NATO STANDARD

AJP-3.20

ALLIED JOINT DOCTRINE
FOR CYBERSPACE OPERATIONS

Edition A Version 1

JANUARY 2020

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED JOINT PUBLICATION

Intentionally blank

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

29 January 2020

1.   The enclosed Allied joint publication AJP-3.20, Edition A, Version 1, ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS, which has been approved by the nations in the Military Committee Joint Standardization Board, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 6514.

2.   AJP-3.20, Edition A, Version 1, is effective upon receipt.

3.   This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database ((https://nso.nato.int/nso/) or through your national standardization authorities.

4.   This publication shall be handled in accordance with C-M(2002)60.

Zoltán GULYÁS
Brigadier General, HUNAF
Director, NATO Standardization Office

Intentionally blank

RESERVED FOR NATIONAL LETTER OF PROMULGATION

Intentionally blank

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

Intentionally blank

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
GBR	The AJP refers to cyberspace operations as being, dependent on the context, potential violations of international law as a breach of sovereignty. Whilst sovereignty is fundamental to the international rules-based system, the UK government does not consider that the current state of international law allows for a specific rule or additional prohibition for cyberspace operations beyond that of a prohibited intervention.
USA	Reservation 1. The United States recommends removal of glossary/lexicon terms and definitions that are not NATO Agreed, quoted verbatim from NATOTerm, correctly cited IAW AAP-47 Allied Joint Doctrine Development, correctly introduced or revised IAW AAP-77, NATO Terminology Manual, nor have terminology tracking forms submitted. This reservation will be lifted when the relevant NATO terms and definitions are corrected (see matrix for any specificity with terms).
	Reservation 2. The United States recommends using the term 'international law' in place of 'humanitarian law' (when expressed) as the term is misused per national understanding and compliance with the Geneva Conventions.
	Reservation 3. The United States expects that approved text will be harmonized with capstone and operations keystone AJPs otherwise United States personnel will use national joint doctrine to overcome variances.
	Reservation 4. The United States recommends removal of the text in paragraph 1.16, 1.38, 1.39, and 2.3 that mischaracterizes "effects" and "unintended effects" as "effects" are created to support achievement of objectives and the discussion of "unintended effects" should be consistent with national policy.
	Reservation 5. The United States recommends recognizing 5 domains: four physical (air, land, maritime, and space) and one within the information environment (cyberspace). This reservation will be lifted when the text is corrected to not conflict with this position.

Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.

Intentionally blank

Table of contents

Lexicon

Related documents

SH/CCD/J6/CD/OPP/50/15 – 308810, 7 Apr 2015	*SACEUR'S Direction and Guidance on Cyber Defence*
AC/237-D(2017)0001, 8 Jun 2017	*NATO Crisis Response System Manual 2017*
C-M(2008)0029-COR1, 2 Apr 2008	*Proposals on a way ahead on Comprehensive Approach*
C-M(2011)0022, 14 Mar 2011	*Political Guidance*
MC 0064/11, 20 Aug 2018	*NATO Electronic Warfare Policy*
MC 0422/5, 11 Feb 2015	*NATO Military Policy for Information Operations*
MC 0560/2, 6 Sep 2017	*MC Policy for Military Engineering*
MC 0571/1, 30 Sep 2015	*MC Policy for Cyber Defence*
MC 0586/1, 9 Aug 2012	*MC Policy for Allied Forces and their Use for Operations*
MC 0593/1, 12 Jul 2017	*The Minimum Level of Command and Control Service Capabilities in Support of Combined Joint NATO Led Operations*
MC 0628, 26 Jul 2017	*NATO Military Policy on Strategic Communications*
MC 0665, 12 Jun 2018	*Military Vision and Strategy on Cyberspace as a Domain of Operations*
MCM-0041-2010, 20 Jul 2010	*MC Position on the Use of Effects in Operations*
MCM-0077-2000, 17 May 2000	*MC Guidance on the Relationship between NATO Policy and Military Doctrine*
MCM-0112-2018, 31 May 2018	*Framework Mechanism for the Integration of Sovereign Cyber Effects Provided Voluntarily by Allies into Alliance Operations and Missions*
PO(2010)0143, 13 Oct 2010	*Comprehensive Approach Report*
PO(2010)0169, 19 Nov 2010	*The Alliance's Strategic Concept*
PO(2011)0045, 7 Mar 2011	*Updated List of Tasks for the Implementation of the Comprehensive Approach Action Plan and the*

Lisbon Summit Decisions on the Comprehensive Approach

PO(2011)0141, 11 Apr 2011   *Political Military Framework for Partner Involvement in NATO-Led Operations*

PO(2014)0358, 27 May 2014   *Enhanced NATO Policy on Cyber Defence*

PO(2017)0501, 30 Oct 2017   *Approval of the Principles to Support the Integration of Sovereign Cyber Effects Provided Voluntarily by Allies into Alliance Operations and Missions*

PO(2017)0564, 29 Nov 2017   *Review of the 2011 Comprehensive Approach Action Plan*

SG(2006)0244 Rev 1, 2 May 2006   *Force Declarations and Designations*

SG(2008)0806(INV), 29 Oct 2008   *NATO Lessons Learned Policy*

AAP-03   *Directive for the Production, Maintenance and Management of NATO Standardization Documents*

AAP-06   *NATO Glossary of Terms and Definitions*

AAP-15   *NATO Glossary of Abbreviations Used in NATO Documents and Publications*

AAP-47   *Allied Joint Doctrine Development*

AJP-01   *Allied Joint Doctrine*

AJP-2   *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*

AJP-2.4   *Allied Joint Doctrine for Signals Intelligence*

AJP-2.7   *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance*

AJP-3   *Allied Joint Doctrine for the Conduct of Operations*

AJP-3.5   *Allied Joint Doctrine for Special Operations*

AJP-3.6   *Allied Joint Doctrine for Electronic Warfare*

AJP-3.9   *Allied Joint Doctrine for Joint Targeting*

AJP-3.10	*Allied Joint Doctrine for Information Operations*
AJP-3.12	*Allied Joint Doctrine for Military Engineering*
AJP-3.14	*Allied Joint Doctrine for Force Protection*
AJP-3.19	*Allied Joint Doctrine for Civil-Military Cooperation*
AJP-3.21	*Allied Joint Doctrine for Military Police*
AJP-5	*Allied Joint Doctrine for the Planning of Operations*
AJP-6	*Allied Joint Doctrine for Communication and Information Systems*

Intentionally blank

Edition A Version 1

Preface

Scope

1.   Allied Joint Publication (AJP)-3.20, *Allied Joint Doctrine for Cyberspace Operations,* is the NATO doctrine to plan, execute and assess cyberspace operations (CO) in the context of Allied joint operations. AJP-3.20 is a part of NATO's operations architecture and derives its authority from and complements AJP-3, *Allied Joint Doctrine for the Conduct of Operations.*

Purpose

2.   AJP-3.20 focuses on the principles of joint CO. It does not restrict the authority of commanders; they will be expected to organise assigned forces and to plan and execute operations as appropriate. Subordinate NATO publications may be developed to provide detailed guidance on the application of these principles and their translation into practices and procedures.

Application

3.   AJP-3.20 is intended primarily as guidance for NATO commanders, staffs and forces. However, the doctrine provides guidance for a coalition of NATO member states, partners, non-NATO nations and other organisations. It also provides a reference for NATO civilian and non-NATO civilian actors.

Legal

4.   The conduct of Alliance operations and missions is governed by international law and the domestic law of the participating nations. Within this framework, NATO sets out the parameters within which its military forces can operate, as set out in AJP-01, *Allied Joint Doctrine.* Legal considerations play a key role in the decision-making process and during an operation. This is particularly important at the operational level where campaigns are designed and directed. International law provides prescriptions and limitations for forces and individuals.

Intentionally blank

Chapter 1 – Introducing cyberspace operations

Section 1 – Introduction

Background

1.1.   The Alliance finds itself operating in increasingly interconnected environments, in particular, cyberspace and the information environment (IE). The free flow of data and seamless functioning of networks have become critical for functions and services for civil society and for military forces. State and non-state actors seek to exploit vulnerabilities in military and non-military information systems to exfiltrate, corrupt or destroy data or to gain prestige, political or military advantage or profit. Digital networks and systems, therefore, need to be safeguarded against information denial by disruption, degradation or destruction, and manipulation and exfiltration. In an interconnected world where military success may depend as much on the ability to control one's narrative as the ability to create physical effects, freedom of action in cyberspace may be as important as control over land, air and space, or sea.

1.2.   Cyberspace is far more than merely the Internet. All devices reachable via cyberspace could be potential targets and potential threats. This includes networks and devices connected by wired connections, wireless connections and those that appear to be not connected at all. Adding to this ever growing domain is the use of such technology in the expanding number of domestic goods, also known as the internet of things (IoT).

1.3.   The IE comprises the information itself, the individuals, organisations and systems that receive, process and convey the information, as well as the cognitive, virtual and physical space in which this occurs. This environment has seen significant changes in recent years. The importance of worldwide distributed information, the speed at which information is communicated, the role of social media and the reliability of information systems have created a situation in which no Alliance decision or action can be taken without considering its potential impact on the IE, or the IE's influence on the decision. The ubiquitous nature of information and the potential strategic ramifications of tactical actions add to the challenge faced by commanders. In this new IE it is more difficult to distinguish between the strategic, operational and tactical levels. The coordination, synchronisation and execution of information activities that deliberately create effects in the IE is essential to the Alliance's successful functioning in peace, crisis and conflict.

1.4.   It is essential to understand that a nation's vulnerability in cyberspace is related to its dependence upon cyberspace. Cyberspace provides options for friendly, neutral and opposing forces. The Alliance, therefore, needs to be able to counter opposing actors and support operations as capabilities continue to develop and become more advanced.

1.5.   Freedom of action in cyberspace also affects the armed forces. Effective operations depend on many networks, including, critical national infrastructure, industrial control systems, weapon systems, command and control (C2) systems and logistics systems. In

order to assure confidentiality, integrity and availability (CIA) of information, as well as user/entity authentication and non-repudiation, communication and information systems (CIS), including networks and data repositories, must be highly resilient to threats from cyberspace both in peacetime and during armed conflict.

1.6.   Although today's dependency on cyberspace brings associated risks,[1] it provides military opportunities as well. An adversary may similarly rely on parts of cyberspace, such as computers, computerised networks, mobile devices and the electromagnetic environment and, therefore, may exhibit similar vulnerabilities.

1.7.   NATO mission networks will likely take the form of federated systems.[2] All members in the federated system should ensure compliance to established security standards as the system security is only as good as its weakest link.

Cyberspace described

1.8.   Cyberspace is not limited to, but at its core consists of, a computerised environment, artificially constructed and constantly under development. Cyberspace infrastructure is largely globally interconnected; however, geographic boundaries do apply in the context of jurisdiction, with national responsibilities. This is why the assignment of classical operational boundaries in cyberspace is particularly difficult. Cyberspace is not only in constant flux but even more importantly, it may be used by anyone for almost any purpose. Cyberspace is also distinct in that its underlying physical elements are entirely man-made, which is different from land, air and space, and sea. Risks in cyberspace may be managed through manipulation of the domain itself.

---

[1] Risks include the unavailability of NATO CIS or reduced usability of capabilities in all operational domains due to restrictions with regard to confidentiality, integrity and availability.
[2] Federated system is a network of independent networks sharing and exchanging resources and information to support C2 and decision making.

The three-layer model

3. Cyber-persona layer

2. Logical layer

1. Physical layer

Figure 1.1 – The three layers of cyberspace

1.9. Cyberspace can be described in terms of three layers: physical, logical and cyber-persona, as shown in Figure 1.1. Conduct of cyberspace operations (COs) always includes the logical layer, but may also include activities or elements from the other two layers. The desired effects of COs may exist on all layers or ultimately outside of cyberspace. COs may affect human sense and decision-making and may be used or misused to influence behaviour. Likewise, COs may also affect physical entities outside the three layers of cyberspace. Activities outside of cyberspace which have an effect on cyberspace, are not considered COs, e.g. dropping a bomb on CIS.

1.10. Entities at the physical layer, e.g. hardware components, are bound to a geographical location. The tangible components in this layer include computers, servers, routers, hubs, switches, wiring and other equipment crucial to data storage, data processing and data transmission. It also includes the integrated information and communications technology components of other equipment or systems like digital sensors, weapons systems, C2 systems and critical infrastructure. Although the logical layer and the cyber-persona layer have no actual borders, state borders are relevant in legal terms relating to the geographical position of hardware components.

1.11. 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.

1.12. The cyber-persona layer does not consist of real persons or organisations but a representation of their virtual identity. A virtual identity could be an email address, user-identification, a social media account or an alias. Consequently, one person or one organisation can have multiple cyber-personas. Conversely, multiple people or organisations could also create just a single, shared cyber-persona.

Terms and definitions

1.13. For the purposes of this publication, the following definitions are new terms being processed for NATO agreed status via terminology tracking files (TTFs).

---

cyberspace
The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data.

cyberspace operation (CO)
Actions in or through cyberspace intended to preserve friendly freedom of action in cyberspace and/or to create effects to achieve commanders' objectives.

defensive cyberspace operation (DCO)
Defensive actions in or through cyberspace to preserve friendly freedom of action in cyberspace.

offensive cyberspace operation (OCO)
Actions in or through cyberspace that project power to create effects which achieve military objectives.

cyber security (CS)
The application of security measures for the protection of communication, information, and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.

mission assurance (MA)
A process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of NATO mission-essential functions in any operating environment or condition.

The military context

1.14. Due to various societal and technological changes, NATO's traditional operating environments have been enriched with an evolving domain: cyberspace. The operating environment in which armed forces deploy their assets can thus be divided into four domains,[3] maritime, air and space, land and cyberspace. Each domain has specific characteristics which help determine the way effects are created and operations conducted.

1.15. Recognising cyberspace as a domain of operations necessitates an operational shift to a focus on MA. Information assurance emphasises the security and defensive posture related to the protection of information and systems, while MA includes the operational impact of activities in or through cyberspace. Furthermore, recognising cyberspace as a domain may suggest an ambition to undertake strategic and operational coordination and deconfliction of effects within cyberspace and all other domains in the context of overall NATO planning of operations.

1.16. It is important to address the relationship between creating effects in the IE by COs and by other means. Whatever the channel or the capabilities committed to achieve effects within the IE, they have to be synchronised in order to maximise efficiency and avoid fratricide. COs apply capabilities in cyberspace to create effects which support operations across the physical domains and cyberspace. While some COs may support information operations, other COs will be conducted in support of operations in the physical domains to achieve objectives. Information operations are more specifically concerned with the integrated employment of information-related capabilities during military operations, in concert with the lines of operation, to influence, disrupt, corrupt or usurp the decision-making of adversaries while protecting our own. Thus, cyberspace is a medium through which some information-related capabilities and techniques, such as psychological operations or deception, may be employed. However, information activities/information operations may also use capabilities from the physical domains to achieve its objectives. COs, including Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA),[4] are integrated within joint operations requiring coordination and implementation with established military processes.

---

[3] NATO has only declared cyberspace as a domain with maritime, land and air and space being declared environments. For the purpose of consistency in this document maritime, land, air and space and cyberspace will be referred to as domains. AJP-3, *Allied Joint Doctrine for the Conduct of Operations.*

[4] Enclosure 1 to MCM-0112-2018, *Framework mechanism for the integration of Sovereign Cyber Effects Provided Voluntarily by Allies into Alliance operations and missions* and PO(2017)0501, *Approval of the Principles to Support the Integration of Sovereign Cyber Effects Provided Voluntarily by Allies into Alliance operations and missions*.

Threat actors

1.17.   Alliance activities in or through cyberspace are exposed to a wide range of threats just as in traditional domains. However, due to the interconnected and ubiquitous nature of cyberspace, low-cost capabilities can result in disproportionate effects against a technology-dependent alliance or nation. Attribution is difficult given various methods and techniques available to disguise activities in or through cyberspace. This provides actors who could not otherwise effectively oppose NATO with an asymmetric alternative. Adversaries may see these technology options as much cheaper alternatives to procuring traditional weapons to pose a significant threat to the security of NATO and member states.

1.18.   **State actors**. Adversaries may pose a significant threat to Alliance operations and missions (AOM) with activities such as terrorism, espionage, subversion, sabotage, organised crime or other malicious activities. For example, the relatively safe and global reach of espionage actions via cyberspace implies that many states have rapidly deployed such capabilities to operate in and intercept data sent through cyberspace. The targets vary from government departments and the defence industry to businesses in the top tier sectors. Various states are developing the ability to carry out defensive and offensive cyberspace operations and have included military actions in cyberspace in their military doctrines. They could deploy COs against adversaries to compete below the level of armed conflict or during open hostilities. Although there are still very few precedents on an international scale in the conduct of attacks in or through cyberspace, their potential impact could be significant.

1.19.   **Non-state actors**. In principle, non-state actors operate for themselves and not for states. Nevertheless, a proxy may work for a state when that state lacks the required skills, knowledge and means to operate in cyberspace. Another reason for states to use proxy actors could be related to political unwillingness to openly employ state personnel, or in cases when state COs do not match with legal, ethical or cultural norms. Actions by proxy could provide these states with plausible deniability, whilst not exposing state-owned technical capability. Activities in or through cyberspace by a non-state actor are still attributable to a state if the state factually exercises effective control over that specific conduct of the non-state actor. In addition to the proxy actors, various other non-state actors can be identified, such as hacktivists and terrorists.

1.20.   **Criminals**. Criminals have moved into cyberspace to take advantage of its connectivity and anonymity. Criminal activity may impact military operations, but generally remains the jurisdiction of the national law enforcement bodies through established law.[5]

1.21.   **Insiders**. Disgruntled personnel may seek to deliberately exploit cyberspace to cause harm to the Alliance. Additionally, all personnel, regardless of their role or seniority, are on the front line in cyberspace and can give an opening to military systems by ignoring or circumventing cyber security (CS).

---

[5] See AJP-3.21, *Allied Joint Doctrine for Military Police* for further details.

Threat types

1.22. Threats in cyberspace can be classified according to their origin, type and technique.

  a. Threats can be characterised by their origin, e.g.:

   • adversary actions;

   • accidents;

   • nature;

   • negligence or incompetence.

  b. Threats can be characterised by their type, e.g.:

   • physical, like fire, flooding, loss of power;

   • technical failures of equipment;

   • compromise of functions stemming from errors, abuses, subversion.

  c. Specific techniques of malicious activity vary over time based on changes in technology, but common techniques include:

   • denial-of-service;

   • deception of authorised users into taking actions that compromise security;

   • unauthorised access and then escalate privileges to enable further actions;[6]

   • installation of malware for ongoing system exploitation.

Section 2 – The joint functions

1.23. As defined in AJP-3, *Allied Joint Doctrine for the Conduct of Operations*, joint functions provide a framework to help integrate and synchronise capabilities and activities in joint operations. COs may support other operations or achieve operational objectives by itself. Effects by COs are synchronised with other effects and capabilities of the overall operation to create synergy.

---

[6] Escalate privileges means to gain elevated access to resources that are normally protected from an application or user.

1.24. In addition to traditional targets, COs add potential opportunities to the range of targets, for example adversaries' cyber-persona and entities in the logical layer such as operating systems, firmware, applications, (other) software, protocols or data. By altering these aspects in cyberspace, it is possible to influence the adversary's combat effectiveness.

1.25. In order to describe COs in the context of each joint function and to allow a clearer understanding, COs are highlighted from the perspectives of being supporting operations and supported operations.

Manoeuvre

1.26. Manoeuvre is the employment of forces on the battlefield through movement in combination with fire, or fire potential, to achieve a position of advantage in respect to the enemy in order to accomplish the mission. COs provide an additional manoeuvre element in or through cyberspace next to the traditional land, maritime or air manoeuvre elements. It extends the commander's means and assets for creating effects and can be actively conducted to attack the adversary. COs might give the commander the opportunity to achieve partial objectives of an operation by creating the prerequisites for operational success, without physically deploying forces, or provide important information via exploitation. However, if an isolated area of cyberspace is targeted, other manoeuvre elements may need to support the COs, for example, to get access to a certain physical object or device.

1.27. Another component of manoeuvre in cyberspace is the ability to move data to a place where it has maximum military utility, including movement of data out of harm's way and into a secure location. Having access to secure digital voice and data communications is similar to maintaining physical lines of communication.

Fires

1.28. COs can be used as an asset to extend the variety of a commander's options with a wide spectrum of psychological, logical or even physical effects. This variety of possible effects, the complex architecture of CIS and the interconnection throughout all layers can make it more difficult to do a collateral damage estimate. Additionally, fires in the physical domains can also support COs if the overall success of a CO relies on prerequisites that can only be created by physical measures rather than by virtual ones. Depending upon the commander's objective, fires in cyberspace can be offensive or defensive, supporting or supported. Like all forms of fires, fires in or through cyberspace should be included in the joint planning process to facilitate synchronisation, unity of effort and overall co-ordination through the joint targeting process.

1.29. As COs partially rely on the use of the electromagnetic environment, COs must be coordinated with electromagnetic operations, including electronic warfare. As a minimum,

coordination must be achieved through a common participation in the relevant processes. Coordinating COs may also require inputs to the Joint Restricted Frequency List.[7]

Command and control

1.30. An effective C2 structure is a necessary element to plan, synchronise and conduct effective COs. COs may have effects throughout all military domains. The use of COs to hamper the adversary's abilities should only be permitted after assessing the risk of undesired consequences. This includes identifying Alliance C2 vulnerabilities and mechanisms to provide protection. This requires continuous and effective risk management.

Intelligence

1.31. Intelligence is defined as the product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision-makers.[8] Cyberspace is fundamental to the availability and sharing of information and plays a major role, especially in contributing to the intelligence collection disciplines, within a joint mission. COs should be aligned with NATO intelligence doctrine for requesting information and prioritising the commander's intelligence requirements as they apply in cyberspace.

Information

1.32. The information function helps commanders and staff using information, while integrating with other functions, to influence relevant actor perceptions, behaviour, action or inaction and decision making. Key enablers are Strategic Communications (STRATCOM), Information Operations, Psychological Operations and Military Public Affairs. These key enablers should be integrated at the start of the planning process, support on-going military operations and be consistent with the overall information strategy and desired end state. Coordination is also required to ensure that other activities by the joint force do not undermine activities in the IE and vice versa. COs are an integral part of the information function and may support information activities by providing both a vector for deploying information and effects that influence targeted audiences. The interdependence between COs and other means of using information as an instrument of power demands a close coordination of activity.

---

[7] See AJP-3.6, *Allied Joint Doctrine for Electronic Warfare*.
[8] NATOTerm.

Sustainment

1.33. Military engineering,[9] logistics and medical and health support provide vital elements of sustainment. These areas are dependent on cyberspace with their reliance on computerised networks, for example, to:

- share information;
- order material and medication;
- process databases; or
- have a logistical overview.

To ensure the unobstructed access to these systems and maintain the ability to perform these processes, COs can provide functionality and security for sustainment of networks. In addition, sustainment of entities within cyberspace is required to preserve operational effectiveness.

Force protection

1.34. Force protection (FP) is designed to minimise vulnerabilities of personnel, facilities, operations and activities from threats and hazards in order to preserve freedom of movement and operational effectiveness, thereby contributing to mission success.[10] To increase security and improve FP, Commanders should ensure personnel understand their role in ensuing CS. In addition COs may support FP by gathering additional information in or through cyberspace about an adversary's abilities or intent against friendly forces. And, by supporting effective CS, COs can defend own assets and thereby decrease the vulnerability of own activities or operations against adversary threats in cyberspace. In case of an attack, resilience and good execution of contingency plans can help to maintain or regain own force momentum and freedom of action in or through cyberspace.

Civil-military cooperation

1.35. Civil-military cooperation (CIMIC) as a joint function allows the commander to support the comprehensive approach to operations. Cyberspace allows commanders to establish information links with civilian counterparts and other civilian audiences. In addition, COs support to civil authorities or other non-military actors can improve their CS. Therefore, enhancing information sharing and mutual assistance in preventing, mitigating and recovering from attacks in or through cyberspace is important. This requires civil-military interaction, which can be facilitated by CIMIC. A positive result from CIMIC is enhanced support to COs through maintaining freedom of access to cyberspace and capacity building.

---

[9] AJP-3.12, *Allied Joint Doctrine for Military Engineering.*
[10] NATOTerm.

Section 3 – Roles and responsibilities

1.36.   The roles and responsibilities with regard to NATO CIS are detailed in AJP-6, *Allied Joint Doctrine for Communication and Information Systems*. Additional roles and responsibilities for conducting COs fall to the Cyberspace Operations Centre (CyOC).

1.37.   The centralisation of the CyOC recognises the unique characteristic of reach (see para 2.2), especially the ability, from a single location, to achieve operational effects in multiple and geographically dispersed theatres.

1.38.   The CyOC serves as the primary point for coordination of NATO COs. The CyOC is tasked to:

- optimise the employment of effects in or through cyberspace;

- provide cyberspace and CO expertise to SACEUR, NATO Command Structure and NATO Force Structure HQs;

- provide timely and effective advice on the planning and conduct of COs, based on the recognised cyberspace picture (see para 3.17) and wider consolidated situational awareness;

- facilitate the integration of SCEPVA into AOM.

1.39.   Any form of command or control over forces providing SCEPVA remains with the contributing nation. The integration of these effects, utilising well established processes, is further detailed in the framework mechanism for the integration of SCEPVA into AOM.[11]

---

[11] Enclosure 1 to MCM-0112-2018, *Framework Mechanism for the Integration of Sovereign Cyber Effects Provided Voluntarily by Allies into Alliance Operations and Missions.*

Intentionally blank

Chapter 2 – Fundamental characteristics of cyberspace operations

Section 1 – Characteristics

2.1. Cyberspace is different from the other domains because it is man-made, partly non-physical and may not conform to geographical boundaries. Cyberspace operations (COs) impact many environments, such as the electromagnetic and information environments. Cyberspace exists by virtue of physical components on land, at sea, in the air and in space. Conversely, operations in the physical domains function effectively by virtue of cyberspace. Consequently, the four domains are dynamically interlinked; a change in one domain may have implications for the situation in the other domains.

2.2. **Reach**. Although the cyberspace domain comprises physical entities in the other domains, for example computers, networks or servers, the reach of effects in or through cyberspace are largely unaffected by the boundaries and limitations that generally apply to other domains. Since cyberspace has pervasive global reach and connectedness, actors in cyberspace can create effects in other parts of the world almost instantaneously. The pervasive and borderless nature of COs significantly increases the possibilities to select targets. Due to the inherent interconnectivity of cyberspace, when affecting just one item, whether that is one webpage, one router or one device, the effect can cascade, enabling effects to be created at multiple points on a global scale. This can be both intended and unintended. The area of operations in cyberspace is, therefore, not limited to the usual geographical area of operations as in the other domains; it is limited by the (non-)connectivity.

2.3. **Asymmetric effect**. Cyberspace may offer easy, economical and global access. An individual, or relatively small organisation with the appropriate motivation, resourcing and technical capability could conduct an attack in or through cyberspace with strategic and/or large-scale effects, disproportionate to the size and relative strength of the adversary. As adversaries are also likely to benefit from the unique possibilities cyberspace offers, there is an increased risk of homeland attacks in response to military activities in theatre. Activities in or through cyberspace are initially directed against digital systems, networks or devices, although the effects may be created in any of the three layers of cyberspace (see Figure 1.1).

2.4. **Anonymity**. Thorough understanding and situational awareness of cyberspace is essential. The virtual identities in the cyber-persona layer often allow actors to remain anonymous and to mask their intent, enabling others to act on their behalf. In addition, anonymity enables deception. The cyberspace domain is dynamic and constantly evolving. COs may be difficult to trace and, despite technological developments, many incidents are likely to be deniable and some untraceable. The attribution of activities in or through cyberspace is essential, but does not solely depend on digital information. A combination of multi-source intelligence, regular forensics and other methods all contribute to reveal an actor's identity. Non-attributable attacks increase uncertainty and misperception, and thus

lead to a perceived reduced political risk and a reduced opportunity for response. The possibility of COs conducted by proxy, or under false flags, must therefore be taken into account.

2.5.   **Time and speed.** Capabilities used in cyberspace range from relatively simple technological means that can be developed rapidly, to sophisticated instruments requiring a long development period. Such capabilities can exert tactical effects or achieve strategic impacts and all possible variations in between. The complexity and level of technology mainly depends on the effects to be achieved, and the hardening and complexity of the targeted system. Three time and speed related aspects should, therefore, be considered:

> a.   Within milliseconds, actions in or through cyberspace in one country can have distant digital effects in multiple other countries, but any effects in the physical world would follow later.

> b.   The preparation time will be longer where target complexity, intelligence gathering, specific effects, collateral damage, access and/or anonymity are important. Consequently, the period between the decision to create an effect and preparation and delivery of the payload could be significantly longer than when using traditional weapons. Equally, the time could be short where these considerations are of no concern.

> c.   The effects of the payload can be instant, or purposely delayed.

2.6.   **Versatility and reusability.** Effects in or through cyberspace can be designed to be temporary and reversible, as well as irreversible. This decision may be taken even after deployment if designed appropriately. The reusability of the means to create an effect in or through cyberspace may be an advantage in certain situations, but may increase the risk of loss of anonymity, capture, subsequent exploitation and re-engineering by the adversary, ultimately turning the means against other targets or its originator.

Section 2 – Principles of cyberspace operations

2.7.   When conducting joint operations, commanders prepare to face a variety of threats. Consequently, commanders require sufficient freedom of action in cyberspace to enable mission assurance (MA) to achieve their objectives. To that end, the risks associated with operations in or through cyberspace must be managed. Commanders should develop effective measures for COs, develop communication back-up plans and ensure confidentiality, integrity and availability (CIA) of information and CIS.

2.8.   Adversaries may have various objectives at different levels regarding NATO networks and systems. Adversarial COs may be directly aimed at reducing NATO's military capabilities, either specific capabilities in cyberspace or other capabilities depending on cyberspace.

However, adversaries' COs may also be conducted indirectly, in support of other operations. Therefore, situational awareness in cyberspace is essential to make proper threat and risk assessments.

2.9.   Due to the characteristics of cyberspace, the effects of COs may seem intangible to those not directly involved. This may make the military value of specific effects in cyberspace more difficult to quantify.

2.10.   COs recognise the same considerations and experience similar challenges as other joint capabilities and functions. In general, the principles of joint operations[12] are also applicable to COs; however, the interpretation of these principles may be different due to the nature of this domain. Traditional military land, maritime and air forces are limited by laws of nature. Cyberspace also has natural laws but of a different type e.g., notions of time and reach have other implications in this domain.

2.11.   **Security**. Security is essential to freedom of action in cyberspace, by limiting vulnerability to hostile activities and threats through appropriate measures. Cyber security (CS) goes beyond dealing with malicious activities directed at NATO systems and networks. It also involves protection against inherent internal system failures and disruptions not caused by external influences, but which could have a similar disruptive impact. Unwanted disclosure of known adversaries' vulnerabilities, their exploitation, methods, techniques and available capabilities may compromise the effectiveness of future COs.

2.12.   **Surprise**. On the basis of its inherent characteristics of time and speed, reach and anonymity, COs can often take advantage of the element of surprise. The effects of COs can be difficult to foresee, detect and trace, therefore, warning times may be significantly reduced or non-existent. In addition, COs can enable deception, which can contribute to surprise. COs can, therefore, run at a tempo and campaign phase that differs from other military activities, including shaping and information activities. Effects of COs can appear at a time, place and in a manner for which the targeted party is unprepared and achieve results greater than the effort expended.

2.13.   **Concentration of force.** Based on the unique characteristics of COs, especially reach, as well as time and speed, military effects could be created simultaneously at different locations. This expands the traditional concept of concentration of force to encompass mutually supporting, simultaneous effects in different locations.

2.14.   **Maintenance of morale.** COs can be used to manipulate systems or information. This may result in diminished trust in NATO CIS and NATO leadership. This can also impact the force through manipulation or denial of the Internet, including social media.

---

[12] The principles as defined in AJP-1, *Allied Joint Doctrine* – unity of effort, concentration of force, economy of effort, freedom of action, definition of objectives, flexibility, initiative, offensive spirit, surprise, security, simplicity and maintenance of morale.

2.15. **Freedom of action.** Maintaining freedom of action in cyberspace benefits military, government and civilian organisations. Freedom of action in cyberspace has a direct impact on all military operations, but particularly on COs, information operations, intelligence, deception and strategic communications.

Section 3 – Types of cyberspace operations

2.16. Well-defined and well-executed COs are paramount to the combat efficiency of the force.

2.17. In general, COs are conducted through two types of operations depending on commander's intent and objectives. It is important to note that these types of COs may be executed both by Allies and adversaries:

- defensive cyberspace operations (DCOs); and

- offensive cyberspace operations (OCOs).[13]

2.18. As part of Alliance operations and missions (AOM), NATO may seek to create effects in or through cyberspace beyond NATO CIS and the networks or systems for which NATO has been granted authorised access. This will be resolved through the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) mechanism, irrespective of whether the intent is defensive or offensive.

Defensive cyberspace operations

2.19. Commanders should be aware of adversaries' capabilities to launch COs against own forces and, therefore, plan to respond to them as appropriate.

2.20. DCOs consist of measures to preserve the ability to use cyberspace with the purpose of enabling own freedom of action and force protection. This may include vulnerability assessment and risk management as well as considering possible responsive measures in line with operational needs.

2.21. DCOs are generally aimed at preventing and/or terminating and mitigating ongoing malicious activities in cyberspace and recovering from their effects, thus preserving mission assurance (MA). DCOs protect networks and systems, and the information therein, for which NATO has been granted authorised access. The commander should understand the scope of DCOs being conducted to comprehend the potential impact on AOM. Adversary COs may

---

[13] This recognises that nations contributing to the Alliance can conduct OCOs which may contribute to the capabilities potentially available to the commander.

require actions in response, necessary to provide MA and achieve commander's objectives. The response may be in or through cyberspace, other domains or other means.

2.22.   DCOs can prompt SCEPVA that may generate a cyberspace coordination challenge for the commander.

Offensive cyberspace operations

2.23.   Any OCO will be conducted through the SCEPVA mechanism in accordance with the principles agreed to by NATO.[14]

2.24. OCOs may be executed as standalone operations or in conjunction with other operations. The commander should understand the scope of OCOs being conducted to comprehend the potential impact to AOM.

Section 4 – Effects created in or through cyberspace

2.25. COs can create various effects, either in cyberspace or in other domains and environments. COs, including the effects described in this section, can support the Alliance or be used against the Alliance by adversaries. Some of the effects described here are adapted from NATO Standardisation Agreement (STANAG) 2287 for use in this publication.

2.26. Adversaries' COs are likely to target infrastructure supporting NATO CIS or data therein, to such an extent that these are no longer confidential, reliable or available; either in reality or in perception. Although all adversaries' COs are inherently digital, i.e. effects in or through the logical layer,[15] they may use a variety of methods and techniques across all domains to gain unauthorised access, including physical proximity.

2.27. COs are always conducted at the logical layer,[16] encompassing direct effects to software, data and protocols. However, indirect effects may be aimed at the other layers of cyberspace, or at creating other higher-order effects in other domains.

2.28. Undesired effects are not unique to COs. However, the interconnectivity and interdependence of military, civil, private and/or corporate networks and systems increases the risk of undesired effects. This makes the assessment of potential cascading or collateral

---

[14] Enclosure 1 to MCM-0112-2018, *Framework mechanism for the integration of Sovereign Cyber Effects Provided Voluntarily by Allies into Alliance Operations and Missions*, and PO(2017)0501, *Approval of the Principles to Support the Integration of Sovereign Cyber Effects Provided Voluntarily by Allies into Alliance Operations and Missions.*

[15] See para 1.8, Figure 1.1.

[16] See para 1.8, Figure 1.1.

effects – in the case of a CO – particularly important, and difficult. Commanders should understand these interdependencies and the potential impact on their own operations.

2.29.   It is noteworthy that, although effects may be created by COs, the response need not be mitigated or combated by activities in or through cyberspace.

2.30.   COs can have direct and indirect effects. These effects may include, but are not limited to, the following:

> a.   **Secure**. Prevent compromise of the CIA of designated parts of cyberspace and the data stored or processed therein by adversarial COs.[17]
>
> b.   **Isolate**. Block the line(s) of communication between adversary and their malicious code/activity within affected systems.
>
> c.   **Contain**. Stop malicious code/activity from further spreading.
>
> d.   **Neutralise**. Render malicious code/activity permanently incapable of further affecting the CIA of parts of systems.
>
> e.   **Recover**. Remove and mitigate the effects of malicious code/activity in affected systems in order to restore functionality.
>
> f.   **Manipulate**. To control, change, or compromise the integrity of adversary's information, systems and/or networks in a manner that supports the commander's objectives.
>
> g.   **Exfiltrate**. To gather, download, disclose or gain possession of information through unauthorised access.
>
> h.   **Degrade**. To deny access to, or operation of, an asset to a reduced level of its capacity and/or performance. A desired reduction level is normally specified.
>
> i.   **Disrupt**. To completely deny access to, or operation of, an asset for a period of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level selected is 100 percent for a period of time.
>
> j.   **Destroy**. To completely and irreparably deny access to, or operation of, an asset. The asset is affected to the maximum extent, both in terms of outage time and damage caused.

---

[17] See AJP-6, *Allied Joint Doctrine for Communication and Information Systems,* for NATO network and systems secure functions.

Chapter 3 – Planning and conduct

Section 1 – General

3.1.   All cyberspace operations (COs) are likely to be an integral part of Alliance operations and missions (AOM) and need to be considered from the early stages of planning. Due to the inherent sensitivities of some COs their planning may have to be compartmented. Planning for activities in or through cyberspace should identify areas where these activities could create effects or substitute other means that could create similar effects. Expertise in being able to identify, describe and develop possible effects and decisive conditions in cyberspace should be available to the commander, as well as the ability to identify risks involved with activities in or through cyberspace.

3.2.   The commander should, to the maximum extent possible, deconflict, synchronise, and coordinate activities in all domains to obtain the desired effects.

Section 2 – Legal considerations

3.3.   NATO Allies recognise that international law applies in cyberspace.[18] NATO COs must be conducted in accordance with international law, including the United Nations (UN) Charter, Law of Armed Conflict (LOAC)[19] and human rights law,[20] as applicable.[21] As a matter of principle, Allies contributing COs on behalf of the Alliance must conduct those COs consistent with applicable international law, as well as adhere to their own relevant national laws.

3.4.   The legal framework applicable to and the required authority to conduct COs depends on the nature and context of the activities, such as, but not limited to:

- a North Atlantic Council (NAC) approved operation plan and annexes to include rules of engagement (ROE)[22] for COs, as applicable;

- standing authority or policy;

- the expected effects of COs;

---

[18] Wales Summit Declaration, 5 September 2014.

[19] Also known by many Allies as International Humanitarian Law.

[20] Warsaw Summit Communique, 8-9 July 2016.

[21] Additionally see AJP-01, *Allied Joint Doctrine*, subsection on *Use of force in international law,* for details on the three basic criteria in international law (self defence, United Nations Security Council mandate, or invitation by host-nation state), under which NATO can act as an international political and military cooperation organisation; all of which apply in the cyberspace domain as they do in the other operational domains.

[22] See AJP-01, *Allied Joint Doctrine* for details on ROE.

- whether the COs are conducted during an armed conflict, in self-defence or AOM that fall below the threshold of an armed conflict;[23] and

- the type of CO, whether defensive or offensive.

3.5.   Before conducting COs, commanders, planners and operators must understand the relevant legal framework and authorities under which they are operating to comply with applicable laws, treaties and policies. It is essential to consult legal counsel familiar with COs during planning and execution of COs.

3.6.   **Effects of cyberspace operations.** COs may pose challenging legal questions because of the variety of effects that COs can create. While many of these effects will likely fall below the threshold of a use of force or an armed attack, some COs can create effects that may amount to the use of force under Article 2(4) of the UN Charter or an armed attack giving rise to the inherent right of individual or collective self-defence under Article 51 of the UN Charter.[24] For example, if COs cause effects that, if caused by traditional physical means, would be regarded as a use of force under Article 2(4) of the UN Charter or an armed attack under *jus ad bellum,*[25] then such COs could similarly be regarded as a use of force or armed attack.

3.7.   Criteria that could be considered in making this assessment include the scale and effects of the attack, which might take into account such factors as interference with critical infrastructure or functionality, severity and reversibility of effects, the immediacy of consequences, the directness between act and consequences, and the invasiveness of effects. COs that generally would not constitute a use of force or armed attack might involve effects that create only temporary disruptions or denials of service, or those intended merely for disseminating or gathering information.[26] However, if done to enable or facilitate a wider, concurrent (or an imminent threat of) conventional attack, COs which independently would not ordinarily constitute a use of force, like a temporary denial of service, could be considered an armed attack. As a result, the legality of the response depends entirely on the context and the effects of the respective COs.

---

[23] See AJP-01, *Allied Joint Doctrine,* for details on operation themes from warfighting, security or stability operations, peace support and peacetime military engagement.

[24] AJP-3.9, *Allied Joint Doctrine for Targeting,* refers to lethal and non-lethal capabilities 'that could be applied to generate the desired physical or psychological effects to achieve objectives'.

[25] The concept of *jus ad bellum* refers to the conditions under which states may resort to the use of armed force, including self-defence.

[26] Depending on the context, such COs may nevertheless constitute a violation of international law as a breach of sovereignty or other internationally wrongful act.

3.8.   **Cyberspace operations conducted during an armed conflict (*jus in bello*).**[27] As a general rule, any offensive cyberspace operation (OCO) during AOM will come through the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) mechanism and only in the context of a NAC approved operation or mission. Any deviation from the above-stated general rule would require the express approval of the NAC. For AOM, including COs, the conduct of target engagements must comply with agreed NATO doctrine.[28]

3.9.   Consistent with the recognition by NATO Allies that international law applies in cyberspace, the fundamental LOAC principles of military necessity, humanity, proportionality and distinction,[29] apply to COs. Additionally, targeting in COs conducted in support or furtherance of an AOM should adhere to the target validation process, as adopted in AJP-3.9, *Allied Joint Doctrine for Joint Targeting*.[30] This validation seeks to ensure compliance with the LOAC framework and ensures that targets meet the objectives and criteria outlined by the NAC-approved operation plan, targeting annexes and ROE, as applicable. Target validation further ensures continued compliance with the commander's objectives, guidance, intent and desired effects. CO targeting conducted for an AOM should be synchronised and deconflicted with other targeting activities through the relevant processes.[31]

3.10.   **Dual-use objects.** An attack is only lawful if directed at a military objective. Commanders must be mindful that, especially in cyberspace, some objects or entities may have both military and civilian uses, sometimes informally referred to as 'dual-use'. This may render these types of objects more difficult to identify as legitimate military objectives. Examples of dual-use objects may include airports, electrical systems or network infrastructure. Hence, if dual-use objects are to be targeted, careful analysis must be carried out to determine if they constitute a lawful military objective, i.e. if it has lost its protection as a civilian object or otherwise offers a definite military advantage.[32] Furthermore, even if a dual-use object constitutes a legitimate military objective, attack against it would be unlawful if the 'expected total incidental loss [civilian injury or death, or damage to civilian objects] would be excessive in relation to the direct anticipated military advantage'.[33]

3.11.   **Collateral damage estimation.** Assessing incidental injury or death to collateral objects when conducting a proportionality analysis can be more difficult in the context of CO as compared to more traditional physical means or methods.[34]

---

[27] *Jus in bello* regulates the conduct of parties engaged in an armed conflict.

[28] See AJP-3, *Allied Joint Doctrine for the Conduct of Operations,* subsection *Joint Targeting.*

[29] See AJP-3.9, *Allied Joint Doctrine for Joint Targeting,* for details on the application of LOAC principles.

[30] There will likely be a targeting process conducted concurrently at the national level.

[31] See AJP-3.9, *Allied Joint Doctrine for Joint Targeting,* and AJP-3.10*, Allied Joint Doctrine for Information Operations.*

[32] See AJP-3.9, *Allied Joint Doctrine for Joint Targeting,* for details on determining military objectives and the targeting of 'dual use' objects.

[33] See AJP-3.9, *Allied Joint Doctrine for Joint Targeting,* for details on the principle of proportionality.

[34] See AJP-3.9, *Allied Joint Doctrine for Joint Targeting,* for details on collateral damage considerations.

3.12.   **Discrimination (Principle of Distinction).** The expected effects of COs which cannot be directed at a specific military objective or whose effects cannot be controlled would be inherently indiscriminate and therefore unlawful under LOAC.

3.13.   **The Law of Neutrality.** It will be for individual states to interpret and apply the law of neutrality in delivery of SCEPVA in support of AOM.

3.14.   **Collective self-defence (*jus ad bellum*).** A state's inherent right of individual and collective self-defence is recognised by Article 51 of the UN Charter and is also recognised as constituting customary international law. An armed attack or imminent armed attack can trigger the right to exercise self-defence. Any response under self-defence (jus ad bellum) must be necessary and proportionate. As a result, nations have the right to exercise individual and collective self-defence if they determine that malicious activity in or through cyberspace constitutes an armed attack. But, a decision to invoke Article 5 of the North Atlantic Treaty would be taken by the NAC on a case-by-case basis and reported to the UN Security Council.[35]

3.15.   Attribution may pose a difficult factual and legal question in responding to COs. This is mainly because there is a high likelihood of deception and use of proxies to hide the origin of activity and/or to implicate innocent parties. It is, however, the responsibility of the state that is the object of the armed attack, as well as that of those states coming to its collective defence, to perform an independent assessment. Any collective defence response by NATO will be subject to the political decisions of the NAC.

3.16.   **Peacetime operations or other operations, missions/activities that fall below the threshold of an armed conflict.** As cited in AJP-01, *Allied Joint Doctrine*, NATO faces threats from state and non-state actors, including their use of malicious activities against the Alliance, which often remain below the threshold of an armed attack. The responses[36] may include Article 4 North Atlantic Treaty consultations and may require a broader approach, employing integrated capabilities some of which may be unconventional in nature.[37] Effects of COs used in AOM that fall below the threshold of an armed conflict would have to be addressed by the NAC and be considered against legitimacy and authority.

---

[35] Wales Summit Declaration 2014.

[36] It is an unsettled area of the law whether international organisations or other states may conduct countermeasures on behalf of an injured state for unlawful acts that occur below the threshold of an armed attack. Countermeasures – an internationally wrongful act committed by a state entitles the injured state to take proportionate countermeasures (otherwise unlawful acts but for qualification as a countermeasure).

[37] See AJP-01, *Allied Joint Doctrine,* for details on 21st Century threats.

Section 3 – Planning

Analysis of the operating environment

3.17.   Commanders continuously monitor their areas of interest to anticipate potential crises and allow them to assist the strategic level in understanding any situation. This also includes an analysis of cyberspace as part of the overall understanding of the operating environment, for instance the generation of a recognised cyberspace picture (RCP).[38] This allows continuous assessment of relevant parts of cyberspace to take place, involving coordination and information exchange with relevant staff branches, all of which should be conducting their own assessments.

Operations planning process

3.18.   Planning for COs should address how to effectively integrate capabilities and effects in cyberspace, counter an adversary's use of cyberspace, defend mission critical networks, operate in a degraded environment, efficiently use limited assets and consolidate operational requirements for capabilities and effects in cyberspace. COs planning follows the normal sequence of planning activities.[39]

3.19.   Cyberspace-specific assessments should be achieved in very close coordination with the broader information environment assessment at both the strategic and operational levels.

3.20.   **Initiation**. Planning staff develop and refine their analysis and assessment of the operational situation in cyberspace, including possible desired effects. On this basis, the commander will take the possibility of using SCEPVA into consideration when developing the commander's initial planning guidance.

3.21.   **Mission analysis.** Planning staff complete a number of different tasks covering both types of COs, including the following:

- identify relevant aspects of all layers of cyberspace in coordination with the Cyberspace Operations Centre (CyOC) and other branches and capabilities;[40]

- participate in identifying adversary and other actor's activities and capabilities in or through cyberspace;

---

[38] The RCP matches and integrates various views of cyberspace aspects, maps adversaries' cyberspace and is used in direct support of the planning and the execution of current and future operations. The RCP can support deconflicting activities in cyberspace, with other activities.

[39] AJP-5, *Allied Joint Doctrine for the Planning of Operations*.

[40] See para 1.8, Figure 1.1.

- consider deconfliction, synchronisation, and the impact of any constraints or restraints imposed by higher authority, such as the following;

  o mission-specific guidance on CO;

  o political, legal and ROE issues, with particular regards to international law, custom and practice, host nation;

  o agreements/arrangements, support by other nations and other sensitivities.

- identify if and how other military capabilities can support COs;

- conduct an initial CO risk assessment including reviewing operations security considerations and potential risks to friendly or neutral usage of cyberspace, including possible action outside the joint operations area against NATO, member nations, or neutral nations/entities;

- identify and develop potential desired and undesired effects in coordination with the Target Support Cell, J2 and the CyOC. Identified effects will be compiled in an effects list within an operation plan annex.

3.22. **Course of action development**. Using the outputs from the mission analysis, the planning staff assist in the course of action (COA) development to:

- recommend how COs may be executed to create or contribute to the desired effect for each COA;

- develop measures of effectiveness and their indicators for each COA;

- synchronise COs within each COA;

- validate effects included in the developed COAs with the CyOC; and

- continue to develop the CO element of the staff estimate, inputs for the COA decision brief and inputs for target folders.

3.23. **Course of action analysis.** The planning staff:

- assist in analysing each COA, taking COs into consideration;

- identify decision points for employing possible CO; and

- provide CO input into synchronisation matrices or other decision-making tools.

3.24. **Course of action validation and comparison.** The planning staff:

- assist in comparing each COA in relation to the desired effects created by COs; and

- assist in prioritising COAs from a CO perspective.

3.25. **Commander's course of action decision.** The planning staff provide the commander with a clear and concise recommendation of how COs best contribute to mission success in each of the COAs briefed, and which COA is preferred.

3.26. **Concept of operations and plan development.** The planning staff ensure that chosen COs are included in the plan.

Section 4 – Risk management

3.27. Risk management is a continuous process. The balance between creating an effect and the associated risk must be carefully considered. It demands a deliberate decision on how risks should be treated.[41]

3.28. Since cyberspace is a global domain, there is a risk of COs having an impact outside the joint operations area. COs can create undesired effects on our own forces and other entities, who are part of, or not part of, the mission. This risk, as with similar risks in other domains, is factored into the planning.

3.29. Differences in the reaction to COs and their effects can become a risk, as it can be difficult to assess how the affected parties perceive activity in or through cyberspace. The risk of escalation should be considered and managed.

Section 5 – Conduct

Preparation

3.30. **Pre-deployment training.** Planning and exercising the integration of COs should take place before deployment. Ideally, this involves all elements of the force.

3.31. **Preparing the joint operations area.** Shaping, securing and maintaining access to the joint operations area is a pre-condition for mission success and is coordinated with the commander. COs may support such activities. The commander works to understand and

---

[41] See AJP-01, *Allied Joint Doctrine*, AJP-3, *Allied Joint Doctrine for the Conduct of Operations,* and AJP-5, *Allied Joint Doctrine for the Planning of Operations,* for further information.

assess COs that are used to shape the environment, to ensure they are legally and operationally acceptable, and within policy constraints.

Execution

3.32. COs will be conducted according to the operation plan. As such, SCEPVA, when authorised, might give the commander alternative options to create effects. These options are integrated, coordinated and synchronised across force components to achieve objectives as efficiently as possible.

3.33. **Command and control.** The commander and staff should understand the command and control (C2) arrangements for COs. In many circumstances there might not be a direct C2 arrangement; however, the commander must understand and use the planning process to integrate COs in the campaign planning and execution.

3.34. **Operations management.** Integrating force elements is generally the most effective way to conduct operations, however, for SCEPVA it may not be feasible. Additionally, some COs may be conducted by forces not physically in theatre.

3.35. **Battlespace management and synchronisation.** Coordination and deconfliction are conducted through battlespace management at the joint forces level. COs are coordinated and deconflicted with other capabilities/functions. Synchronised forces may operate independently but towards a common goal. In such instances, COs may directly support or enable other force elements, but in any case should be complementary to them.

3.36. **Situational awareness.** NATO requires situational awareness of cyberspace. Situational awareness is a combination of a near real-time updated RCP, analysis and information management. Participating nations in a campaign are encouraged to contribute to NATO situational awareness of cyberspace.

3.37. **Battle rhythm.** The battle rhythm process is critical to the Joint Force Headquarters. Typical battle rhythm events which require input regarding COs may include:

- commander's briefs;
- Joint Operations Planning Group (JOPG);
- Cyber Defence Working Group (CDWG);
- Joint Collection Management Board (JCMB);
- Joint Targeting Coordination Board (JTCB);
- Joint Coordination Board (JCB);
- other coordination boards, such as the Information Activities Coordination Board (IACB).

3.38. **Assessment.** Assessment is integrated into all phases of the planning and execution processes. Measures of effectiveness and measures of performance need to be objective. The complexity and classification of COs can complicate their assessment.[42]

3.39. **Plan refinement.** Cyberspace changes and evolves continuously; this requires a thorough interaction across all staff branches. Staff responsible for activities in or through cyberspace must remain in constant interaction with the relevant command regarding SCEPVA to provide updates to plans.

Section 6 – Targeting

Contribution to target nomination

3.40. Like every other operation, COs are initially considered in the joint targeting process, to identify targeting options where COs could be conducted to create specific effects in support of the commander's mission objectives. During planning, and continuously as part of execution, target nominations are required to implement COs. These are initiated through the joint targeting process into the relevant working groups for development to be fed into relevant boards for inclusion on the joint prioritised target list (JPTL). The cyclic target development process during planning should include input for COs at all relevant levels. The commander has to take into account that certain types of COs can take significant time to plan, develop, authorise and execute.

3.41. AJP-3.9, *Allied Joint Doctrine for Joint Targeting*, provides guidance for integrating targeting into operations, and the fundamentals on how to integrate COs into the targeting process. Targeting using COs may well require specific national arrangements.

---

[42] Measures of performance and measures of effectiveness are defined in AJP-5, *Allied Joint Doctrine for the Planning of Operations*.

Intentionally blank

Lexicon

Part 1 – Acronyms and abbreviations

AAP	Allied administrative publication
AJP	Allied joint publication
AOM	Alliance operations and missions
C2	command and control
CDWG	Cyber Defence Working Group
CIA	confidentiality, integrity and availability
CIMIC	civil-military cooperation
CIS	communication and information systems
CO	cyberspace operation
COA	course of action
CS	cyber security
CyOC	Cyberspace Operations Centre
DCO	defensive cyberspace operation
FP	force protection
IACB	Information Activities Coordination Board
IE	information environment
JCB	Joint Coordination Board
JCMB	Joint Collection Management Board
JOPG	Joint Operations Planning Group
JTCB	Joint Targeting Coordination Board
LOAC	Law of Armed Conflict
MA	mission assurance
MC	Military Committee
MCM	Military Committee memorandum
NAC	North Atlantic Council
OCO	offensive cyberspace operation
RCP	recognised cyberspace picture
ROE	rules of engagement

SACEUR   Supreme Allied Commander Europe

SCEPVA   Sovereign Cyber Effects Provided Voluntarily by Allies

STANAG   NATO Standardisation Agreement

TTF   terminology tracking file

UN   United Nations

Part 2 – Terms and definitions

cyberspace

The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data.[43]

cyberspace operation

Actions in or through cyberspace intended to preserve friendly freedom of action in cyberspace and/or to create effects to achieve commanders' objectives.[44]

cyber security

The application of security measures for the protection of communication, information, and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.[45]

defensive cyberspace operation

Defensive actions in or through cyberspace to preserve friendly freedom of action in cyberspace.[46]

mission assurance

A process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information

---

[43] TTF 2015-0029
[44] TTF 2014-0268
[45] TTF 2018-0247
[46] TTF 2014-0269

systems, infrastructure, and supply chains, critical to the execution of NATO mission-essential functions in any operating environment or condition.[47]

offensive cyberspace operation

Actions in or through cyberspace that project power to create effects which achieve military objectives.[48]

---

[47] TTF 2018-0089
[48] TTF 2014-0270

AJP-3.20(A)(1)