Crossed Swords: a cyber red team oriented technical exercise

Bernhards Blumbergs; Rain Ottis; Risto Vaarandi

Blumbergs, Bernhards; Ottis, Rain; Vaarandi, Risto (2019). Crossed Swords: a cyber red team oriented technical exercise. Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019 : University of Coimbra, Portugal, 4-5 July 2019. Reading, UK: ACPI, 37−44.

Crossed Swords: A Cyber Red Team Oriented Technical Exercise

Bernhards Blumbergs[1,2], Rain Ottis[2], Risto Vaarandi[2]
[1] CERT.LV, IMCS University of Latvia, Riga, Latvia
[2] Centre for Digital Forensics and Cyber Security, TalTech, Tallinn, Estonia
bernhards.blumbergs[a]cert.lv
rain.ottis[a]taltech.ee
risto.vaarandi[a]taltech.ee

Abstract:
This paper describes the use-case of international technical cyber exercise "Crossed Swords" aimed at training the NATO nation cyber red teams within a responsive cyber defence scenario. This exercise plays a full-spectrum cyber operation, incorporates novel red teaming techniques, tools, tactics and procedures (TTTPs), assesses team design and management, trains the skills for target information system covert infiltration, precision take-down, cyberattack attribution, and considers legal implications. Exercise developers and participants have confirmed the learning benefits, significant improvements in understanding the employed TTTPs, cyber-kinetic interaction, stealthy computer network infiltration and full-spectrum cyber operation execution.

Keywords: Technical Cyber Exercise, Cyber Red Teaming, Responsive Cyber Defence, Computer Network Operations

1. Introduction

The majority of exercises are cyber defence oriented with the defending blue team (BT) being the primary training audience and the attacking cyber red team (CRT) role-playing the adversary to provide the learning experience for the defenders (Leblanc, et al., 2011; Ogee, et al., 2015; Dewar, 2018; Fox, et al., 2018). However, technical exercises, oriented at advancing the readiness level and experience of a CRT, are lacking, limited in scope, not mentioned or described publicly (Lewis, 2015). To enable the development of defensive approaches, both sides – blue and red, must be exercised, especially if they are dependent on each other in real operations. To integrate and explore the concepts of responsive cyber defence (RCD), computer network operations (CNO), CRT techniques, tools, tactics and procedures (TTTPs), detection mechanisms, cyber deceptions, and cyber red team operational infrastructure, a unified environment is required. A technical cyber exercise oriented not only at training single facet of the CRT but implementing a full cyber operation environment would improve the CRT training experience. Additionally, CRT interactions and inter-dependencies with other operational entities, such as conventional kinetic or special operations forces (SOF), should also be explored to see how cyber operations fit within the larger picture. This paper defines and assesses the CRT oriented technical cyber exercise "Crossed Swords" since year 2014.
The main contribution of this paper is a detailed description of the CRT oriented technical cyber exercise "Crossed Swords" that has been conducted since 2014. To the best of our knowledge, no research papers on CRT exercise design have been published before, and this paper fills this gap. Also, "Crossed Swords" exercise has several unique design features, such as multi-disciplinary nature of the exercise and training audience, complex scenario which adds geo-political, strategic and cyber-kinetic dimensions to advanced technical challenges, and near real-time feedback to exercise participants via situational awareness system.
The remainder of this paper is organized as follows – section 2 provides an overview of related work, section 3 focuses on various design aspects of "Crossed Swords" exercise, and section 4 concludes the paper.

2. Related Work

Leblanc et.al. (Leblanc, et al., 2011) explore and analyse multiple war-gaming exercises and implemented exercise support tool-sets, as described in this paragraph. "CyberStorm" is the US Department of Homeland Security developed exercise with the aim of examining readiness and response mechanisms to a simulated cyber event. Participation is strictly limited to Five Eyes alliance members. "Piranet" is the French developed response plan and a simulation exercise of a major cyber-attack against France's Critical Information Infrastructure (CII). "Divine Matrix" is the India's war-gaming exercise to simulate a nuclear attack accompanied by a massive cyber-attack with kinetic effects against India. "Standoff", organized by PHDays conference, involves a competition without fixed scenario

between attackers, defenders, and security monitoring teams. Airbus commercial Cyber-Range platform hosts the playground for "European Cyber Week Challenge Final". Similarly, NATO Cyber-Range is used for running "Crossed Swords" exercise.
Mauer, Stackpole and Johnson (Mauer, et al., 2012) look at developing small team-based cyber security exercises for use at the university as a practical hands-on part within the courses. The research explains the management and roles of the engaged parties in the exercise creation and execution. The developed game network is comprised of a small set of virtualized machines used by a group of participants to attack, defend and monitor the event. DeLooze, McKeen, Mostow and Graig (DeLooze, et al., 2004) examine the US Strategic Command developed simulation environment to train and exercise CNO and determine if these complex concepts can be more effectively taught in the classroom. The simulation environment consists of "Virtual Network Simulator", comprised of two or more networked computers designed to represent attack effects in an interactive graphical environment, and the "Internet Attack Simulator", presenting a set of simple attacks, ranging from reconnaissance to DoS, available for launching against the network simulator's virtual network. Mostow and Graig confirm the benefit of CNO simulation exercises by measuring the increase of knowledge of the participants.
The issues tackled, in the related work for the cyber defence exercises are either narrow in scope, specific to a nation or small set of nations, restricted only to exercising just the decision-making process or a small subset of a full-scale cyber operation, or limited to just simulation of common cyber-attacks. Additionally, the majority of the exercises are delivered for the defensive capability building, and the CRT is either simulated or role-playing the adversary. However, a dedicated technical exercise for training CRT capabilities is required.

3. Cyber Red Team Exercise Design

Cyber exercise "Crossed Swords" (XS) (NATO CCD CoE, 2019), organized jointly by NATO CCD CoE and CERT.LV, is an annual international technical exercise oriented at training CRT with the latest technologies and striving to deliver highly realistic training. Since its inception, the exercise has grown in complexity and size. The exercise spans across three consecutive days representing a 24-hour fast-paced and intensive operation. More importantly, this exercise has served as a platform for implementing, testing, confirming, and conducting academic studies in the areas of CRT TTTPs, learning effectiveness, and near real-time situational awareness (Kont, et al., 2017).
The exercise is designed to implement the following cyber red team training objectives (TO):

1. Perform defended system compromise assessment, practice evidence gathering and information analysis for technical attribution, identify the origins of malicious activities and take actions stop them;
2. Execute a responsive cyber defence scenario for adversarial information system infiltration;
3. Employ stealthy attack approaches, and evaluate applicable TTTPs for fast-paced covert operations;
4. Exercise working as a united team in achieving the laid-out mission objectives;
5. Develop specialized cyber red teaming soft and technical skills needed for operation management, information flow, and target information system takeover; and
6. Explore and evaluate the full-spectrum operation's cyber-kinetic interdependencies.

The following subsections will provide a detailed description of the exercise.

3.1. Cyber Red Team Structure and Chain-of-Command

The exercise developers, execution managers, and the participants are allocated to various teams and sub-teams based on the specifics and activity focus area. The exercise has the following teams based on the area of operations: cyber-kinetic operations team (Red Team – RT), adversary and user simulation team (Blue Team – BT), exercise control and scenario management (White Team – WT), near real-time attack and situational awareness team (Yellow Team – YT), and game network infrastructure development and support team (Green Team – GT). As stated, the structure and chain-of-command for such cyber-kinetic operations has not been publicly discussed or disclosed by any nation; therefore, this exercise strives to experiment and uncover the organizational model providing simple chain-of-command and separation of duties.
The designed chain-of-command model for "Crossed Swords 2019" exercise is depicted in Figure 1, where the grey boxes represent the cyber red team at strategic, operational and tactical levels (with respective grey colour shading for every level), and the white boxes indicate the white team presence and assistance to the CRT. In the "Crossed Swords" exercise the CRT is divided into the sub-teams based on the expertise in technologies to be targeted (e.g.,

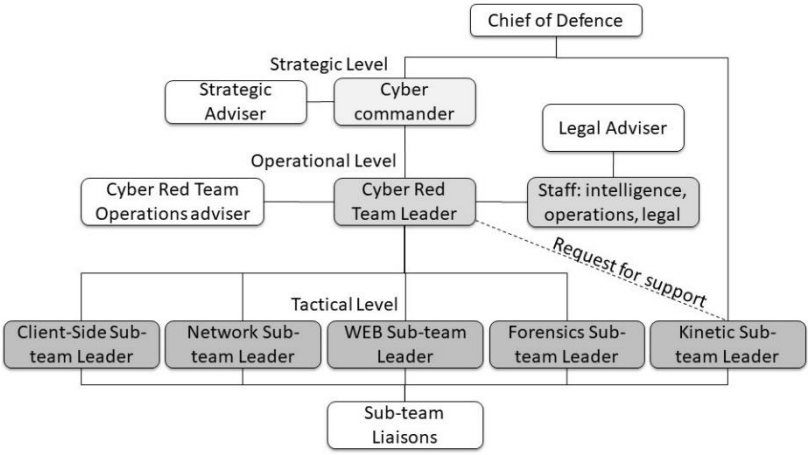

Figure 1: "Crossed Swords 2019" chain-of-command

web applications, network protocols). This exercise favours the speciality based sub-team creation to allow participant engagement throughout the exercise game-play and not only for explicit phases of the cyber operation. These teams are subdivided into sub-teams according to the specialization and operational management level:

1. **Red Team**: being the largest team of around fifty experts consists of exercise training audience. The chain-of-command and various sub-teams are the following:
    a. *Cyber commander.* The top-level officer in charge of commanding the cyber operation at a political level. Cyber commander, as part of the training audience, manages and coordinates the cyber operation to reach the set mission goals and coordinates the high-level activities, based on the desired effects, of the sub-teams;
    b. *Strategic adviser.* Is a member of the exercise development and management team (WT) with the role to provide the advice to the cyber commander, and, if needed, give minor hints to keep the red team activities on the course of designed scenario. This option allows exercise developers to explore the nuances and alternative paths for the developed scenario, allowing deviations if the result objectives are met;
    c. Red team leader group. This small group of experts, operating at an operational level and under direct command of the cyber commander, are responsible for fulfilling assigned operational effects by working with the sub-team leaders and ensuring that objectives, force protection, and intelligence activities are correctly executed and reached. This group consists of three experts: the overall red team leader, OPSEC officer, and an intelligence officer;
    d. *Sub-team leaders.* The main red team consists of five expert-focused sub-teams, at a tactical level, which are represented by their leaders. The purpose of every sub-team is to deliver the intended effects in their responsibility area. Over the exercise iterations it has been identified that sub-team size of 6-10 experts offers the best trade-off between required capability and management efficiency. The role and purpose of every sub-team is as follows:
        i. *Client-side attack sub-team.* This team focuses on executing attacks targeted at exploiting end-user (i.e., human vulnerabilities) to get the initial foothold, such as creating a *spear-phishing* campaign, setting up *watering-hole* or *drive-by* attacks. Once initial breach has succeeded this team ensures persistence in the target computer network;
        ii. *Network attack and exploit development sub-team.* The goal for this team is to target exposed computer network services, gain control over them by abusing the misconfiguration, poor implementation, abuse, or developing and exploiting software vulnerabilities. Additionally, this team is conducting IP network (IPv4 and IPv6) and service mapping, and executing attacks against specialized systems, such as tactical radio networks, mobile operator base stations, and ICS elements;
        iii. *Web-application attack sub-team.* For this team all web-based systems and technologies, such as web-applications, services, and back-end relational databases, are the target. This

team extracts valuable information from the web-applications, such as user credentials, e-mails, or application source code, as well as breaches the security of an exposed web-application to gain access to the internal network services, and establish persistence;

iv. *Digital battle-field forensics sub-team.* The main effort of this team is to perform data carving and artefact extraction from various sources, such as hardware devices (e.g., smart phones, portable computers and other electronics), computer memory or hard disk images. This team serves as the bridge between the cyber and kinetic operational components as it is tasked to perform analysis of forensic evidence extracted either by the cyber sub-teams or brought in from the field by the kinetic team; and

v. *Kinetic forces sub-team.* This team formed from trained military and law-enforcement experts performing various kinetic operations, including high interaction with the CRT capability, such as forced entry, covert access, hardware extraction, target capture or take-down, intelligence collection, surveillance, or kinetic activities on enemy territory. The interaction with the rest of the red team provides one of the key aspects for cyber-kinetic game-play. This team is managed and trained by industry experts (e.g., HTCI – High-Tech Crime Institute) and SOF instructors (e.g., NATO SOF School). The created scenario is designed to have the interdependencies within the CRT and anticipates the cyber-kinetic cooperation.

e. *Sub-team liaisons.* For every mentioned sub-team there is an attached WT liaison responsible for observing and, if required, providing minor hints to the sub-team leader to ensure that the team is not wasting too much time on some targets, such as cyber decoys and honeypots, and does not deviate from the intended scenario significantly; and

f. *Legal advisers.* Legal advisers are embedded to assist every level of the chain-of-command. The role of these experts is to provide their assessment of the activities from the international and domestic law perspectives.

2. *Blue Team.* A small team of up to four experts experienced in conducting cyber red team activities. This team is under direct control and supervision of WT and is used to manage the CRT progression within the adversary's computer networks. The main tasks for this team are user and adversary simulation. As a user simulation role-player, they are directly engaged in client-side conducted activities, such as examining and deciding to open received malicious attachments, visiting the web links, or browsing the in-game web services. Their task is to observe, assess and deny, or permit, the CRT initial foothold, based on the quality and delivery method sophistication level;
3. *White Team.* A small group of experts, typically no more than two, responsible for controlling and steering the exercise according to the developed scenario. As mentioned before, deviations from scenario are accepted and sometimes encouraged if the overall focus is not lost, and mission objectives can be reached. The exercise does not have the goal of succeeding in accomplishing the intended scenario and fulfilling entirely the laid mission goals by any means necessary. Depending on the activities pursued by the CRT, their course-of-action and time limitations, the mission might be a failure, as it can happen in real life. Within the past iterations of the exercise the red team only once successfully accomplished all the mission objectives, and in other cases completed them partially.
4. *Yellow Team.* This team focuses various areas of threat and anomaly detection, such as monitoring, big data analytics, intrusion detection, and situational awareness. The most crucial task for this team is to provide the near-real time situational awareness picture to the CRT from the perspective of neutral and hostile actors. This feedback allows the CRT to immediately spot mistakes and adjust their operations and tool usage to avoid detection, therefore not only increasing the level of stealth, but also having a better understanding on the used tools and performed actions; and
5. *Green Team.* Is responsible for tasks, such as maintaining the cyber range platform, supporting the game network technical requirements, developing the game network hosts and targets, and integrating new technologies.

3.2. Technical Environment and Technical Exercise Scenario

The "Crossed Swords" (XS) exercise game network is hosted on a cyber range running VMware ESXi hypervisor and it consists of around 200 virtual machines for in-game core networking, simulated Internet, CRT segment, and a set of target networks. Not all intended technical game-play elements can be virtualized, therefore the game network is expanded by connecting physical hosts and systems through the cyber range infrastructure. Before creating the overarching geo-political scenario, the technical scenario is established based on the core development team ideas and intended technical game-play intentions. Due to XS being relatively small, with respect to the game-network scale and training audience size, experimentation and introduction of new, recently prototyped, and unorthodox technologies can be afforded making the technical game-play more attractive and as close to the real-life as possible. The network also uses the traditional IT systems to provide the networking and common workstation operating systems, such as MS Windows and GNU/Linux, to provide replicate the structure of a regular office and business networks. The following list briefly summarizes some of the technologies introduced in the XS game series, to highlight the technical level:

1. Bunker door – control system employing a set of interconnected Siemens developed S7-1200 based PROFINET IO-devices. The CRT must reverse-engineer the communication protocol to inject remotely the commands controlling the bunker door;
2. Alarm system – protected premises by the Paradox alarm system, which must be targeted remotely by analysing the used bus-protocol, and capturing and decoding the PIN code;
3. CCTV IP camera – CRT has to find and exploit the flaws in the IP-based surveillance camera's web interface to gain full control remotely;
4. Distributed power-grid – based on IEC-60870-5-104 industrial Ethernet protocol series and a Martem produced remote terminal unit (RTU) is used to manage and supervise the power-grid. The CRT has to reverse-engineer the protocol and perform remote command injection to control the power supply;
5. Unmanned aerial vehicle (UAV) – Threod manufactured UAVs flying over the protected territory must be targeted to gain control over the steering and video stream;
6. Unmanned ground vehicle (UGV) – Milrem developed UGVs serve as an adversary-controlled tank force and the cyber red team is tasked to take full control over them by targeting either the used network protocols or the controlling workstation;
7. Maritime navigation – a vessel's steering and tracking system based on the AIS (Automatic Identification System) maritime protocol is targeted by the CRT to gain control over the ship and inject fake naval tracks;
8. Radio communication network – Harris-based military-grade data network must be infiltrated by the CRT by extracting the encryption keys;
9. Mobile network base stations – the cyber red team must infiltrate the LMT (Latvian Mobile Telephone) operator provided base stations connected to the actual mobile network, analyse and parse the intercepted communications to decode the adversary agent's message exchange (SMS) and pinpoint their physical location; and
10. Railroad control station – a system based on Siemens created S7-1200 PLC running s7comm+ protocol, controls the in-game railroad network. The CRT is tasked to gain control over the railroad control stations to stop or derail the train.

The various technical challenges implemented across nearly all game-net systems, are designed in a way, that no single CRT sub-team can solve them on its own. Instead, cooperation, information exchange, objective tracking, and operation management is emphasized to provide the collaborative training experience and attempting to push the participants out of their comfort zones. The technical scenario, being time limited and fast-paced, cannot be fully solved, therefore the CRT has to consider ways and approaches on how to prioritize the technical objectives and manage the focus of force to accomplish the overall mission objectives within the exercise time.

The integration of real-life vulnerabilities and systems (Blumbergs & Vaarandi, 2017) (Blumbergs, 2019) deliver the learning perspective to the exercise participants. Examining, developing exploits, and attacking the systems which are widely used for automation and industrial process control are challenging and allow the training audience to comprehend the actual state of security for such industrial components. Furthermore, some participants might have such systems in their organizations, but are not allowed to execute attacks or tests due to them being in a production state. CRT members, with some guidance by the instructors, follow the full weakness identification, vulnerability

determination, and exploit development life-cycle. This allows the participants to successfully exploit the industrial control protocols and devices.

3.3. Geo-political Exercise Scenario

The technical scenario, describing the interdependencies, attack vectors, and alternative paths, only covers the part for the actual work to be conducted by the exercise participants. To deliver the context, reasoning, and clear objectives, the overarching scenario is required. This scenario provides the elements, such as the state-of-the-world background, geo-political situation, intelligence information on what has happened, why the response is being triggered, what are the objectives and rules of engagement. The main geo-political story revolves around a fictitious group of Cyberbian islands, where every island is a sovereign country with its technological advancements, political stance, alliances, and intentions. The three island-countries are Berylia, Crimsonia, and Revalia. Berylia being the smallest with a modest military force, part of NATO alliance, and its main economic income originating from the electronics manufacturing. Crimsonia is the largest island with a strong military, rich in natural resources, not part of any alliance, and is expressing some signs of aggression against its neighbouring island-countries. Revalia is a small, self-sustained, and politically neutral country. Within the scenario, the exercise participants assume the role of Berylian team, which is assembled to address the looming crisis. Every year, with a new exercise edition, the scenario evolves and the tensions between Berylia and Crimsonia have been escalating, ranging from Crimsonia conducting a series of debilitating cyber-attacks against Berylian CII, abuse of a neutral nation infrastructure, placing insiders and double-agents, forming military blockades, up to launching a military invasion of Berylia. The various levels of conflict are designed to explore the technical, cyber-kinetic, and legal game-plays as every scenario opens new opportunities and provides flexibility in conducting the responsive computer network operations. The operational environment for the kinetic force's unit is extremely important, as this restricts, or enables, some types of activities to be exercised.

3.4. Legal considerations

The legal aspects are incorporated in the form of legal scenario injects aimed to trigger the discussion and legal implication consideration by the command element. Legal advisers are assigned to the chain-of-command to assess and consult the exercise participants. The legal aspects of the conducted cyber-kinetic operations and applied TTTPs, within the context of the scenario, typically tackle at least the following legal considerations as covered in Tallinn Manual 2.0 (Schmitt, et al., 2017):

1. *Applicable law*. Depending on the scenario, the lawyers are tasked to ascertain which regimes of public international law apply to the cyber operations occurring during the exercise;
2. *States entitled to take countermeasures*. Only state affiliated institutions and organizations, such as military or intelligence, can conduct responsive activities on the state's behalf as long as the activities they engage in do not constitute an internationally wrongful act;
3. *Effect of RCD on third parties*. Since RCD has extraterritorial nature and implicates pursuing the adversary, as well as, performing malicious service take-down within the cyberspace, the legal advisers are required to assess the legality of the RCD effects on the third parties. For the CRT to complete their mission objectives, the RCD activities have to be deemed lawful;
4. *Limitations on RCD*. Depending on the legal qualification of the RCD operations, various limitations, such as concerning necessity, proportionality, imminence and immediacy, are attached to this operation. The legal advisers are tasked to identify any applicable limitations, such as requirements for the RCD to be necessary and proportional, and provide these legal implications to the commander or sub-team leaders;
5. *Self-defence against an armed attack*. The scenario is designed in such a manner that the severity of the offensive action against the victim state amounts to an armed attack, thus permitting to respond in self-defence with immediate asymmetric responsive cyber operations against a stronger and advanced adversary;
6. *Geographical limitations of cyber operations*. The effects of cyber operations have to be limited to the intended target information systems and geographical locations. This, although not always being possible to limit geographically, is taken into consideration by the CRT when executing the cyber operation which may include the activities, such as placement of drive-by exploit-kits on third-party services;

7. *Means and methods of cyber warfare*. The exercise scenario plays on the various levels of aggression and conflicts;
8. *Precautions*. For the executed cyber operations, the CRT is asked to exercise constant care, perform verification of targets, choice of means or methods, choice of targets, evaluate proportionality, and estimate the effects of cyber-attack whenever it is reasonably possible and applicable;
9. *Cyber operations in neutral territory*. The adversary may proxy their cyber-attacks or route the kinetic attack, such as drone flying through neutral state's air space before heading to the intended target. In such cases, the red team's response might have uncertainty and limitations on taken actions in the neutral state's cyberspace.; and
10. *False-flag and no-flag operations.* For the CRT to protect their identity, assets and intended objectives, a false-flag or no-flag operation could be considered to be executed to imply uncertainty and make attribution harder. From the technical perspective, the cyber red team might adapt the known TTTPs of a chosen threat actor to deceive the adversary. From the legal point of view, it is not clear if such operations are permitted when, for example, impersonating and adversarial profile of a threat actor with high certainty attributable to a third state.

3.5. Training Assessment and Real-time Feedback

One of the key aspects of the "Crossed Swords" exercise is to provide the environment, where the CRT can experiment, practice applicable TTTPs and observe their effects in near real-time. Such opportunity provides the necessary feedback to the exercise participants for their tool and procedure stealth and efficiency, as well as, to the exercise management to evaluate the progress of the CRT and the fulfilment of training objectives. To accomplish this, a dedicated framework, called the *Frankenstack* (Kont, et al., 2017), is developed to deliver the required visibility through meaningful visual means and notifications. The *Frankenstack* development is facilitated and coordinated by NATO CCD CoE since 2016. The development team is assembled from technical experts in the field of monitoring, data visualization, threat detection and assessment, and big data analytics. The contributions include NATO CCD CoE partners, such as Arc4dia, Stamus Networks (Suricata IDS), Greycortex, Cymmetria, Tallinn University of Technology, CERT.LV, and CERT-EE. The *Frankencoding* events (https://github.com/ccdcoe/Frankencoding) have resulted in an ongoing *Frankenstack* development with its source code released publicly on GitHub under the MIT license (https://github.com/ccdcoe/frankenstack).

The solution is easily deployable in the game network and can accept any possible sources of information to be further processed, which can be from at least the following origins:

1. *ERSPAN (Encapsulated Remote Switched Port ANalyser)* traffic mirror collecting all the network data recording, parsing, and deep packet inspection;
2. *NetFlow* from game network routers for traffic statistical analysis and evaluation;
3. *data from the systems*, such as system performance metrics (e.g., CPU load, HDD utilization, network interface card statistics), and logs (e.g., Syslog, and application textual log-files);
4. *honeypots and cyber decoys* placed in the network to attract and deceive the cyber red team into revealing its TTTPs; and
5. *aggregates the information from all sources* in textual format allowing this to be reduced to a log correlation and analysis problem.

During the "Crossed Swords 2017" execution the members of WT performed the assessment of the deployed *Frankenstack* solution for its usefulness and training benefits (Kont, et al., 2017). The identified findings were addressed and incorporated into the following exercise editions. The conducted expert qualitative interviews and online survey results reflected the following:

1. the deployed tools themselves do not increase the learning perspective, but is up to how red team members perceive and use the tools;
2. the addition of situational awareness solutions to the exercise is welcome and seen as a necessary component;
3. the four large screens in the execution room, showing the yellow team provided information, was preferred and checked approximately every 45 minutes by most of the training audience;
4. exercise participants also used the opportunity to access the *Frankenstack* dashboards locally on their computers and dig deeper when attempting new attack vectors;

5. *Alerta* tool, showing the identified attacks as priority categorized alerts, was found most useful by most of the trainees;
6. it was acknowledged, that ease of use should be further improved especially when considering the merger of high intensity technical exercise with monitoring tools not known to all participants;
7. majority of the training audience strongly agreed that the provided situational awareness was beneficial to the learning process, was accurate and delivered in acceptable speed;
8. the larger part of the training audience agreed that they learned more regarding how their actions can be detected and tried to be stealthier; and
9. integration of various tools into the *Frankenstack* has to be evaluated carefully to avoid visual distractions and making the output more self-explanatory.

4. Conclusions and Future Work

In this paper, we have presented the "Crossed Swords" exercise which involves intense game-play scenario and near real-time feedback, and explores novel concepts of CRT structure, cyber operation management and execution, and TTTPs applicability and stealth. For the future work, we plan to study the impact of the exercise on participant learning efficiency, on participant knowledge retention and change of perception about red team cyber operations, and on best practices for red team cyber operations.

Acknowledgements

The authors thank Liis Vihul and Joonsoo Kim for their valuable contribution.

References

Blumbergs, B., 2019. *Remote Exploit Development for Cyber Red Team Computer Network Operations Targeting Industrial Control Systems.* Prague, Scitepress, 5th International Conference on Information Systems Security and Privacy.

Blumbergs, B. & Vaarandi, R., 2017. *Bbuzz: A Bit-aware Fuzzing Framework for Network Protocol Systematic Reverse Engineering and Analysis.* Baltimore, IEEE Milcom.

DeLooze, L., McKean, P., Mostow, J. & Graig, C., 2004. *Simulation for training computer network operations.* WestPoint, IEEE Fifth SMC Annual Information Assurance Workshop.

Dewar, R. S., 2018. *Cyber Defense Report: Cyber Security and Cyber Defense Exercises,* Zürich: Center for Security Studies (CSS), ETH Zürich.

Fox, D. B., McCollum, C. D., Arnoth, E. I. & Mak, D. J., 2018. *Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context,* Massachusetts : The MITRE Corporation.

Kont, M. et al., 2017. *Frankenstack: Toward Real-time Red Team Feedback.* Baltimore, IEEE Milcom.

Leblanc, S., Partington, A., Chapman, I. & Bernier, M., 2011. *An Overview of Cyber Attack and Computer Network Operations Simulatio.* SanDiego, Proceedings of the 2011 Military Modeling & Simulation Symposium.

Lewis, J., 2015. *The Role of Offensive Cyber Operations in NATO's Collective Defence.* Tallinn, NATO CCD CoE.

Mauer, B., Stackpole, W. & Johnson, D., 2012. *Developing Small Team-based Cyber Security Exercises.* LasVegas, International Conference on Security and Management.

NATO CCD CoE, 2019. *Crossed Swords.* [Online]
Available at: https://ccdcoe.org/exercises/crossed-swords/

Ogee, A., Gavrila, R. & Trimintzios, P., 2015. *The 2015 Report on National and International Cyber Security Exercises: Survey, Analysis and Recommendations,* Athens: ENISA.

Schmitt, M. et al., 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Tallinn: Cambridge University Press.