The Optimal Organisational Structure for Cyber Operations based on Exercise Lessons

Marko Arik, Adrian Nicholas Venables and Rain Ottis
Department of Software Science, Tallinn University of Technology Tallinn, Estonia.

marko.arik@taltech.ee
adrian.venables@taltech.ee
rain.ottis@taltech.ee

Abstract: The NATO Cooperative Cyber Defence Centre (CCDCOE) of Excellence hosts annual Locked Shields (LS) and Crossed Swords (CS) cyber exercises to help NATO nations develop, train, and test their cyber capabilities. These exercises have successfully experimented with cyber capabilities and human organisational structures. However, there are still opportunities to optimise cyber exercise structures. This article employs a use case study based on these exercises to compare structures used by NATO nations in cyber exercises and cyber operations. This identified an optimal structure for operational-level cyber defence and offence exercises and proposed methods for their planning, development, and execution.

Keywords: Cyber Operations Exercises, Cyber Command organisational structure, Blue Team organisational structure, Red Team organisational Structure.

1. Introduction

Cyberspace threat actors can exploit advanced nations' reliance on the information environment, necessitating the establishment, training, and preparation of a military force to counter adversary activities. However, countries developing cyber defence capabilities are often reluctant to disclose specific information about them. Cyber exercises can contribute to the e training and preparation of cyberspace forces and the development of their operational-level organisational structures. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) organises two well-known annual cyber exercises, Locked Shields[1] and Crossed Swords[2], to assist nations in developing, training, and testing their cyber capabilities. This research examines the cyber capabilities and structures by collecting and interpreting new data to analyse the Operational and Tactical levels of Command. This addresses the challenge of obtaining reliable data from non-classified exercises to reveal cyber organisations' optimum Command structures.

2. Methods

This article employs a use case study based on the 2022 Locked Shields and Crossed Swords cyber exercises organised by the CCDCOE. It provides an overview of NATO Cyber Operations and exercise organisational structures. The literature review examined the Locked Shields exercise from “after-action” reports used for research purposes. Interviews with experts from Estonian Defence Forces Cyber Command, CCDCOE, Locked Shields 2022 Red Team, and NATO Cyberspace Operations Centre supplement the review.

3. Literature Review

Three sources were used for data in this research. As the leading global cyber power, the US offers insight into large organisations' structures (Voo et. al., 2022, p. 11). The smaller Estonian Cyber Command and its organisational structures were also reviewed as the exercises were organised by the CCDCOE based in Tallinn, and data on its composition was available. Finally, the publicly available NATO Cyber Operations (CO) command organisational structures are reviewed (Pederson et al., 2022), (Dalmijn et al., 2020), (Blumbergs, 2019), (Kohler, 2020).

3.1 Cyber Operation Organisational Structures

In the Routledge Handbook of International Cybersecurity, Piret Pernik states the role of a cyber command as follows:

[1] https://ccdcoe.org/exercises/locked-shields/
[2] https://ccdcoe.org/exercises/crossed-swords/

"At a minimum, a cyber command should be composed of staff sections (capabilities) for strategic and policy analyses and planning (including legal and technological development), intelligence, situational awareness, operational planning, and conduct of cyber operations. A military centre of excellence for research and competence and a cyber range should support the cyber command. Finally, the command should have a degree of authority for the acquisition and personnel policies (including reserve forces and conscription if applicable), as well as education, training, and exercises" (Pernik, 2020). In addition, the organisation's success depends on its members' training and experience to succeed (Pomerleau, 2022)

An article by Air Land Sea Space Application Center (Pederson et al., 2022) discusses cyber operations structures. The current USCYBERCOM cyberspace operations structure is a temporary fix, a 'band-aid' that patches the infrastructure using the least expensive materials. For the optimal solution, Pedersen proposed a separate standing organisational structure as the optimal solution for U.S. military forces and the protection of DOD cyberspace from adversaries (Ibid). The subsequent structures include more details concerning the organisations' roles and departments or teams.

2020, the CCDCOE published 'The Cyber Commanders` Handbook' (Dalmijn et al., 2020). This stated, "A one-size-fits-all Cyber Command structure is impossible to define." Instead, the handbook proposed a reference organisational structure, which includes the core activities of cyber operations. The Cyber Commanders' Handbook outlines an organisational structure with four levels: Commander, Advisors, Staff, and Subcommand. Specialised branches facilitate military cyber operations, including C2 for situational awareness, C3 for cyber defence, C5 for planning, and C6 for communications. Legad provides legal guidance on national and international laws in cyber operations.

A different cyber operations structure focused on Specialized Cyber Red Team Responsive Computer Network Operations was proposed by Blumbergs (Blumbergs, 2019). Dr. Blumberg's concept of Red Team (RT) can be expanded to offensive cyber operations in general. It is not restricted to narrow "red teaming" or opposing force framework but is a product of the CCDCOE exercise culture where Blue Teams are on the defence, while the Red Teams are on the offensive role. This was done in a very abstract version of the chain of command. This described the chain of command based on the specific activity focus area, shown in white in Figure 1.

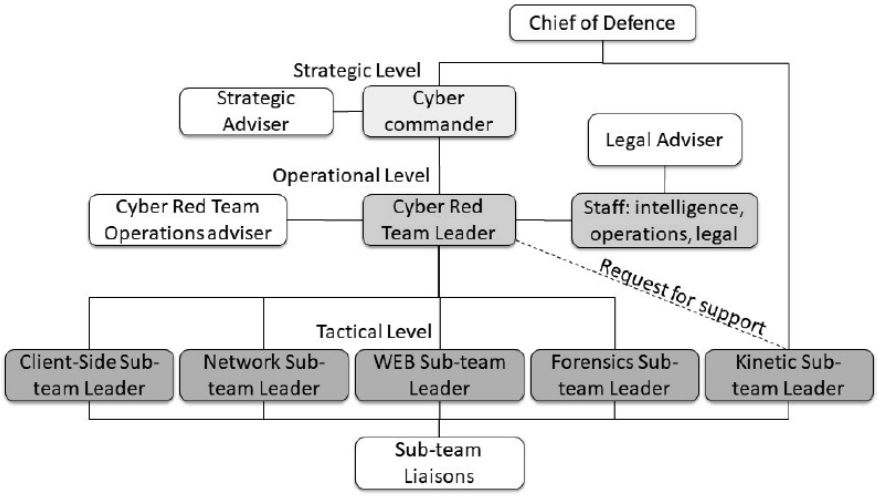

Figure 1: Exercise Crossed Swords 2019 Cyber Red Team chain-of-command (Blumbergs, 2019).

The 2019 Crossed Swords exercise adapted this structure to introduce a chain-of-command model with grey rectangles representing the Cyber Red Team at political, strategic, and tactical levels. Chain-of-command represents a hierarchy of authority in which each position is accountable to the one directly superior. This highlighted linkages to exercise control functions and sub-teams are based on expertise in targeted technologies.

An alternative model is utilised in Estonia's Defence Forces Command organisational structure by Kohler (Kohler, 2020). This offers an example of how the organisational structure of the Cyber Command can be located inside the broader Armed Force's organisation.

The Cyber Commanders' handbooks provide a helpful reference organisational structure for those nations seeking to establish an initial capability. In addition, Dr Blumberg provides a basis for developing Cyber Red

Teaming structures for exercises. These structures for peacetime cyber operations should be independent of other military Services and supported by research and cyber range capabilities.

3.2 Selected Cyber Exercises Organisational Structures Review

The Locked Shields 2022 Blue Teams' "after-action" reports reveal their organizational structures, with 14 out of 23 reports providing an overview. Multi-nation structures were excluded because they are often operation/case-specific and thus temporary. This research resulted in reviewing nine national team structures, including the related functional components such as the departments or teams within the organisation. An analysis of these structures focused on identifying commonalities and differences. Figure 2 illustrates the organisational structure of each team. The horizontal axis represents the team number, and the vertical axis represents the elements in the organisation. The minimum number was eight elements, the maximum was 23, and the average team consisted of 14 elements. The elements of the structures represent the roles and departments or teams within the organisation.

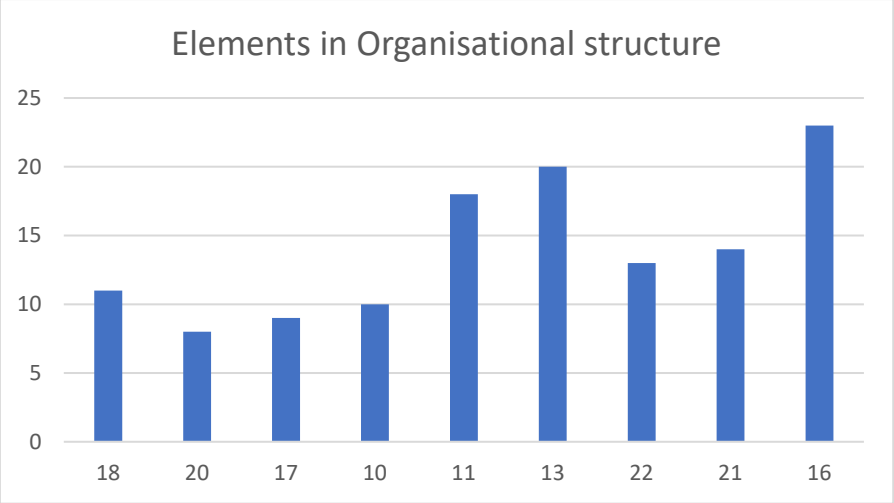

Figure 2: Exercise Locked Shields 22 selected Team Elements in Organisational Structure.

Figure 3 illustrates the number of personnel in each team. The average was 80 persons per team, with the smallest number being 50 and the largest comprising 102 people. The horizontal axis represents the team number against the number of personnel in each team.

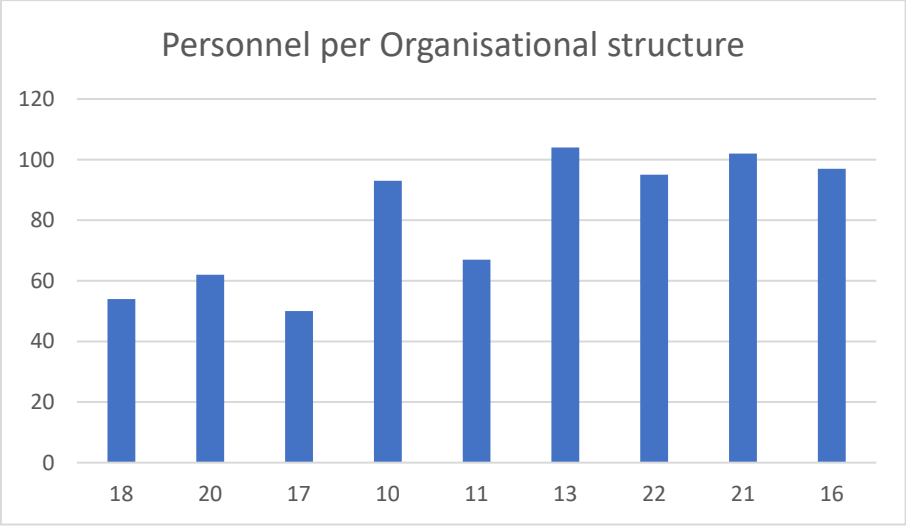

Figure 3: Exercise Locked Shields 22 selected Team Personnel per Organisational structure.

Error! Reference source not found. indicates the proportion of each team with earlier experience in a similar exercise.

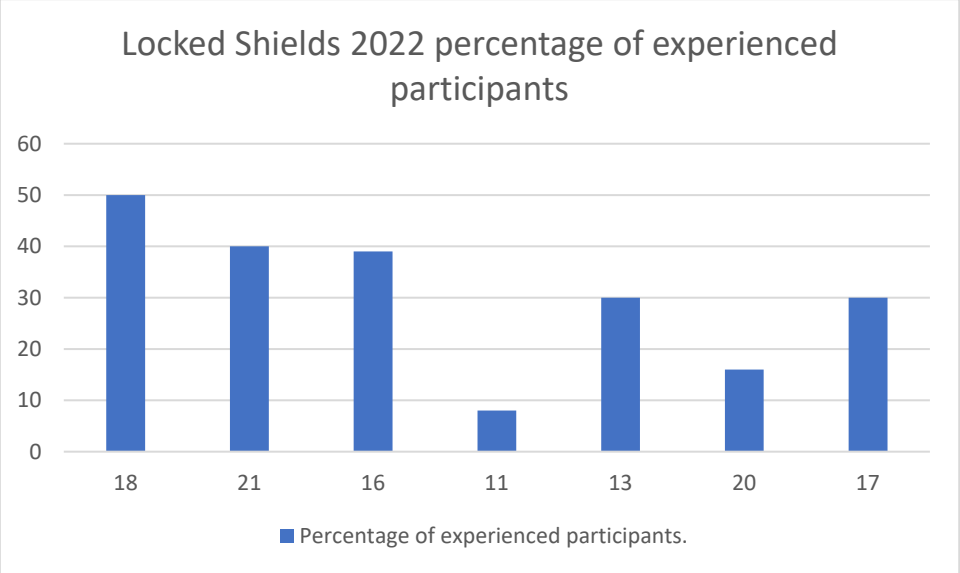

Figure 4: Locked Shields 2022 percentage of experienced participants.

The following section highlights the key attributes of a sample of a team's organisational structure.

The organisational structure of team Number 18 is shown in Figure 5. It should be noted that this team was the winner of the exercise. The winning score was calculated by CCDCOE's exercise evaluation team and is based on a complex scoring algorithm, which includes factors such as cyber-attacks successfully defended, availability of defended assets, forensics and legal.

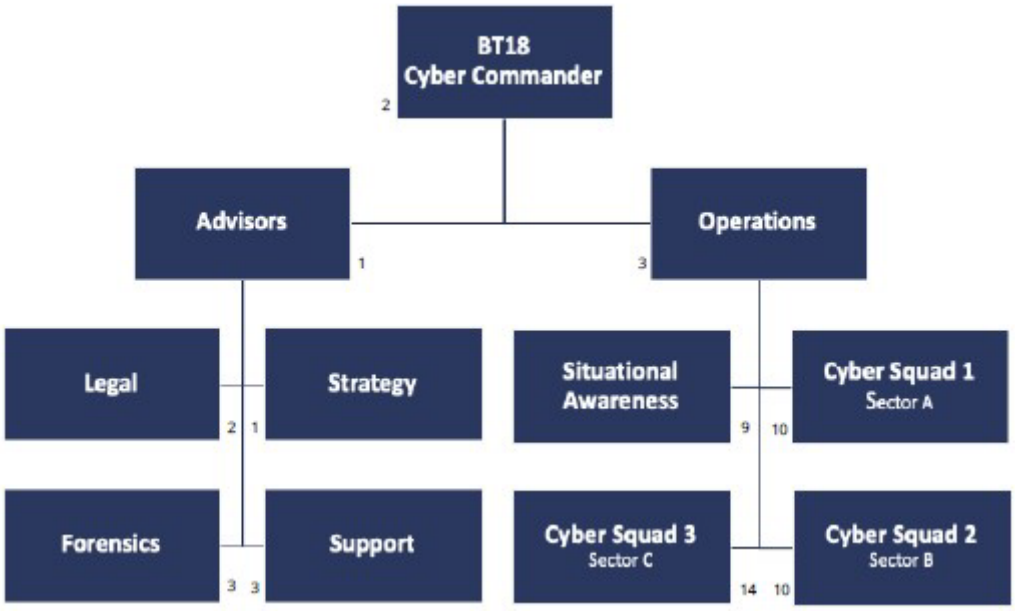

Figure 5: Exercise Locked Shields 2022 Blue Team 18 organisational structure.

Team number 20 had an operational framework and objectives based on various software applications. A little over a quarter of the team had participated in previous similar exercises. Based on the exercise scoring system, the team's results were in the last third.

Team number 17 had team objectives in place, and their strategy and tactics were derived from their national Standard Operational Procedures (SOP). Many tools were used, both in-house and externally provided. The team was placed close to last based on the exercise scoring system.

Team number 10 utilised a capability-based approach, focusing on results unrelated to team size. Capability-based planning is an approach that ensures that changes in an organisation are aligned with the overarching strategic vision. Their unique organisational structure includes a Task Group, Tactical Operations Commanders, and a Joint Cyber element. The team's results were in the bottom third.

Team number 11, organisational structures, used elements from different domestic organisations. These elements originated from the nation's military, governmental and academic sectors. Based on the exercise scoring system, the results of this team were slightly below average.

Team number 13 comprised 104 participants from 25 organisations with a complex organisational structure. Based on the exercise scoring system, the team's results were in the last third. However, they planned to maintain this structure for subsequent exercises, with only a proposed increase in information-sharing and reporting aspects.

Team 22 combined military and civilian personnel with six sub-elements and was placed in the top five.

Team 21 comprised 102 participants from 25 organisations, including private companies, energy, finance, national police, military, and telecoms. Despite providing their team objectives, the strategy and tools used were withheld from the report. This team was placed in the top ten.

Team number 16 had 97 participants from private and governmental sectors, including the military, public agencies, and academia. A distinctive feature of this team was the inclusion of a Finance element, and they were also placed in the top ten.

The results of the "after-action" reports are summarised in Table 1, and their similarities are highlighted.

Table 1: Exercise Locked Shields 2022 AAR summary.

Strategy in place	Tactics in place	Goal set	Tools	Previous LS experience	Military leader	Forensics el. in structure	Legal el. in structure
66%	44.00%	88.00%	88.00%	75%	77%	55%	88%

4. Results of the Interviews

While preparing for the Crossed Swords exercise, an interview was held with the cyber headquarters' chief of staff (COS) (CHQ). The CHQ was the only operational-level headquarters involved in the exercise. The interview was focused on the organisational command structure for the exercise.

The command element organisational structure is shown in **Error! Reference source not found.**6 and was based on the previous year's exercise. Based on the exercise feedback, mentors were added for the 2022 exercise organisational structure. The exercise feedback was received through the questionnaire that the article's author conducted in December 2021. These were utilised to share knowledge and pass the experience to the new cyber operators (Gaston, 2022).

In 2022, CHQ initially utilised the Military Decision-Making Process (MDMP) to develop Standard Operating Procedures. However, the lead author of this paper proposed an alternative approach called Intelligence Preparation of the Cyber Environment (IPCE) (Lemay et al., 2014) to complement the MDMP process. The military decision-making process (MDMP) is an iterative planning methodology. However, the IPSE complements it with a detailed intelligence planning process to address the limitations of cyber operations planning.

The CHQ aimed to create an operational plan for sub-units, practice MDMP, and improve procedures. They focused on planning tasks, aligning tasks with relevant kinetic military units, and considering interactions between the Air Force, Navy, and cyber units. The Commander had complete command of the tactical units, divided into Defensive (DCO) and Offensive (OCO) teams. Live exercise units are marked in **Error! Reference source not found.** 6 with dotted lines.

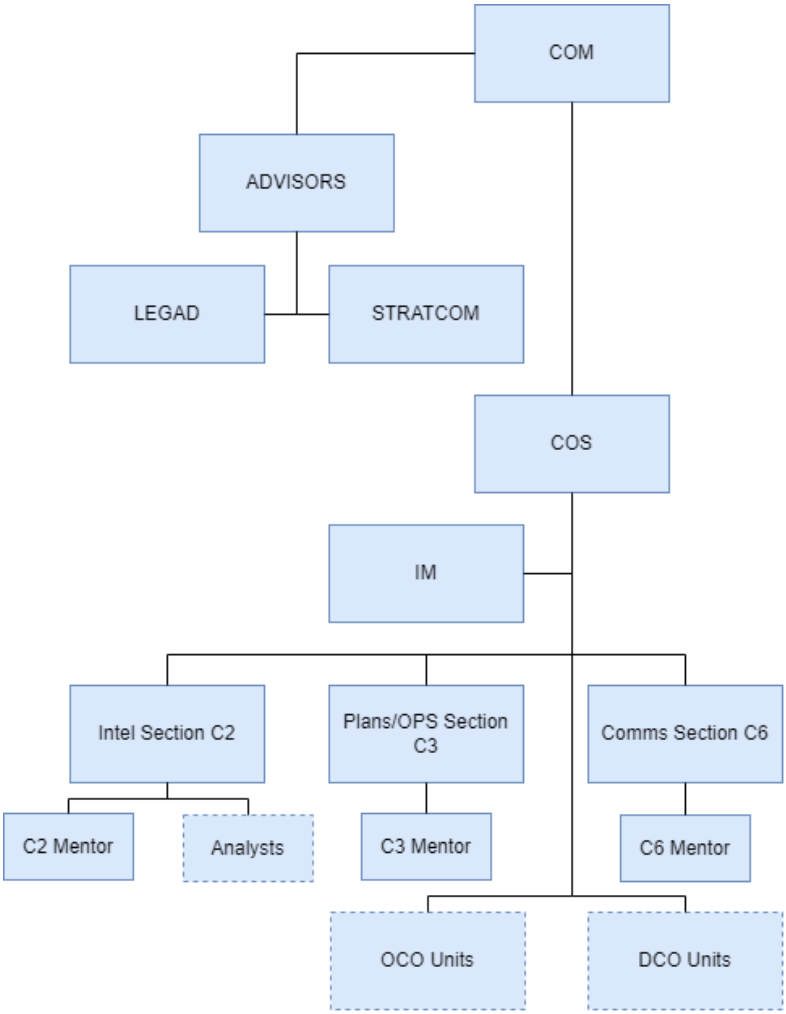

Figure 6: Estonian Defence Forces Cyber Exercises 2022 CHQ organisational structure.

The challenge in creating a cyber exercise command structure is appointing suitably qualified and experienced staff to critical positions. These include technical operators and intelligence and operations personnel to ensure a clear and comprehensible structure for military entities. The exact number of C2 and C3 positions should be proportional to the intensity of the exercise. The most critical roles from the CHQ planning perspective are C2, C3, COS, and Legad.

4.1 LS 2022 Case Study

In April 2022, the CCDCOE held the international cyber defence exercise, LS 2022, which involved 2000 participants from 32 nations (Papp, 2022). At the beginning of the exercise, the Red Team leader was interviewed to determine the prerequisites for conducting Red Teaming.

Successful Red Teaming exercises in tactical units require a two-day workshop, rigorous screening, and subjective assessment. Emphasising the importance of harmonised teams, the Red Team leader assembles sub-teams and identifies non-harmonized teams as a known weakness leading to mission failure. Novel aspects include recognising the significance of understanding Blue Team's motivations, the ability to develop custom tools, and adaptability to exercise the infrastructure's tempo. These prerequisites ensure a robust foundation for effective Red Teaming operations, encompassing technical readiness, strategic understanding, tool development proficiency, and flexibility in response to exercise dynamics.

The second interview with the Red Team leader took place in September 2022. The interview was about preparing an organisational command structure for Locked Shields. The interview aimed to illustrate and specify the details of the Read Team organisational command structure.

The Red Team's management methodology is based on twelve years of experience in cyber exercises. This allows the Red Team leader to plan and control activities without a detailed order, utilising good memory, common sense, and realism. The Red team composition is shown in *Figure* 7.

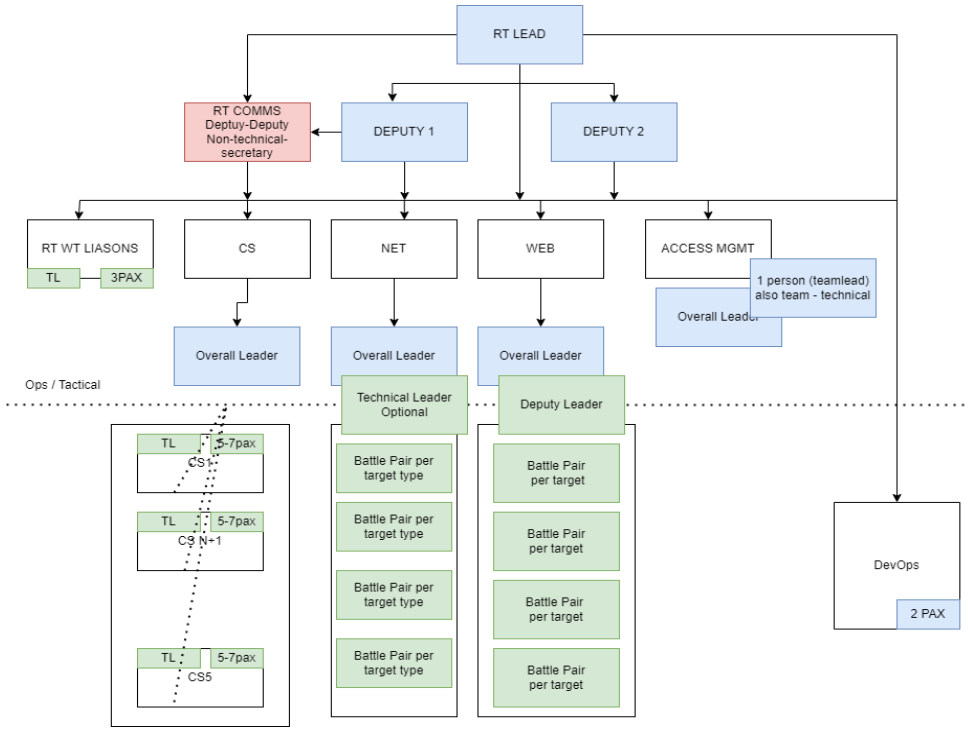

Figure 7: Exercise Locked Shields 2022 Red Team organisational structure.

The Red Team structure during the Locked Shields exercise consists of the following sub-teams: network (NET), client-side (CS), web application (WEB), and access management team. The NET team handles network attacks, the CS team prepares and executes client-side attacks, and the WEB team handles web application attacks.

The Red Team leader and their two deputies managed the major DevOps and COMMS teams. These created technical tools for the Red Team and managed information and human resources. The CS team had five sub-teams led by a Team leader, with five to seven subordinates, compared to NET and WEB teams, which were divided into battle pairs per target type.

The Red Team leader created a scalable structure depending on the size of the exercise, with the operational level handling mission planning and the tactical level engaging targets. The technical team leads with field experience supporting operational planning, while other participants support the command element. Sub-teams are involved with CS, NET, and WEB mission development to execute decisions during planning.

A further interview was conducted with a former military officer who has experience planning cyber operations. The interview highlighted the differences between real-life and exercise structures and was conducted before the CS 2022 execution period in November 2022.

The interview suggested that a headquarters' organisation is determined by exercise objectives and the Commander's experience or can be created through dialogue between higher command and tactical units. It was highlighted that a rule of thumb in military structures is that a commander should have at most seven subordinates to ensure the effectiveness of command and control (C2) activities. The meaning of command is the authority delegated to someone/somebody to give orders and directions, and control – is the ability to influence the execution of the orders mentioned above by allocating or withholding resources needed. This applies to cyber organisations as well as conventional military structures.

4.1.1 Locked Shields

LS exercises follow procedures to maintain the technical integrity of the network, which can prevent operational testing due to planning constraints. However, real-life operations have no restrictions, with politicians deciding priorities.

Blue Teams are often pre-formed with internal C2 structures and pre-agreed procedures created for mutual understanding and interoperability. However, this setup has limitations, requiring minimal modifications and preventing operational-level involvement.

4.1.2 Crossed Swords

In contrast to LS, most of the CS training audience (TA) is brought together as individuals only for the exercise execution without prior collaboration training. The structures formed for the exercise cannot go through team dynamics such as forming, storming, norming, and performing. This describes the path teams follow to high performance (Tuckman, 1965).

The CS exercise enables cyber headquarters personnel to simulate real-world scenarios, training in a realistic and dynamic environment. In contrast, the LS exercise maintains fixed rules, limiting its focus to technical aspects and revealing operational gaps due to shorter planning times. Participants need help integrating technical, operational, and strategic layers, particularly in the operational domain, where resources may need to be increased. Preparing competent cyberspace officers, establishing specific goals, and considering Joint Multinational Training Center (JMRC, 2022) courses are recommended to address this. Drawing inspiration from a similar training approach at the Joint Multinational Training Center in Germany, incorporating full-time military unit engagements against opposing forces could be a valuable future enhancement for CS exercises.

The CS Cyber Command element headquarters (CHQ) for the observed exercise was established Ad hoc. It was compiled from individual experts rather than involving an established vertical organisational structure. This provided the opportunity for CHQ to utilise previously developed and tested SOPs. The exercise provides an opportunity to test and re-assess the SOP and implement improvements based on the experience gained. In 2022, CHQ planned to develop and test its SOP. An iterative planning methodology known as the military decision-making process (MDMP) was used to comprehend the situation and mission, devise an action plan, and create an operating plan or order. The MDMP is designed against a predictable enemy who follows a doctrinal approach.

Based on the US Marine Corps Cyberspace Training and Readiness Manual, the recommendation is to create a Mission Essential Task List (METL) to address operational issues (NAVMC, 2018). The METL aids in defining organisational structures, tools, and equipment for planning, developing, and executing cyber operations. An example of Mission Essential Task List Relations in the Crossed Swords Exercises is provided in Figure 8.

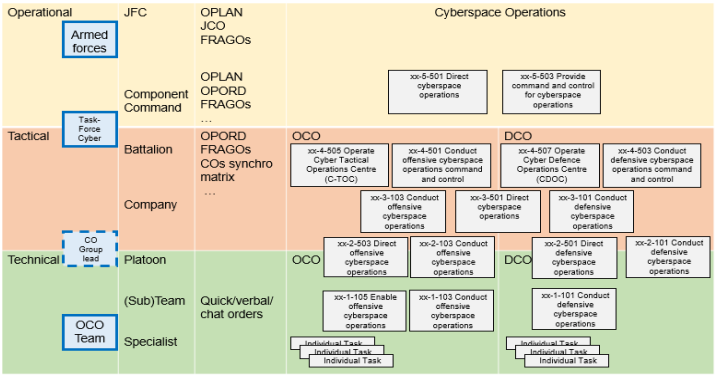

Figure 8: Example Mission Essential Task List Relations in the Crossed Swords Exercises.

A concluding interview transpired with a Plans Staff Officer within the NATO Cyberspace Operations Centre (CYOC). It was asserted that the exercise's command and control (C2) framework ought to be meticulously delineated, encompassing due consideration for the headquarters' inherent processes and procedures. The structural configuration should be tailored to align with the distinct objectives of the training audience, contingent upon their hierarchical positioning within the organisational framework.

Regarding the differences between cyberattack and -defence organisational structures, NATO's official policy is defined as "NATO is a defensive alliance with no plans to develop its offensive cyber capabilities. In cyberspace, as in all other domains, NATO acts in line with its defensive mandate and international law" (Ackerman, 2019). Therefore, it can be concluded that NATO has not developed its own OCO capabilities. Instead, it relies on its Member States. The Sovereign Cyber Effects Provided Voluntarily by Allies (SCPEVA) mechanism requests offensive cyber effects on a target (Goździewicz, 2019).

An exercise organisational structure requires a clear understanding of roles, responsibilities, and authority, addressing all functional areas without overlapping responsibilities. Integrating cyberspace into all HQ functions is the best practice. Different exercises should focus on training technical, operational, strategic, and political participants. A diverse range of stakeholders is crucial for success. Additionally, innovative aspects of the layered exercise design are proposed. Recommending distinct exercises for technical, operational, strategic, and political level participants to address their specific training requirements.

4.2 Findings from the Interviews

The main challenge in building a cyber exercise command structure is staffing the required positions, selecting people with the appropriate cyberspace competencies, and having well-instructed sub-team leaders. A goal-oriented structure with seven to eight subordinates is essential, with technical leads providing opinions on operational planning. Cyber operations exercises should involve strategic and operational planning, including cyberspace experts and trusted agents. Addressing the operational level planning resource gap is crucial, with a proposed Joint Multinational Training Center as a potential solution. To excel, create a cyberspace-specific framework for planning and execution, set training objectives, and effectively manage time. The uniqueness of a cyber exercise command structure lies in its specialised staffing, technical focus, goal-oriented approach, inclusion of cyberspace experts, international collaboration, cyberspace-specific framework, and emphasis on addressing operational challenges specific to the cyber domain. A Mission Essential Task List (METL) is crucial for organisational structures, setting mission-critical tasks with necessary tools and equipment. This study proposes Intelligence Preparation of the Cyber Environment (IPCE) as a supplement to the iterative MDMP, providing a detailed intelligence planning process to enhance cyber operations planning.

5. Results

An analysis of the organisational structures of the Blue Teams participating in LS enables structural elements to be correlated with the place achieved in the exercise. Figure 9 shows that in the top three teams (teams nr 18, 22, and 21), the number of elements in their organisational structure ranges from eleven to fourteen. Although this might suggest that the most optimal number of organisational elements is in this range, further research is required to analyse each team's skill set. No clear indication of an optimal team size based upon this limited sample size is recognised, and these results represent only Exercise Locked Shields 2022.

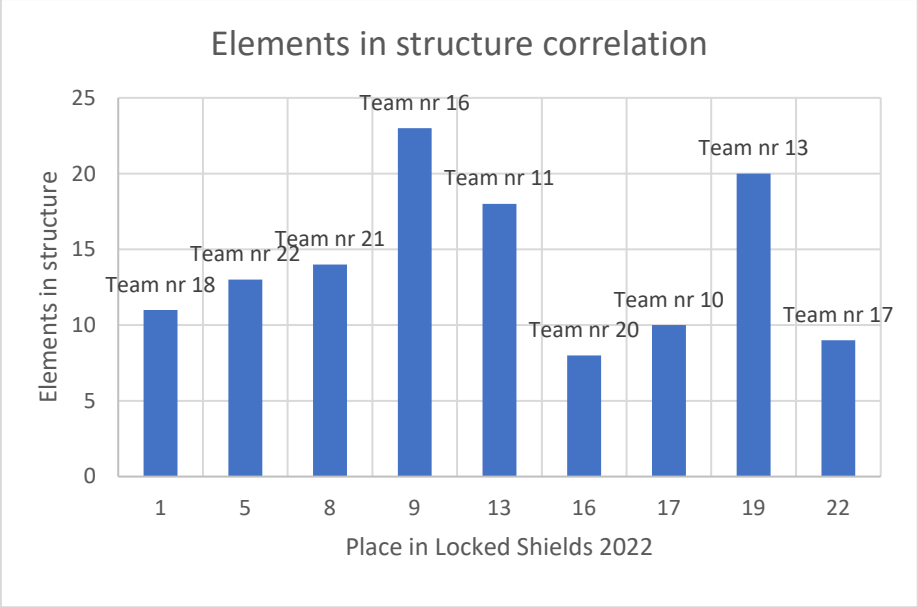

Figure 9: Exercise Locked Shields selected Blue Teams organisational structure, element count correlation.

A further characteristic recognised is the number of people per organisational structure. This is illustrated in Figure 3 and Figure 10, which illustrate the personnel appointed in each team's organisational structure in correlation with the place achieved in the exercise. The top three teams are highlighted on the left side of the graph. Their personnel count per organisational structure remains between 54 and 102. The personnel to organisational structure element ratio for the first-place team is 4.9, for the second 7.3 and the third 7.2. The

22nd team had a ratio of 5,5, and the 19th-place team had a ratio of 5.2. This indicates that the ratio of the number of people per organisational structure and the team size is irrelevant to the team's overall success. Over half of the observed teams had more than 80 persons per organisational structure. This might indicate that the number of people per organisational unit and units per team does not significantly influence the team's success.

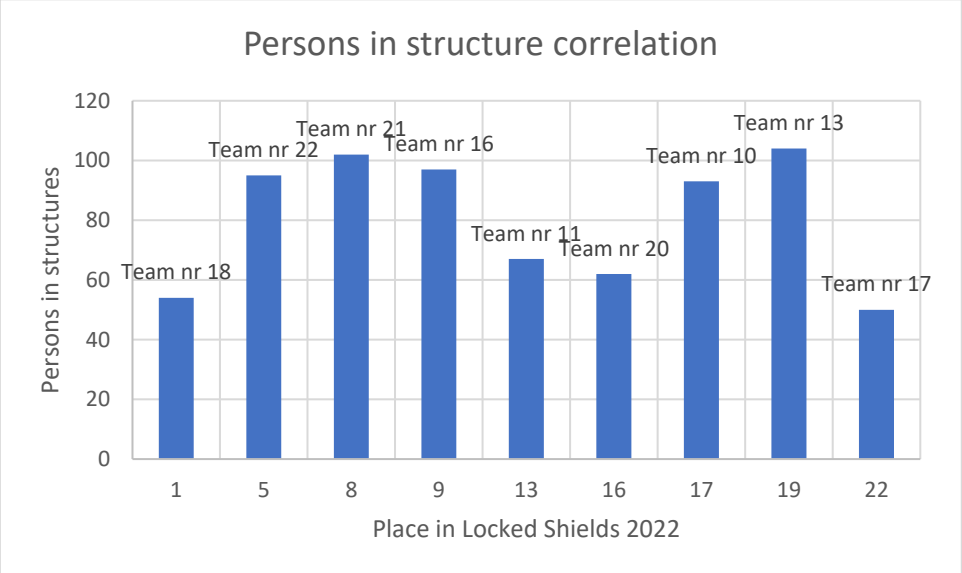

Figure 10: Exercise Locked Shields selected Blue Teams organisational structure, personnel count correlation.

The study analysed team composition and personnel count per organisational structure. The winning team had 11 elements, 54 personnel, and an average 4.9 personnel-to-structure element ratio. The correlation between place in the exercise and number of people was -0.09, suggesting a need for more relevance in success. The study reveals that success in the Locked Shields exercise relies on well-defined strategies, clear training objectives, technical readiness, and personnel experience, with team size and structural elements not determining success.

Successful teams in the Locked Shields exercise have standard skill sets, including military commanders, forensics, and legal advisors. They prioritise strategic planning and collaboration, engaging organisational structure members 3-4 months before exercise execution. They rely on customised software tools, demonstrating adaptability and commitment to technology readiness.

The success of LS team structures relied on effective leadership, specialised elements, early planning, and tailored software tools, providing valuable insights for cybersecurity exercise preparedness.

In compiling all the data collected, the optimal structure for the Locked Shields Blue Teams may consist of 11 elements and 55 personnel. At a minimum, there must be the following elements: a commander, Legad, forensics, and technology capabilities. Based on the exercise's technical challenges, up to eight separate Technology Capabilities elements might be included. These skillsets are shown in Figure 11 and could include capabilities such as Industrial control system (ICS), Network, Windows, Linux, Monitoring, Web, Mobile and Threat Hunting.

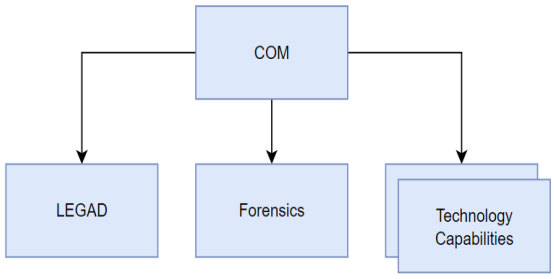

Figure 11: The Optimal Blue Team Structure for Locked Shields Exercise

6. Conclusions

The research emphasises the need for adaptive organisational structures in cyber exercises, addressing challenges unique to cyber operations training. A resource gap in cyber headquarters development requires preparing competent officers and leveraging training programs. This underscores the complexity of cyber exercises, emphasising continuous improvement and flexibility in structures and training to meet incipient expectations.

Cyber power countries are adjusting their cyber operations structures for future employment, requiring modifications to their Cyber Commanders Handbook and goal-specific structure for NATO exercises.

The Estonian Defence Forces Command's organisational structure is an example, and nations should consider the need to train dedicated cyber ranges. Dr. Blumbergs' designed chain-of-command for the Crossed Swords exercise is advantageous, as it outlines the hierarchy of tactical, operational, and strategic levels.

The top three Blue Teams' organisational structure elements in Exercise Locked Shields 2022 were 11-14, with 8-15 elements, although there needed to be a clear correlation and further analysis is required. As for conventional exercises, cyber exercises should include tactics, strategies, objectives, and tools with experienced individuals. Military commanders are preferred to the team, with members forming 3-4 months before an exercise. The Blue Teams structure typically includes Legal, Strategy, Advisors, and Operations, which are managed by the headquarters Plans/Operations (C3) sections. The EDF Cyber Exercises 2022 CHQ structure faced challenges in filling the necessary planning staff, as cyber operations planners' competencies are uncharted, requiring further research. The structure should be proportional to the exercise level and complexity.

Dr. Blumberg's design of the Red Team's organisational structure for Locked Shields is nearing optimal. With team leaders having no more than five to seven subordinates, goal-oriented is supported by interviews and provides an optimal and scalable structure for Red Teaming exercises.

A distinctive feature of the Red Team is that no specific direction is needed depending on the attackable systems and experience of the Red Teamers. However, Blue Teams need a higher command level to plan and maintain DCO. Therefore, planners and commanders must understand this essential difference and that roles, procedures, and tools differ. Red Teams focus on recruiting individuals with practical and hands-on skills relevant to cyber operations. In contrast, blue teams manage structures that categorise members based on specific skill sets, such as specialising in cybersecurity products or defendable assets. The need for additional research is emphasised, suggesting that further investigation or exploration is required to understand and refine the distinctions and roles within these teams. Red Teamers require special tools, infrastructure, and planning time, with good sub-team leaders and harmonised teams.

Planning officers must understand command-and-control authority and chain-of-command differences and integrate cyber into all HQ functions to prepare for entire spectrum operations, integrating kinetic and cyber operations.

Exercise participants face technical, operational, and strategic challenges, particularly at the operational layer. Cyber headquarters structural evolution needs faster development, with increasing numbers of competent officers and specialists needed. CHQs need to improve SOP and cyber operations planning, using alternative methods and setting goals during execution. However, in-depth planning is challenging due to strategic, operational, and tactical differences between cyber and other operations.

The research recommends implementing the US Marine Corps Cyberspace Training and Readiness Manual's recommendation for creating a Mission Essential Task List to enhance preparedness and operational response.

As cyber exercises increase in complexity, the command-and-control aspect for each headquarters becomes more critical. The CYOC experience underscores the need for diverse technical, operational, strategic, and political layers in one exercise, fostering trust and building cyber operations training structures.

This research revealed the complexity of cyber exercises and the importance of planning, training, and collaboration to address the unique challenges of cyber operations. It also highlights the need for adaptation and flexibility in organisational structures to meet the evolving demands of cyber operations training.

References

Ackerman. (2019) “NATO Cyber Policy Under Construction”, [online], https://tinyurl.com/txwufe8b
Blumbergs. (2019) “Specialized Cyber Red Team Responsive”. Tallinn: Tallinn University of Technology.
Dalmijn et al. (2020) Cyber Commanders’ Handbook. In NATO CCDCOE Publications (pp. 26-27). Tallinn: North Atlantic Treaty Organization.
Gaston. (2022) “Air Force officers share paths to personal and professional success with cadets”, [online], https://tinyurl.com/bdwhyd3a
Goździewicz. (2019) “Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)”, [online], https://tinyurl.com/4zjydnpe
JMRC. (2022) “7th Army Training Command. Retrieved from 7th Army Training Command”, [online], https://www.7atc.army.mil//
Kohler. (2020) “Cyberdefense Report: Estonia’s National Cybersecurity and Cyberdefense Posture. Zürich: ETH Zürich”.
Lemay et al. (2014) “Intelligence Preparation of the Cyber Environment (IPCE)”, Journal of Information Warfare, Vol. 13, No. 3 (2014), pp. 46-56.
NAVMC. (2018). NAVMC 3500.124. Department of the Navy Headquarters United States Marine Corps.
Papp. (2022) “Locked Shields 2022 - Multinational Cyber Defense Exercise”, [online], https://defence.hu/news/locked-shields-2022-multinational-cyber-defense-exercise.html
Pederson et al. (2022) “DOD Cyberspace: Establishing a Shared Understanding and How to Protect It”, [online], https://tinyurl.com/y6dvyn4p
Pernik. (2020). Handbook of International Cybersecurity. Routledge: National Cyber Commands.
Pomerleau. (2022) “DoD must focus on skilled cyber defenders, not just new tech, warns weapons tester”, [online], https://tinyurl.com/4fzyu6c2
Tuckman. (1965) “Developmental Sequence in Small groups”, [online], https://tinyurl.com/2xymzt7z
Voo et al. (2022) “National Cyber Power Index 2020”, [online], https://tinyurl.com/2aukkv4z