.

During the exercise tens of thousands of emails were sent and received, also including an e-mail-based Denial of Service -attack, as well as general spam, and e-mails from automated reporting systems. BTs also forwarded information to each other using large mailing lists. Some teams included their own address into these lists, and therefore received many copies of their own mails. White Team also answered to requests and inquiries that were directed to higher levels of organisations not occupied in the exercise.

Figure 2 illustrates all used message paths between parties. Red nodes represent attacker-controlled domains, coloured ones are the Blue Teams. Edge colour indicates the sending party. The graph shows that Teams two and five never communicated directly, even though they should have.

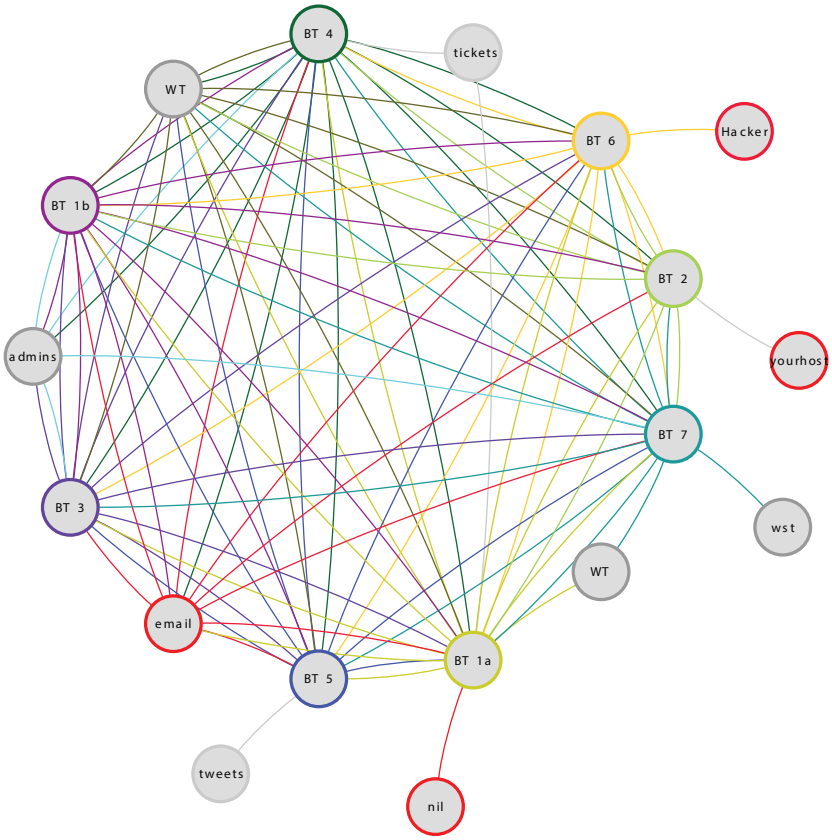
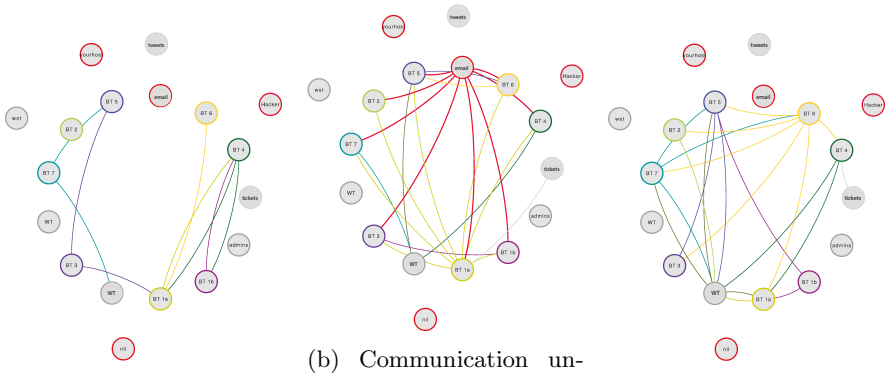


Fig. 2: The complete communication graph between domains.

The mailing patterns mostly reflect the nature and purpose of each team. Blue Team one, which was responsible for the core services, communicated with all other organisations actively. Their mails informed the organisations that were using their services about various disruptions, estimated repair times, and detected threats. Blue Team two was noticeably less active. They sent only a few notices of service disruptions, and mainly co-operated with Blue Team one, even though they were kept up to date by other teams. Blue Team three mostly co-operated with Blue Team five, which was expected. Blue Team six communicated actively with every other team, delivering threat intelligence and analysis services. Blue Teams four and one were also targeted by external Denial of Service and phishing campaigns. This may have affected their capability to send and receive mails.

In figure 3a, a typical set of service requests and responses is made. They indicate that the teams still have control over their infrastructure, and are able to take defensive measures. Figure 3b illustrates a phishing attempt, which later evolved into a spamming attack. Grey nodes represent mailboxes belonging to non-playing teams, while red nodes are controlled by threat actor (RT). In figure 3c Blue Team six has detected an unusually intensive port scanning originating from the Internet. The team informs others, and it can be seen that one team asks for more details.



(a) Generic communication during the exercise.

(b) Communication under spam and phishing attacks.

(c) Communication under port scanning attack.

Fig. 3: Example of communication patterns.

Although the analysis of communication patterns revealed some omissions and errors that teams made, it does not have enough information for White Team to form a robust SA. Also, the analysis of communication pattern is not conducted in the real time and more real time reporting tool is required for improving the situational awareness of White Team. It can be concluded, that a special real time reporting system is required for obtaining data and understanding the Blue Team behaviour during the complex cyber security exercise.

5 Reporting Tool for Improving White Team SA

Situational awareness is required as a basis for decision making. OODA loop (Observation-Orientation-Decision-Action) is a classical model for decision making [21, 15]. Another similar decision-making loop is introduced in four stages of an adaptive security architecture (Predict-Prevent-Detect-Respond) [17]. When reflected to both of those loops and earlier introduced definition of SA, SA is an extremely important element of decision making. When considering different data from different sources or sensors, there is a requirement for data fusion or multi-sensor data fusion, which is a process of synthesising overlapping and scattered data from the different sensors or sources to the user for achieving comprehensive SA of focused events [11, 2].

In the cyber security exercises, the Blue Team reporting tool for gathering the SA is required in two functions. First the Blue Teams report (automatically from sensors or manually) their observations to the tool and forms their SA based on data fusion. Secondly, White Team is able to monitor what the Blue Teams are reporting and what mitigation actions they are executing [16].

The developed Reporting Tools was tested in the cyber security exercise in the industrial domain [20]. Industrial cyber security exercise is piloted in the project of the European Regional Development Fund/Leverage from the EU 2014-2020, called JYVSECTEC Center and managed by JAMK University of Applied Sciences Institute of Information Technology.

5.1 Reporting Process and Software Tool

A specialised reporting process and a supporting state-of-the-art software tool for Blue Teams was developed with the aim that the new system would lower the barrier for reporting. The previous systems failed to encourage the teams or reporting actionable information. Although the teams did use earlier tools to report events, the messages were short, uninformative, and untimely. In addition, the earlier platform was cumbersome, which further discouraged reporting. Reporting is seen in Blue Teams as an unnecessary artificial chore that hinders their ability under the cyber-attacks or incidents.

The goal of development was to construct a reporting tool and process that would be unobtrusive and quick to use. Comprehensive reporting was encouraged by providing a template which contained necessary headings and hints what to put under them. GUI with muted colours was opted to use instead of the console-based solutions.

5.2 Reporting Format

For helping the trainees during the complex exercise scenarios, the reporting format is kept relatively simple; it borrows elements from military-style situation report structure. Table 1 presents the main elements of the format. In addition to the presented elements, each report has a time-stamp and title.

Table 1: Report template fields, translations, and purpose.

Field (in Finnish)	**Field (translated in English)**	**Purpose**
Havainnon laatu	Type of observation	What is being reported? Error condition, support request, malicious program, etc.
Tapahtuma	Incident	What has happened?
Seuraukset	Consequences	What impact will this incident cause? What further measures will be likely taken to mitigate the impact?
Tarkennukset	Further information	Additional details about the incident or of the overall situation.
Paikka	Place	Place, if relevant

A formal language was constructed for describing the reporting format in order to construct domain specific language (DSL). This domain specific language (DSL) allows the reports to be both human and machine readable. DSL is also expandable; other message types can be added in the future. The DSL was also equipped with syntax highlighting in the tool. As the DSL is verified using a formal language parser, the program can also notify user if values are missing or invalid.

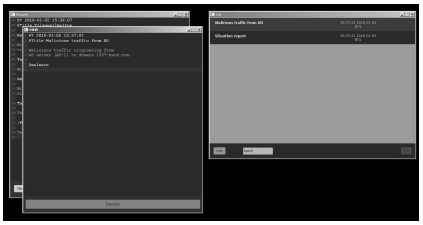
The main view is illustrated in figure 4a By default, the user sees two windows, one of which lists all reports made by his/her team, the other window is for creating a new report. By clicking the reports, they can be opened into a new window and examined separately. The screen-shot shows one additional window that the user has opened.

Figure 4b is a screen-shot of the reporting screen. For keeping the tool simple during the complex and hectic exercise, there are only two buttons and one syntax indicator present in the editor. The button labelled Tilanneilmoitus (Situation report) will fill the editor with the report template. The indicator states if the document does not conform to our DSL specification. The reporting window is a text editor with additional syntax highlighting features.

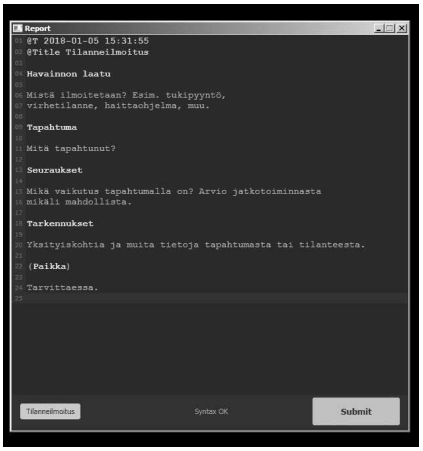
The tool was implemented using Java programming language and JavaFX UI framework, making the tool cross-platform ready [19]. The program utilises a message bus for synchronising messages between team members and delivering a copy of each message to White Team. Our implementation used Apache ActiveMQ message bus for communication [1].

6 Conclusion

Monitoring Blue Team communication provides further insight into both exercise status and team behaviour. As the analysis suggests, communication monitoring can be a useful tool in measuring Blue Team performance during the cyber security exercise. The analysis revealed several omissions made by the Blue Teams.



(a) Main view of the application. The list shows past reports, and the top window shows one of them in full detail. The report editor is in the background.



(b) Report editor with the report template loaded.

Fig. 4: Screen shots of reporting tool.

In addition, although the overall inject timing was successful, some teams might have benefited from intense workload.

When planning the injects, it could be useful to consider which teams are affected, and who is responsible for keeping them informed. By implementing real-time communication monitoring, the White Team can efficiently tell if the teams are acting correctly.

By using e-mail graphs in conjunction with other monitoring mechanisms, real-time mail visualisation aids White Team to build a more robust situational awareness over the exercise. This allows more fine tuned and accurate control, as well as more comprehensive results from the exercise.

However, the special reporting system is required to reliably monitor the Blue Team behaviour in real-time during the cyber security exercise. This requires additional timely reports from the Blue Teams, and a convenient, non-intrusive way for writing and delivering them. A specialised report format and state-of-the-art software tool was developed for achieving this goal. The tool was tested in the cyber security exercises within the industrial domain. It will also be used in the future exercises with improvements suggested in the initial tests.

Future work in the communication monitoring includes automating the message parsing and visualisation process so, that it is readily available to White Team during the exercise. This includes the development of a better visualisation system for monitoring purposes. In the future graphics will be designed to visualise multi-edged graphs efficiently for SA purposes. Future work with the reporting system will be more visualised SA of Blue Team behaviour for certain exercise inject and improvements of BT SA used for BTs' tactical leading and decision making.

Acknowledgment

This research is partially done in JYVSECTEC Center project funded by the Regional Council of Central Finland/Council of Tampere Region and European Regional Development Fund/Leverage from the EU 2014-2020.

References

1. The Apache Software Foundation: Apache activemq. `http://activemq.apache.org/`, accessed: 23 April 2018
2. Azimirad, E., Haddadnia, J.: The Comprehensive Review On JDL Model In Data Fusion Networks: Techniques and Methods. (IJCSIS) International Journal of Computer Science and Information Security **13**(1), 53–60 (Jan 2015)
3. Brilingaitė, A., Bukauskas, L., Krinickij, V., Kutka, E.: Environment for Cybersecurity Tabletop Exercises. In: Pivec, M., Josef, G. (eds.) ECGBL 2017 11th European Conference on Game-Based Learning, pp. 47–55. Academic Conferences and Publishing Limited (2017)
4. Brilingaitė, A., Bukauskas, L., Kutka, E.: Development of an Educational Platform for Cyber Defense Training. In: Scanlon, M., Nhien-An, L.K. (eds.) Proceedings of the 16th European Conference on Cyber Warfare and Security, pp. 73–81. Academic Conferences and Publishing Limited (2017)
5. Brynielsson, J., Franke, U., Tariq, M.A., Varga, S.: Using Cyber Defense Exercises to Obtain Additional Data for Attacker Profiling. In: 2016 IEEE Conference on Intelligence and Security Informatics (ISI). pp. 37–42 (Sept 2016). https://doi.org/10.1109/ISI.2016.7745440
6. Brynielsson, J., Franke, U., Varga, S.: Cyber situational awareness testing. In: Akhgar, B., Brewster, B. (eds.) Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities, pp. 209–233. Springer International Publishing (2016)
7. Endsley, M.: Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors **37**(1), 32–64 (1995). https://doi.org/10.1518/001872095779049543
8. European Comission: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (Feb 2013)
9. Evesti, A., Kanstrén, T., Frantti, T.: Cybersecurity Situational Awareness Taxonomy. In: 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). pp. 1–8 (June 2017). https://doi.org/10.1109/CyberSA.2017.8073386
10. Franke, U., Brynielsson, J.: Cyber situational awareness – A systematic review of the literature. Computers & Security **46**, 18–31 (oct 2014)
11. Han, X., Sheng, H.: A New Method of Multi-Sensor Data Fusion. In: 2017 IEEE 3rd Information Technology and Mechatronics Engineering Conference (ITOEC). pp. 877–882 (Oct 2017). https://doi.org/10.1109/ITOEC.2017.8122479
12. JAMK University of Applied Sciences, Institute of Information Technology, JYVSECTEC: Rgce cyber range. `http://www.jyvsectec.fi/en/rgce/`, accessed: 23 April 2018
13. Kick, J.: Cyber exercise playbook. The MITRE Corporation `https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf` (2014), accessed: 23 April 2018

14. Kokkonen, T., Hämäläinen, T., Silokunnas, M., Siltanen, J., Zolotukhin, M., Neijonen, M.: Analysis of Approaches to Internet Traffic Generation for Cyber Security Research and Exercise. In: Balandin, S., Andreev, S., Koucheryavy, Y. (eds.) Lecture Notes in Computer Science, pp. 254–267. Springer International Publishing (2015)
15. Lenders, V., Tanner, A., Blarer, A.: Gaining an Edge in Cyberspace with Advanced Situational Awareness. IEEE Security Privacy **13**(2), 65–74 (Mar 2015). https://doi.org/10.1109/MSP.2015.30
16. Lötjönen, J.: Requirement specification for cyber security situational awareness, Defender's approach in cyber security exercises. Master's thesis, JAMK University of Applied Sciences (Dec 2017)
17. van der Meulen, R.: Build Adaptive Security Architecture Into Your Organization. `https://www.gartner.com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization/` (Jun 2017), accessed: 23 April 2018
18. Ministry of Defence Finland: The authorities of the state administration are trained in cyber-skills in Jyväskylä - Valtionhallinnon viranomaiset harjoittelevat kyberosaamista Jyväskylässä 8.-11.5.2017, official bulletin 3th of may 2017. `https://www.defmin.fi/ajankohtaista/tiedotteet/valtionhallinnon_viranomaiset_harjoittelevat_kyberosaamista_jyvaskylassa_8.-11.5.2017.8418.news` (May 2017), accessed: 23 April 2018
19. Oracle Corporation: Java programming language. `http://www.oracle.com/technetwork/java/index.html`, accessed: 23 April 2018
20. Pajunen, D.: Cyber security is ensured with genuine exercises. `https://www.fingridlehti.fi/en/cyber-security-ensured-genuine-exercises/` (Sep 2017), accessed: 23 April 2018
21. Révay, M., Líška, M.: Ooda loop in command control systems. In: 2017 Communication and Information Technologies (KIT). pp. 1–4 (Oct 2017). https://doi.org/10.23919/KIT.2017.8109463
22. Secretariat of the Security Committee: Finland's Cyber security Strategy, Government Resolution 24.1.2013 (Jan 2013)
23. The Security Committee: Security Strategy for Society, Government Resolution 2.11.2017 (Nov 2017)
24. Shannon, P., Markiel, A., Ozier, O., Baliga, N.S., Wang, J.T., Ramage, D., Amin, N., Schwikowski, B., Ideker, T.: Cytoscape: a software environment for integrated models of biomolecular interaction networks. Genome research **13**(11), 2498–2504 (2003). https://doi.org/10.1101/gr.1239303
25. Sommestad, T., Hallberg, J.: Cyber Security Exercises and Competitions as a Platform for Cyber Security Experiments. In: Jøsang, A., Carlsson, B. (eds.) Secure IT Systems: 17th Nordic Conference, NordSec 2012, Karlskrona, Sweden, October 31 – November 2, 2012. Proceedings. pp. 47–60. Springer Berlin Heidelberg, Berlin, Heidelberg (2012)
26. Wilhelmson, N., Svensson, T.: Handbook for planning, running and evaluating information technology and cyber security exercises. The Swedish National Defence College, Center for Asymmetric Threats Studies (CATS) (2014)