Planning Cyberspace Operations: Exercise Crossed Swords Case Study

M Arik, A Venables, R Ottis

Tallinn University of Technology
Faculty of Information Technology
Tallinn, Estonia

E-mail: maarik@taltech.ee; adrian.venables@taltech.ee; rain.ottis@taltech.ee

Abstract: *Preparation of cyberspace operations (COs) requires planners to consider technical peculiarities, which are not relevant in terms of planning traditional military operations (Barber, Bobo & Sturm 2015). Using Exercise Crossed Swords 2021 as an experimental test bed, a review of the latest NATO doctrinal developments, structured interviews, and a questionnaire were undertaken. The literature review revealed thirteen specificities of COs, and the interviews allowed for the identification of prerequisites for COs planning on strategic, operational, and tactical levels. The questionnaire highlighted four additional areas for improvement in CO planning. As a result of this investigation, twenty improvements to cyberspace operational planning are proposed.*

Keywords: *Cyberspace Operations Planning*

Introduction

Cyberspace is one of NATO's five operational domains. It was recognised as such in 2016 as the fourth domain joining land, sea, and air, and was followed by Space in 2019 (CCDCOE 2021). All NATO member states have national cybersecurity incident response teams, and many are still developing cyber operations capability to improve their capability in this domain. Additionally, NATO has agreed to set up a new Cyberspace Operations Centre as part of its strengthened Command Structure (CCDCOE 2021). There is also a growing interest in offensive cyber operations (OCO) for military purposes, which is expressed in the creation of NATO cyber commands, branches, or services within the armed forces (CCDCOE 2021). By 2022, 27 of the 30 NATO member states will have created cyber forces with Luxemburg, Montenegro, and North Macedonia remaining the exception. Training and exercising are conducted by the NATO-affiliated Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, which hosts the annual Exercise Crossed Swords (CCDCOE 2022). This exercise includes leadership training for the command element, legal aspects, and joint cyber-kinetic operations, in addition to the technical challenges (CCDCOE 2022). For the past two years, Estonia's Cyber Command Headquarters has been engaged in planning and executing cyberspace operations (CO) as part of a wider kinetic military operations process.

To assist commanders and their staff in operational planning, NATO has come out with several joint publications. These include the Allied Joint Doctrine for the Planning of Operations (NATO Standard AJP-5 2019) and the Allied Joint Doctrine for Cyberspace Operations (Ministry of Defence UK 2020). However, as planning for COs requires additional elements compared to what

is typically involved in kinetic military operations (Barber, Bobo & Sturm 2015), further planning methodologies should be identified. These include deeper technical planning on a tactical level.

This article identifies and critically analyses the key differences between planning land-based military operations and planning COs. These are categorized and assessed with recommendations for improving dynamic CO planning. The specific contribution of this work is to propose improvements in CO planning and execution. For this purpose, the key differences between them, which can be validated in subsequent cyber exercises, are identified.

Methods

This paper uses experimental research employing the design science methodology (Kosmol & Leyh 2019) with Exercise Crossed Swords as the platform for concept development, experimentation, and validation. Structured interviews were conducted to extract, document, and analyse information from subject matter experts focussing on established best practices, known challenges, and individual experiences.

To assess CO development, planning, and execution, a literature review was conducted to examine current developments and military doctrines. This compared the latest NATO military operational and CO doctrines with the Allied Joint Doctrines for the Planning of Operations, Cyberspace Operations, Joint Doctrine Note 1-8 Strategy, and Allied Joint Doctrine for the Joint Intelligence, Surveillance, and Reconnaissance. These detail the joint and multinational operation principles for kinetic and COs. Military operational planning is a sequence of activities undertaken by the commander and his or her staff at all levels (Ministry of Defence UK 2021). However, cyberspace has unique characteristics in that it is fabricated, partly nonphysical, and may not conform to geographical boundaries (Ministry of Defence UK 2020). Planning CO goes beyond what is typically required for kinetic military operations and these unique attributes require a different approach in their preparation and conduct (Barber, Bobo & Sturm 2015).

Following the literature review, structured interviews with the commander of the exercise CHQ were conducted, which were complemented by discussions with CHQ section commanders. This was supported by a questionnaire that was distributed to the cyber headquarters element (CHQ) members on the final day of the exercise using the Google Forms platform. From a total of 23 staff members, 19 completed the questionnaire.

Joint NATO doctrinal publications principles have been practised in Crossed Swords exercises since 2019. The staff element—their processes and structure—have evolved over this period to expose a research gap identifying the differences between kinetic and CO planning within NATO.

Results

This section presents the significant findings of the work, starting with the literature review, followed by the interviews, and concluding with the questionnaire results.

Results of the literature review

NATO has released many Joint Publications on CO and military planning. These publications are intended to assist member states in forming the basis for joint operational planning. The latest NATO Joint Publication for operations planning, AJP-5 The Allied Joint Doctrine for the Planning

of Operations, was published in May 2019 (NATO Standard AJP-5 2019). The most recent publication on COs, the Allied Joint Doctrine for Cyberspace Operations (Ministry of Defence UK 2020), was published in July 2020.

The review of the Allied Joint Doctrine for the Planning of Operations and the Allied Joint Doctrine for Cyberspace Operations resulted in the following key findings:

Rules of engagement

In CO and military operations, ROE is issued to the Commander based on his or her delegated authority. COs require an appreciation of a range of legislation, including international law, national law, the United Nations (UN) Charter, Law of Armed Conflict (LOAC), and human rights law.

Higher intent and plan

The CO commander's intent may include defensive or offensive operations. If offensive cyberspace operations (OCO) are planned, they will be conducted through the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) mechanism, by the principles agreed to by NATO (Goździewicz 2019). As NATO has not developed its OCO capabilities but relies on its Member States, the SCPEVA mechanism is used to request offensive cyber effects on a target (Goździewicz 2019).

Complete intelligence analysis of the adversary

Allied Joint Doctrine for Cyberspace Operations refers to Allied Joint Doctrine for Joint Intelligence, Surveillance, and Reconnaissance (NATO Standard AJP-2.7 2019). Cyberspace intelligence is based on availability and sharing. As NATO does not have its own organic cyber intelligence capability, it relies on allied nations to provide this service. This is seen in the Joint Intelligence, Surveillance, and Reconnaissance (JISR) system, where Allies collaborate to collect, analyse, and share information (Joint Intelligence, Surveillance, and Reconnaissance 2022).

Situational awareness of adversary forces

"Gaining situational awareness of adversary forces requires conducting significant intelligence collection, which requires the knowledge of the interconnectivity of networks" (Weiskopff 2017, pp. 22-3). Additionally, in the context of cyber targeting, it requires constant updating to validate intelligence and the positive identification of targets in near real-time (Weiskopff 2017).

Clear definition of cyber effects

CO effects may be categorised as either desired or undesired as well as direct and indirect effects. These are included but are not limited to secure, isolate, contain, neutralize, recover, manipulate, exfiltrate, degrade, disrupt, or destroy. The effects-based operations (EBO) system can be used for targets that are either tangible or abstract (Weiskopff 2017). No definition of EBO has yet been agreed on. Still, for this paper, EBOs are defined as the operations conceived and planned in a systems framework that considers the full range of direct, indirect, and cascading effects. These include the application of military, diplomatic, psychological, and economic instruments of power (Davis 2001).

NATO higher level support in expectation management

Traditionally, in military operations, expectation management is based solely on commanders'

guidance. In OCO the commanders' expectations are partly pre-determined by the SCEPVA mechanism because the NATO OCO capabilities depend on its Member States (Goździewicz 2019).

Dynamic cyber space environment analysis

NATO operations generally occur in a dynamic environment in which actors continually change the political, military, economic, social, infrastructure, and information (PMESII) elements (NATO Standard AJP-5 2019). In operations planning, the PMESII model may be supported or succeeded by JIPOE (Joint Intelligence Preparation of the Operating Environment). Additionally, the Joint Doctrine Note 1-18, Strategy (Joint Doctrine Note 1-18 Strategy 2018) uses the DIME (diplomatic, informational, military, and economic) model to describe national power instruments. This emphasises the complexity of dynamic cyberspace environment analysis.

Technical cyber intelligence gathering

In military operations planning, the commander, the operations planning group, and the more comprehensive staff must formulate their priority intelligence requirements (PIR) and Commander Critical Information Requirements Management (CCIRM) function. Based on these requirements, intelligence processes will be established, where operations branch staff and intelligence functions synchronize and integrate all collections capabilities to support operational planning. In CO, the planning staff identifies relevant aspects of cyber intelligence in coordination with the Cyberspace Operations Centre (CyOC) and other branches and capabilities throughout cyberspace layers—the physical, logical, and cyber-persona. The physical layer consists of hardware components, tied to geographic location, with the logical layer comprising software and data components. The cyber-persona layer does not consist of actual people or organisations but is rather an image of their virtual identity (Ministry of Defence 2020).

Wargaming

In military operations planning, the courses of action (COA) are evaluated with wargaming. In CO planning, the anticipated effects are included in assessing the COAs and would be validated with the Cyberspace Operations Centre (CyOC).

Detailed overview of own forces capabilities

In military operations planning, the operations planning group is advised to consult early with the subject matter experts (SME) of the respective functional areas within its staff and other commands and the respective doctrine. Risk management and vulnerability assessment are examples of activities that help to achieve a detailed overview of their own forces during the preparation of DCOs (Ministry of Defence 2020).

Multi-layered dimension

"Another difference between traditional warfare and cyber warfare is that traditional warfare exists exclusively in the physical world whereas cyber exists in both a physical world and a logical one" (Weiskopff 2017, p. 20). The Allied Joint Doctrine for Cyberspace Operations describes the logical layer as follows: "Entities at the logical layer are elements manifested in code or data, such as firmware, operating systems, protocols, applications, and other software and data components. The logical layer cannot function without the physical layer, and information flows through wired networks or the electromagnetic spectrum. The logical layer, along with the physical layer, allows

the cyber-persona to communicate and act". The recent NATO Allied Joint Doctrine for Cyberspace Operations recognises the persona layer as a separate dimension for conducting COs. The logical and persona layers are not necessarily linked to one specific physical location or device.

High availability of cyberinfrastructure

Conventional military operations, in general, have always been a mandate for state-sponsored entities. In contrast, the cyber infrastructure's vast interconnectivity and high availability provide a wide range of cyber criminals with almost the same opportunities to execute malicious actions in the cyber domain (Weiskopff 2017). Governments and states tend to use cyber criminals as mercenaries.

Targeting

Traditional targeting commonly refers to an exclusive geographical position. On the other hand, achieving the desired effect using cyber means requires considering targets' physical and logical targets at once (Weiskopff 2018). One logical target can be in multiple locations—for example, a virtual server/host.

The Results of the Questionnaire

Between 6-10 December 2021, the CCDCOE organized exercise Crossed Swords 2021 was conducted. A questionnaire was distributed among the cyber headquarters element (CHQ) to assess cyber operations development, planning, and execution. The questionnaire was conducted using the Google Forms platform on the last day of the exercise (9 December 2021). Of the total of twenty-three staff members, nineteen participated in the questionnaire. The results are presented per category of topics.

Cyberspace definitions

Cyber operations were described in nineteen different ways with no referral to known doctrines. Approximately 36% of respondents described cyber operations close to NATO AAP's 2020 cyberspace definition (NATO - AAP-06 2021). 73% of CHQ personnel did not understand cyber terms and concepts uniformly.

Staff tasking and training

The roles and responsibilities among CHQ posts need to be better defined. The Senior leadership required more experience and time to plan and execute cyber operations. 65% of the CHQ staff members self-assessed that their roles were not matched to their abilities. A little over one-third (35%) of the CHQ staff stated that it required more experience to fulfil its post tasks. A third of the answers suggested that experienced mentors were required, while 66% of answers suggested that there was a need to have more exercises.

Mission and awareness

It was identified that the mission of CHQ was not clear among CHQ staff. Less than half (47%) of the CHQ staff understands the operational environment.

Improving the planning of the exercise

To improve the CHQ Exercise structure, the following thirteen different changes were suggested:

1. Improve CHQ SOP (Standard Operating Procedure).
2. Add current ops positions.
3. Add plan ops position.
4. Add C35 (Communications Systems).
5. Add C5 (Cyber, Command, Control, Communications, and Computers Assessments).
6. Add a Cyber Situational Awareness cell.
7. Add info ops officer.
8. Add a targeting officer.
9. Add LNOs to components commands.
10. Add additional information manager.
11. Have more leadership.
12. One answer suggested having several CHQs or several teams in all sections for different outcomes and planning structures.
13. One answer suggested changing the CHQ structure to more like an actual staff structure, with roles and processes.

Over a third of the proposals suggested improving various parts of CHQ SOP. Legal advisors pointed out that they would want to be more involved in the planning of COs. Prior to conducting a major exercise, questionnaire responders confirmed that they would want to have more, smaller, connecting tabletop exercises. Another important issue has been related to CHQ staff, where just over half of them had the software tools necessary to fulfil their duties.

Results of the Interview

A structured interview was conducted after Exercise Crossed Swords 2021. The Interviewee was Uko Valtenberg (OF3-RES), Estonian Defence Forces Cyber Command, Cyber Operations Centre commander in reserve, and Commander of Exercise Crossed Swords 2021 Cyber Headquarters. The interview results presented prerequisites to plan CO at the CHQ level. The CHQ was intended to be an operational level HQ but also had tactical elements, and, overall, the CHQ structure was not clearly defined. The interview revealed that few structural roles, such as cyber intelligence, were not played or present. Secondly, the CHQ began its exercise during the operation's second phase, just before the attack was planned. Specific comments from the interview were categorized through strategic, operational, and tactical levels.

Strategic level prerequisites for planning a CO

It is imperative to have Rules of Engagement (RoE) and a mandate to operate in adversary territory. The CHQ must be provided with a higher commander intent and plan to ensure that operation goals align with joint operation objectives. Preliminary target propositions must be presented to the CHQ to narrow down the scope of planning. A complete intelligence-driven overview of the adversary must be established to allow the CHQ commander to make informed decisions. A full overview of their own forces (including Allies and neighbouring troops), restrictions, and a deconfliction matrix must be provided to the CHQ to ensure efficient coordination of different activities.

Operational level prerequisites for planning a CO

Situational awareness with regard to their own and enemy forces is critical from a CO planning perspective. Developed targets must be prioritized and categorized (for example logistics, energy, military, financial) by the higher-level HQ to support the planning and allocation of available

resources. Cyber effect principles must be clearly defined, understood (for example: degrade, disrupt, deny, destroy), and accepted by all units involved in the CO. In other words, the plan should follow the same principles as in cyber incident management. Cyber planning staff should have a fundamental understanding of information technologies, cybersecurity principles, and risk- and security assessment. Higher level commander support in expectation management is required to ensure technical capabilities correspond to the expectations of operation participants.

Tactical level prerequisites for planning a CO

A commander must have a detailed overview of his or her own force's technical capabilities. It is expected that operators have passed the following training:

1. General IT and cybersecurity training.
2. Individual specialized training.
3. Team exercises.
4. Mixed teams' exercises.
5. Harmonized maturity level assessment.
6. Internal team assessment.

Pre-prepared technical environment

Technical tools (such as non-traceable accounts in different services and systems) used during a CO must be prepared before execution of a CO. ICT infrastructure used for executing the CO must be obfuscated and distributed to impede attribution and efficient implementation of countermeasures by the adversary. "For red teams, using an obfuscated network for testing offers the advantage of hiding who is performing the attack and where it is originating, for a more real-life context. It lets the red team blend in with the normal network traffic while performing reconnaissance and test attacks in a more realistic manner" (Lawson 2021).

Tactical level units must have dedicated support resources with regards to maintenance of CO ICT infrastructure and relevant tools. This is required to speed up the CO by allowing operators to focus on the objectives, instead of conducting administrative tasks during CO execution.

Additional prerequisites for planning a CO

Political, Military, Economic, Social, Information, Infrastructure, and Physical Environment (PMESII) analysis of operational area must be conducted to enable adequate planning activities. Target-related technical cyber intelligence must be provided to the CHQ at every stage of the CO.

Discussion and Conclusions

The planning of cyber- and military operations entails differences at the strategic, operational, and tactical levels. The list of significant findings is presented below, prioritized by their importance:

1. The interview revealed that the preparation of the technical environment should be considered the key element for planning CO. Tactical commanders should prepare an obfuscated and distributed ICT infrastructure for both training purposes and for conducting actual COs. The primary purpose of obfuscating and distributing ICT infrastructure is to mask interrelations of its components, ensure operation continuity, and aggravate attribution if and when individual ICT components are revealed by the target. Creating

and utilizing the preprepared technical environment requires deep-technical planning. The details of the technical environment should be planned and implemented according to the objectives of COs. Additionally, preparation, implementation, and administration of the technical environment require that sufficient resources be allocated to ensure operational security (OPSEC) principles and operational objectives are met.

2. According to the literature review, the complete preparation of forces requires operation planners to consult SMEs during the initial stages of the planning process. Preparation of DCOs involves the execution of risk management and vulnerability assessment activities. However, preparing OCOs requires a deep understanding of their own units' capabilities to achieve mission effects.
3. According to the literature review, the CO planning staff should formulate technical cyber intelligence requirements at all layers of cyberspace: the physical, logical, and cyber-persona. Requirements must be synchronized and integrated with all collection capabilities. Cyber commanders and staff should formulate all the intelligence requirements, regardless of their nature, and submit them to supporting intelligence mechanisms.
4. According to the interview and literature review, the CO mission analysis should include the complete PMESII or more advanced methods (like JIPOE). The PMESII-PT analysis and other similar techniques, such as METT-TC (Haugli 2016) provide the cyber commander with even more value for planning and executing COs.
5. According to the interview and questionnaire, CO tactical level wargaming or Purple Teaming is required before a major exercise or operation. Although wargaming is not an everyday activity concerning COs, it should be considered a critical necessity with a special focus on the technical level. An isolated technical environment is the first requirement to conduct tactical level wargaming. Such a technical environment should be designed as a laboratory (O'Leary 2019) for conducting tests and experiments.
6. According to the literature review and interview, the list of cyber effects is not final, and effect parameters should consider the cyber incident management principles. The parameters of CO's effects should follow the cyber incident management principles. How much of the target is disrupted, 1%-100%? The same principles apply to integrity, availability, and confidentiality impact. An example of an effect requirement for a military tactical operation can be formulated as follows: degrade availability of target ABC 50%, starting from (date, time) to (date, time). "Effects-based operations apply to the cognitive domain, they have the ability to affect the decisions of political leaders, military commanders, or even whole populations" (Weiskopff, p. 40).
7. According to the literature review, targeting in COs must be executed at three layers: the cyber-persona, logical, and physical layers. The enemy should be considered a complex system during the execution of effects-based operations (Weiskopff 2017). This means that cyberspace is considered one of the different attack vectors that targeters can exploit to affect the target. Target development involves the systematic discovery of enemy system components, including the linkage of those components to the actual target and the possible effects on the target if specific components (or linkages) were manipulated. Targeting different components of the same system, through synchronized efforts of available capabilities and resources, can improve the efficiency of effects-based COs. Systematically and consistently planned and executed effects-based COs have the potential to create an impact on a national/state level (Weiskopff 2017). Additionally, it must be considered that, while targeting physical cyber-infrastructure, the destruction or disruption will have collateral damage. COs are conducted primarily on civilian ICT infrastructure, which will

have adverse effects on civilian ICT services.

8. According to the literature review, public cyber infrastructures can be used by cyber criminals to execute malicious actions in the cyber domain. The Sandworm Team, a division of the GRU (Russia's General Staff Main Intelligence Directorate), is an example of a threat group that is known to be using a given approach (MITRE ATT&CK 2017). Ukraine's energy facility was attacked by a Sandworm group in February 2022. Attackers succeeded in planting a new version of the Industroyer malware to disrupt ICS infrastructure at different levels (Brumfield 2022). The cyberattack was detected and prevented by the Ukrainian team. The Ukrainian activity can be considered a self-defence act. "Self-defence in international law refers to the inherent right of a State to use of force in response to an armed attack. Self-defence is one of the exceptions to the prohibition against the use of force under article 2(4) of the UN Charter and customary international law" (International Committee of the Red Cross 2022).
9. According to the literature review, the intelligence processes will be the same but will rely on various sources. NATO does not have its own organic cyber intelligence capability and relies on allied nations to provide this service. A cyber commander should establish and maintain Cyber Intelligence Sharing procedures and channels with allies, partnering intelligence services and cyber incident response communities.
10. According to the literature review, it must consider a set of military doctrines to achieve complete intelligence concerning an adversary. The AJP3.20 doctrine is meant for addressing CO-specific planning. But still, it is related to two dozen other principles. The cyber commander should not focus solely on the cyber doctrines but must orient it in the maze of allied principles
11. According to the questionnaire, CO definitions are not uniformly understood. COs are an emerging discipline, whereas conventional military operations are better understood. It is recommended to use the latest cyberspace definitions for joint COs and exercises published by NATO.
12. According to the questionnaire and interview, the cyber-capable planning staff is a crucial necessity for planning CO. The commanders are responsible for training and preparing the team and for achieving the necessary cyber capabilities. Cyber planning staff should have a fundamental knowledge of information technology as well as a broad understanding of cybersecurity and the risks involved.
13. According to the questionnaire and interview, the CO planning staff should have a harmonized maturity level. The planning staff performs its tasks more unanimously and efficiently if its expertise levels are the same or close to each other.
14. According to the questionnaire, significant enhancements should be implemented to improve situational awareness of the cyber-operational environment. Two significant steps should be taken towards improvements in the operational situational awareness. First is to follow the "CRR Supplemental Resource Guide, Volume 10: Situational Awareness" (Carnegie Mellon University 2016). Secondly, it is necessary to plan and implement a visual tool for presenting and synchronising operational (situational awareness) information from different operation levels.
15. According to the questionnaire, the structure of CO in the headquarters element (CHQ) needs to be revised. It is not clear what the structure of a cyber-HQ staff should be. The proposed structure improvements should be implemented, evaluated, and validated in the following exercises.
16. According to the questionnaire, planning and executing COs require more specific tools.

Cyber commanders should be aware that the development and testing of custom software elements is a time-consuming process. Therefore, the requirements and functionalities must be carefully defined and budgeted promptly. The results of software development activities must eventually help to improve the following:

a. Internal and external cooperation.
b. Situational awareness of the operational environment.
c. Analysis of technical cyber-intelligence.
d. Task- and data-flow management.

17. According to the questionnaire and interview, the CO staff needs to pass a variety of additional training, along with individual specialized training, team exercises, mixed teams exercises, and internal team assessments. The planning staff needs to develop a coherent training plan to achieve a synchronised maturity level. The staff must be trained regularly, until it is capable of planning and executing CO as a team.
18. According to the questionnaire and literature review, legal advisors should be more actively involved in the operation planning process. Operation planners must consider the complex legal environment and involve legal advisors in every step of the operation.
19. According to the literature review, CO relies on cyber intelligence sharing, so liaisons should be involved in relevant branches and capabilities. The CO commander should appoint liaisons to partner branches and ensure appropriate channels and tools are used for (cyber-technical) intelligence sharing. An example of an open-source cyber threat-sharing tool is the MISP (MISP 2022).
20. According to the literature review, OCO involves coordination with the SCEPVA mechanism. NATO does not develop its OCO capabilities but relies on its Member States. The SCPEVA mechanism is used to request offensive cyber effects on a target. This means that cyber-capable nations may be asked to deliver offensive cyber effects on a target assigned by an operational-level commander (Goździewicz 2019).

These findings form the basis of CO planning improvements and should be considered in future CO doctrines, processes, and methods. The significance of this work is to clarify and improve the future of the planning and execution of CO. CO research is limited to exercises, as real-life operations are nationally classified. Subsequent cyber exercises should validate the findings of the current work.

As the usage of digitally assisted weapon systems during modern kinetic military operations inevitably increases, the importance of CO will raise exponentially. Command and control systems, communication networks, GPS-guided missiles, and pre-warning systems (like air-, sea- and land radars) are likely to become high-priority cyberspace targets.

Acknowledgements

The writer would like to express special gratitude to his colleagues at Talgen Cybersecurity OÜ: Mr Uko Valtenberg and Mr Kim Vahturov. Their cyberoperations-related experience allowed for valuable discussions and contributed to the quality of this publication.

References

Barber, D, Bobo, A & Sturm, K 2015, 'Cyberspace operations planning: Operating a technical military force beyond the kinetic domains', *Military Cyber Affairs,* vol. 1, no. 1, pp. 1-8, viewed 19 March 2022, <https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1003&context=mca

/>.
Brumfield, C 2022, 'Ukraine energy facility hit by two waves of cyberattacks from Russia's Sandworm group', viewed 6 November 2022, <https://www.csoonline.com/article/3656954/ukraine-energy-facility-hit-by-two-waves-of-cyberattacks-by-russia-s-sandworm-group.html>.

Carnegie Mellon University 2016, 'CRR supplemental resource guide,' vol. 10, *Situational Awareness*, Version 1.1, viewed 5 November 2022, <https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-SA_0.pdf>.

Cooperative Cyber Defence Centre of Excellence (CCDCOE) 2021, 'Cyber defence', 2 July, viewed 19 March 2022, <https://www.nato.int/cps/en/natohq/topics_78170.htm/>.

—2022, 'Crossed Swords', viewed 19 March 2022, <https://ccdcoe.org/exercises/crossed-swords/>.

Davis, PK 2001, 'Effects-based operations a grand challenge for the analytical community', viewed 23 May 2022, <https://www.rand.org/content/dam/rand/pubs/monograph_reports/2006/MR1477.pdf>.

Goździewicz 2019, 'Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA), viewed 10 May 2022 < https://www.cyberdefensemagazine.com/sovereign-cyber/>.

Haugli 2016, 'METT-TC – What does it actually entail?', viewed 10 May 2022, <https://primaryandsecondary.com/mett-tc-what-does-it-actually-entail/ />.

International Committee of the Red Cross, 'Self-defence', viewed 6 November 2022, <https://casebook.icrc.org/glossary/self-defence#:~:text=Self%2Ddefense%20in%20inter national %20law,Charter%20and%20customary%20international%20law>.

Joint Doctrine Note 1-18 'Strategy' 2018, viewed 18 May 2022, <https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_18.pdf/>.

Joint Intelligence 'Surveillance and Reconnaissance' 2022, viewed 3 May 2022, <https://www.nato.int/cps/en/natohq/topics_111830.htm#:~:text=NATO%20has%20established%20a%20permanent,Alliance's%20deterrence%20and%20defence%20posture.>.

Kosmol, L & Leyh, C 2019, 'ICT usage in industrial symbiosis: Problem identification and study design', *Annals of Computer Science and Information Systems*, vol 18, pp. 685-92, viewed 19 March 2022, <https://annals-csis.org/proceedings/2019/drp/pdf/323.pdf>.

Lawson, G 2021, 'Securityweek 2021, How to improve red team effectiveness using obfuscation', 18 November, viewed 16 April 2022, <https://www.securityweek.com/how-improve-red-team-effectiveness-using-obfuscation>.

Ministry of Defence (UK) 2020, 'Allied Joint Publication (AJP-3.20): Allied joint doctrine for cyberspace operations', viewed 19 March 2022, <https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320/>.

—2021, 'Allied Joint Publication (AJP)-5(A) Allied Joint Doctrine for the planning of operations', updated March 2021, viewed 19 March 2022, <https://www.gov.uk/government/publications/allied-joint-publication-ajp-05a-allied-joint-doctrine-for-the-planning-of-operations/>.

NATO Standard AJP-5 2019, 'Allied Joint Doctrine for the planning of operations', viewed 19 March 2022, <https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_144557/story_content/external_files/AJP-5_EDA_V2_E.pdf />.

NATO Standard AJP-2.7 2019, 'Allied Joint Doctrine for the joint intelligence, surveillance and reconnaissance', viewed 19 March 2022, <https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_152845/Linear/JISR04222102/sharedFiles/AJP27.pdf>.

NATO - AAP-06 2021, 'STANAG 3680 - NATO glossary of terms and definitions (English and French) - AAP-6', viewed 19 March 2022, <https://standards.globalspec.com/std/14486494/aap-06>.

MISP Threat Sharing, viewed 12 May 2022, <https://www.misp-project.org/download/ />.

MITRE ATT&CK 2017, 'Sandworm Team', viewed 11 June 2022, <https://attack.mitre.org/groups/G0034/>.

O'Leary, M 2019, *Cyber Operations: Building, Defending, and Attacking Modern Computer Networks*, APRESS, Towson, MD, US.

Weiskopff, M 2017, 'Effects-based operations in the cyber domain`, viewed 23 May 2022, <https://apps.dtic.mil/sti/citations/AD1033006 >.