



Joint Doctrine for Military Cyberspace Operations

1st edition, A (English)

September 2019



**ROYAL DANISH
DEFENCE COLLEGE**

Copenhagen September 2019
Royal Danish Defence College
Svanemøllens Kaserne
DK-2100 Copenhagen
Tlf.: +45 728 17000
Layout: RDDC
ISBN: 978-87-7147-264-6

Table of Contents

1.	Introduction	3
1.1.	Objective	3
1.2.	Application	3
1.3.	Scope.....	3
1.4.	Background.....	4
1.5.	Who Conducts CO?	4
1.6.	Protection of Own Cyberspace.....	5
1.7.	Structure of the Doctrine.....	5
Part I: Cyberspace	7
2.	Defining Cyberspace.....	7
3.	Cyberspace as an Operational Environment	9
3.1.	Elements in the Cyberspace Operational Environment	9
3.1.1.	Physical Size and Physical Conditions	10
3.1.2.	EMS	11
3.1.3.	Information Environment	11
3.1.4.	Own and Allied Forces and Operations.....	12
3.1.5.	Hostile Actors	14
3.1.6.	Neutral Actors	15
3.1.7.	Influence from Other Operational Environments	16
3.2.	Errors and System Breakdowns.....	16
Part II: Principles for CO	18
4.	CO	18
4.1.	Roles and Responsibilities.....	19
4.1.1.	Role of the Tactical Level in CO	19
5.	Commander's Considerations	22
5.1.	Effects in cyberspace	23
5.2.	Joint Functions.....	24
5.2.1.	Fires.....	24
5.2.2.	Manoeuvre	26
5.2.3.	C2	27
5.2.4.	Intelligence	27

5.2.5.	Information	28
5.2.6.	Sustainment	28
5.2.7.	Force Protection	28
5.2.8.	Civil-Military Cooperation	29
5.3.	Principles of Operation	29
5.3.1.	Unity of Force	29
5.3.2.	Mass	30
5.3.3.	Economy of Force.....	31
5.3.4.	Freedom of Action	31
5.3.5.	Objective	32
5.3.6.	Flexibility	32
5.3.7.	Initiative	33
5.3.8.	Offensive	33
5.3.9.	Surprise.....	34
5.3.10.	Security	34
5.3.11.	Simplicity.....	35
5.3.12.	Morale	36
	Applied Abbreviations.....	37
	Definitions in the Doctrine	38
	References	39
	Figures	40

Annexes

A	Joint planning and conduct of CO, RESTRICTED
B	Summary of considerations on joint planning and implementation of CO
C	Summary of force commander's considerations in connection with integrating and synchronising own operations with CO
D	Phases of OCO
E	Phases of DCO
F	Relations to NATO doctrine on CO

1. Introduction

1.1. Objective

This Joint Doctrine for Military Cyberspace Operations (JDMCO) outlines the principles for planning and implementation of military cyberspace operations (CO) on a national level. JDMCO establishes a joint understanding for CO and assigns principles for CO implementation. JDMCO forms a basis for other national doctrines, procedures, education and training related or referring to CO.

1.2. Application

JDMCO constitutes the main foundation for planning, implementation and integration of CO.

JDMCO is meant to give commanders and planners at the tactical level the knowledge and tools to effectively integrate CO with own operations and activities. JDMCO should not constrain the effort of the commander.

JDMCO establishes applied CO-related terminology.

JDMCO is based on North Atlantic Treaty Organization (NATO) doctrines and policy. JDMCO is an interpretation hereof adjusted to the Danish context.

The remaining doctrinal foundation of the Danish Defence, including NATO's Allied Joint Publications (AJP), applies to areas not covered by JDMCO.¹

In connection with planning and implementation of CO under the auspices of NATO, both existing NATO doctrines and JDMCO apply.² In case of discrepancies, JDMCO applies.

1.3. Scope

The doctrine covers offensive as well as defensive military operations in cyberspace. If nothing else is indicated, the term cyberspace operations and the abbreviation CO concern *military* cyberspace operations, which are defined as: **military activities in or through cyberspace which, delimited in time and space and through application of cyberspace capacities, intend to achieve military objectives**. This delimitation is described in detail in chapter 4.

¹ For the operational level, see Værnsfælles Forsvarskommando, *Bestemmelse for Behandling af NATO AJP Inden for Værnsfælles Forsvarskommandos Område* (ikke-klassificeret), doc. no. VFKBST U.210-0, November 2011.

² Special attention is drawn to the concept of Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA), which refers to application of national doctrine; see annex A (TTJ).

The continuous, day-to-day operation of information and communications technology (ICT) systems, which in other documents and sources may be referred to as CO, is not covered by this doctrine.

Commanders should be aware that it is the context, i.e. the military operation, and not the type of activity that determines whether a given activity is denominated CO or not. Thus, the same type of activity (e.g. analysis of log files from a server) can be a part of CO in one context, while in another context forming part of the ongoing management of IT security in connection with the day-to-day operation of ICT systems.

1.4. Background

The technological development, digitisation and increased dependence on network-based systems has led to new vulnerabilities, but also new opportunities for achieving military advantages through cyberspace.

Hostile activities in cyberspace can increasingly affect a state's cohesion, political decision making and ability to defend itself. Thus, such activities pose a risk to state security.

CO must be able to contribute to countering such risks, while exploiting the potential of cyberspace to independently or by supporting other operations achieve military advantages.

1.5. Who Conducts CO?

In Denmark, offensive CO (OCO) as well as the centralised part of defensive CO (DCO) are conducted by the CNO Capacity. With regard to the latter, the Centre for Cyber Security (CFCS) is the performing entity.

Implementation of CO in connection with other activities by the Danish Defence is by default coordinated at the joint level. However, it is important that CO also form part of the planning at the tactical level, as this level contributes directly to DCO and, through integration with own operations, indirectly to OCO. E.g., an army unit would not deploy own hackers against the adversary; instead the unit could support or receive support from OCO conducted by the CNO Capacity.³

Effective integration of CO with other types of operations, effects and activities depend on tactical level commanders who, regardless of whether their units are capable of conducting CO, are familiar with CO doctrine.⁴

³ For sub-classification of CO and clarification of roles and responsibilities, see chapter 4.

⁴ Sections 5-5.3 describe CO effects, application of the principles of operations and the connection between CO and joint functions.

1.6. Protection of Own Cyberspace

Protection of own cyberspace does not only consist of CO, but of several elements supporting each other and complicating a potential hostile attack. CO constitute a main part of the defence of cyberspace, but cannot alone guarantee confidentiality, integrity and availability or establish and maintain freedom of movement and action in cyberspace. Examples of protective measures, which do not fall within the category of CO, include e.g.:

- Physical security (external security, access control, guarding etc.).
- Data security (protection of data, backup, redundancy etc.).
- Information security (confidentiality, integrity and availability).
- Encryption.
- Network design (subnets, proxy servers etc.).
- Firewalls, antivirus, surveillance.
- ICT management (central management of updates, installation of applications, hardware etc.).
- Cyber security (CS) strategy.
- Cooperation with authorities and companies.
- Organisational education and cyber awareness.⁵

1.7. Structure of the Doctrine

The main text of the doctrine is divided into two parts:

Part I, consists of chapters 2 and 3. It explains and delimits cyberspace in a military context. It describes how cyberspace is considered an operational environment on a par with land, air and maritime operational environments.

Part II, consists of chapters 4 and 5. It outlines principles for how CO can be incorporated and integrated into military operations. In addition, it outlines the overall processes creating, on an operational level, desired effects in cyberspace. Part II is thus addressed to both commanders and planners at the joint operational level as well as commanders at lower levels tasked with integrating and synchronising with CO.

Six detailed annexes are added as supplements to the main text of the doctrine:

Annex A, which describes the processes of planning and implementing CO at the operational level. This annex is classified.

Annex B, which contains a summary of the definitions and considerations of the doctrine for use as reference in connection with planning and implementation of CO at the operational level.

⁵ Cyber awareness refers to an organisation's overall understanding of and attention to threats from and in cyberspace. Cyber awareness is vital to cyber security (CS), as the human factor often constitutes a main part of vulnerabilities in cyberspace.

Annex C, which contains a summary of the definitions and considerations of the doctrine for use as reference for commanders coordinating own activities with CO.

Annex D, which describes a chronological division of the OCO-relevant considerations of the doctrine. This annex has been classified as RESTRICTED.

Annex E, which describes a chronological division of the DCO-relevant considerations of the doctrine.

Annex F, which explains the relation to NATO doctrine for CO, including variations in terminology, definitions and procedures.

The doctrine adopts concepts defined in English doctrine, e.g. AJP.

Part I: Cyberspace

2. Defining Cyberspace

Cyberspace is defined as: **the global volume of entities processing, storing and transmitting digital information and code, regardless of whether they are connected or not.** Entities here refer to digital ICT systems, other electronic systems and networks – and their data.⁶

Thus, cyberspace is more than just the Internet; it also includes intranets and ICT elements of e.g. critical infrastructure and sensor and weapons systems as well as Command and Control (C2) systems.

Cyberspace is divided into three layers: a physical layer, a logical layer and a cyber-persona layer.



Figure 1, The three layers of cyberspace

The physical layer consists of hardware, infrastructure and connecting equipment. This includes network equipment,⁷ computers,⁸ data media,⁹ wired and wireless connections¹⁰ etc.

All elements found at the physical layer have a geographical location, and are owned and governed by national jurisdiction.

⁶ The concept data refers to information that is stored and/or transmitted digitally.

⁷ E.g. modems, hubs, routers and switches.

⁸ E.g. servers, tablets, mobile phones and PCs.

⁹ E.g. hard drives, tapes, memory, CD-ROM and USB keys.

¹⁰ E.g. data cables, sockets, access points and carrier waves.

Through the physical layer, cyberspace is in direct contact with physical operational environments and the electromagnetic spectrum (EMS).

The logical layer is the digital information and command layer, and it consists of data and code. This includes documents, files, firmware, operating systems, protocols, programmes, scripts etc.

The logical layer does not work without the physical layer, as digital information and commands are transmitted and stored at the physical layer.

A distinctive characteristic of cyberspace is that flow and storage of data and commands is not governed by the laws of physics alone, but also by human-made rules and routines which can be influenced.

The logical layer may exist as electromagnetic waves, magnetic conditions, quantum states and voltage.

The cyber-persona layer consists of virtual representations of organisations and identities. These include email addresses, user IDs, social media accounts, aliases, IP and MAC addresses¹¹ etc.

Virtual representations do not necessarily reflect identities in the physical world. A virtual representation (cyber-persona) may be used by several physical persons/organisations. Conversely, one person/organisation may have several virtual representations (cyber-personas).

¹¹ IP addresses are network-assigned addresses. MAC addresses are unique physical identification numbers on equipment capable of accessing networks, e.g. network cards, mobile phones, printers etc.

3. Cyberspace as an Operational Environment

Cyberspace constitutes an operational environment for military operations on a par with land, air and the maritime and electromagnetic operational environments. Just like e.g. the electromagnetic environment (EME),¹² cyberspace is described as a non-physical battlespace.¹³ However, cyberspace also has a physical component (e.g. in the form of entities at the physical layer, computer code's manifestation in electromagnetic states etc.). Therefore, cyberspace is different from, but at the same time in contact with physical operational environments.

Cyberspace is subject to constant human-made development and modification. Therefore, cyberspace is both a complex and opaque environment, and context and effects of the activities conducted can be difficult to predict.

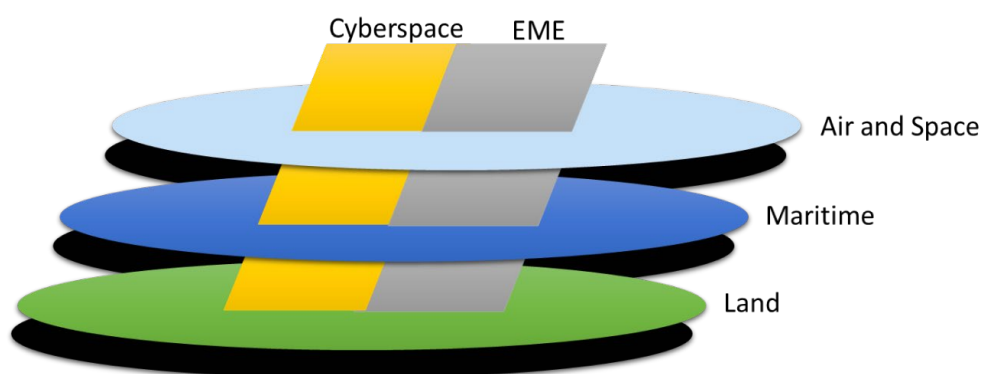


Figure 2, Cyberspace and the other environments

3.1. Elements in the Cyberspace Operational Environment

The cyberspace operational environment can be analysed and described through a series of elements, including various actors, influencing the planning and implementation of CO:

- Physical boundaries and physical conditions.
- EMS.
- Information environment.
- Own and allied forces and operations.
- Hostile actors.
- Neutral actors.
- Influence of other operational environments.

¹³ NATO, *Allied Joint Doctrine for the Conduct of Operations* (unclassified), annex C, doc. no. AJP-3(c), February 2019.

3.1.1. Physical Size and Physical Conditions

Physical conditions such as weather, terrain and geography, which greatly affect land, air and the maritime operational environment, are also relevant to the operational environment of cyberspace. E.g. space weather may affect electromagnetic dissemination of digital data, while temperature may affect the functionality of electronic equipment.

All elements at the physical layer are to some extent vulnerable to physical impact, including weather conditions.

Cyberspace is global, even though its application is more widespread in some parts of the world than others. In addition, cyberspace contains choke points found in connections between networks and systems. These are composed e.g. of Internet Service Providers (ISP), submarine cable connections and ground stations for satellite connections. When such choke points are affected, it may be felt in larger parts of cyberspace.

Through cyberspace it is possible to establish connections to military targets, including objects and persons which cannot be reached physically. Conversely, it is possible in the physical world to establish connections to parts of cyberspace which cannot be reached via cyberspace alone. E.g. special operations forces can be used to plant USB drives containing computer virus or to identify wireless networks and thus establishing connections between two separate parts of cyberspace.¹⁴

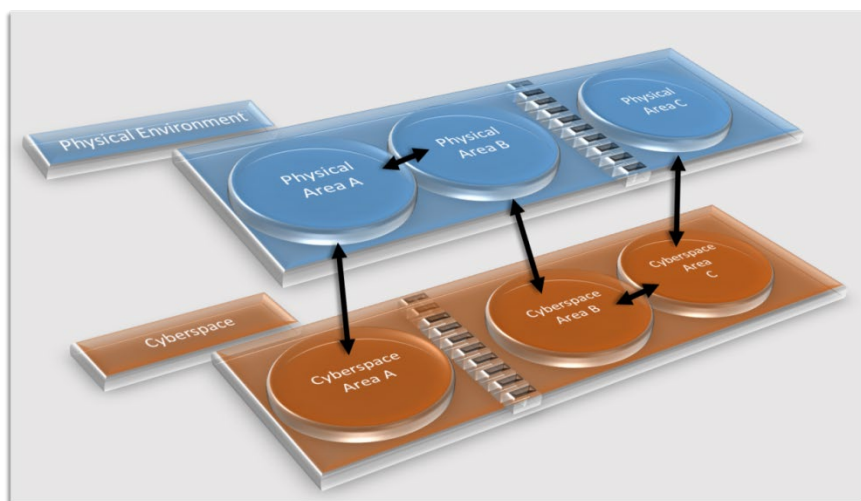


Figure 3, Physical and cyberspace connections

CO targeted at entities in cyberspace require establishing connections to these entities at the logical layer, enabling the transfer of data and/or code to or from them. Geographical location may be important with regard to the legal basis for conducting CO, as the target may be located outside the theatre or belong to a neutral actor. The use

¹⁴ These types of operations are also called Close Access Operations or 'sneaker operations', which refer to the fact that you have to 'put on your sneakers' to reach a target in cyberspace.

of cloud solutions makes it to some extent difficult to locate entities geographically and blurs the boundaries between civilian and military services.¹⁵

If there is no network connection to a system or network, connection may be established using e.g. a USB key, data cables or by forcing the system onto a wireless network. The geographical location of the system or network and physical means of access can thus affect the ability to conduct CO.

3.1.2. EMS

Wireless digital ICT is increasingly supplementing or replacing wired connections, even though the majority of all data traffic in cyberspace still runs via wired connections. As such, EMS is not a part of cyberspace, but data and code can reside in or be transmitted through the EMS. In this understanding, carrier waves can be considered electromagnetic versions of data cables. The EMS includes e.g. gamma radiation, thermal radiation etc., which neither contains data nor code.¹⁶

Even though there is some convergence between CO and electromagnetic operations (EMO) in relation to the use of the EMS, the two types of operations cannot be equated. Cyberspace and the EMS are different, but entangled.

EMO can create effects in cyberspace, e.g. by jamming a wireless data connection, as well as outside cyberspace, e.g. by jamming an analogue VHF channel. Similarly, CO can create effects in the EMS, e.g. by disconnecting a wireless access point, as well as outside the EMS, e.g. by changing data saved on a USB drive.

CO affecting EMS may be coordinated with spectrum management and EMO. Similarly, EMO affecting one or more layers in cyberspace must be coordinated with CO. This coordination is conducted during operation planning and ongoing during the conduct of the operation.

3.1.3. Information Environment

Information made available in cyberspace can be accessed globally almost immediately. Cyberspace thus offers good conditions for sharing or searching for information.

¹⁵ Cloud solutions are mainly comprised of cloud computing and cloud storage – services offered online for computing power and digital storage, respectively.

¹⁶ EMS is comprised of the total distribution of electromagnetic waves in terms of frequency or wavelength. This includes radio waves, microwaves, thermal radiation, visible light, ultraviolet light, X-ray beams, electromagnetic cosmic radiation and gamma radiation. See NATO, *Allied Joint Doctrine for Electronic Warfare* (NATO RESTRICTED), edition B version 1, doc. no. AJP-3.6, July 2012.

Cyberspace contains a large amount of information in the form of data in open as well as closed networks and systems and metadata connected with the storage and flow of data.¹⁷

Cyberspace is part of the information environment, and CO can be used in connection with information activities (IA). E.g., IA maybe comprised of manipulation of information in cyberspace. CO can thus contribute to information warfare (IW).

The information environment contains several layers, including a cognitive layer,¹⁸ which is where people deliberately make decisions based on their understanding of the current situation. Some actors use cyberspace to affect the global information environment in order to create or affect the understanding of the situation, narratives, opinions, political agendas etc. and thus influence decisions.

3.1.4. Own and Allied Forces and Operations

Activities at the logical layer of cyberspace and their effects are not necessarily directly visible. Therefore, several units can operate in the same part of cyberspace simultaneously and not be aware of each other's presence. E.g. this may cause unit A to block the efforts of unit B, if unit A turns off the targeted server from which unit B is in the process of copying data.

Coordination is therefore vital, but can, if several allies are working together, be difficult, because it involves sharing sensitive information. In connection with early operation planning, agreements and frameworks must therefore be established to determine the process for and extent of this sharing and coordination. Relevant considerations in this context are e.g.:

- Balancing pros and cons in exposing or indicating offensive as well as defensive capabilities.
- Balancing risks of exposing technologies that have to remain secret in order to conduct future CO successfully.
- Extent of planned activities, including the estimated operational advantages.
- Considerations concerning operational security.

Other actors, even trusted partners and allies, can be expected to be reticent about sharing information about current, past or future CO and the enabling technology. It should therefore be noted that the CO of allies and partners may also have negative impact on own forces' ability to operate.

¹⁷ Metadata is data about data, e.g. information about the author of a Word document, GPS data for a digital photograph etc.

¹⁸ NATO, *Allied Joint Doctrine for Information Operations* (NATO UNCLASSIFIED), edition A version 1, doc. no. AJP-3.10, December 2015.

Coordination between units is optimised through knowledge of each other's CO with regard to:

- Information about applied technology, including information about known/exploited vulnerabilities, mode of delivery etc.
- Information about applied effect, including target, time, duration, cascading effects etc.

Coordination of OCO help to prevent activities in cyberspace from affecting other operations – own or those of allies – negatively. Coordination of DCO is important, e.g. in connection with the use of shared or connected computer networks or of the same programmes.

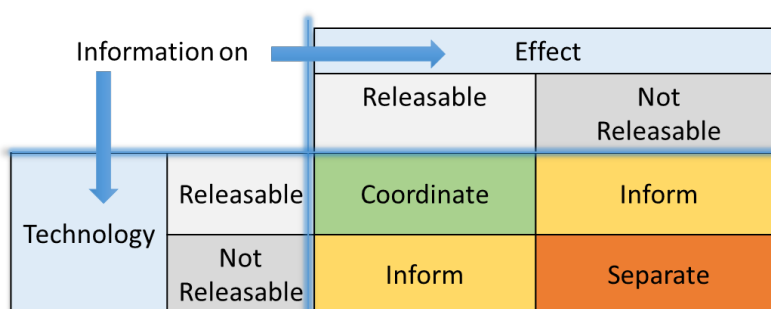
Full coordination of CO with other operations – own or those of allies – requires sharing information about the technology applied in the operation and about the delivered effect.

E.g. if sharing information about the applied technology of a cyber weapon is not a viable solution, it is important to the greatest possible extent to provide information on the effect the application hereof will have, including where and when. This will minimise the risk that the CO in question will unnecessarily affect the other operations negatively.

If sharing information about the applied technology as well as the planned effect is considered an unviable solution, the planning of the given CO should go to the greatest length possible to create *own separation* and, in so doing, reduce the risk of undesired side effects.

Maintaining *own separation* entails planning and conducting CO in such a way that undesired effects on other known activities are reduced as much as possible. Own separation can be established in time and/or space based on an up-to-date situational picture of the physical operation area and cyberspace.

For CO, i.e. for both OCO og DCO, plans must, based on the extent of information sharing, include: 1) direct coordination, 2) limited information sharing or 3) maintaining own separation.



		Effect	
		Releasable	Not Releasable
Technology	Releasable	Coordinate	Inform
	Not Releasable	Inform	Separate

Figure 4, Coordination with allies and collaborators

3.1.5. Hostile Actors

Military units' freedom of movement and action in cyberspace faces several threats. The easy access to cyberspace, technical knowhow and computer and network equipment have paved the way for actors who otherwise would not have been able to conduct offensive operations at the global level. Non-state actors are able to create effects even with relatively small investments in technology and technical knowhow, even though the scale, quality and duration of these activities are rarely on par with those of state actors. At the same time, cyberspace provides good opportunities for concealing actors who are conducting or are responsible for harmful activities in cyberspace. It is therefore difficult to assess the landscape of actors in cyberspace, and there is not always a direct connection between cyber-personas and identities in the physical world.

The complexity and opacity of cyberspace makes it possible to camouflage or conceal connections. It can therefore be difficult to identify the actor behind a given activity.

In cases where a hostile activity in cyberspace can be linked to a physical identity, it may be difficult to prove a command relationship to an organisation or state through technical evidence alone. It can therefore be necessary to do a more detailed analysis of the nature of the activity. This involves e.g. more detailed technical and behavioural analyses aiming to map the underlying context. Identifying an actor may also require legal, political and military-strategic considerations.¹⁹

Hostile State Actors

Several states have developed the ability to utilise cyberspace to gain access to systems, networks and protected information in order to achieve military, political and financial advantages. Conflicts between states, including war, can thus be expected to involve hostile activities in cyberspace. These activities can be aimed at all pillars of society, including the military pillar. Hostile activities can affect all layers of cyberspace as well as create second order effects outside of cyberspace.

The functions of a state can be more or less integrated with cyberspace. The larger the integration, the larger the consequences for the state if something in cyberspace should stop working (correctly). The effect of activities and operations in cyberspace may directly or indirectly affect the cohesion and the ability and the will of states to resist hostile attacks in or outside cyberspace. In addition to tactical and operational effects, CO can thus have strategic effects as a supplement or alternative to the effect of physical activities.

¹⁹ Legal considerations may e.g. be whether the actions of an actor can be attributed to a party to the conflict.

The effect CO may create is proportional to the defending actors' dependence on cyberspace. As states maintain different degrees of CS, the relation between such dependence and how easy it is to create the desired effect is not necessarily proportional. Thus, CO cannot necessarily replace any other type of operation.

State actors generally have more resources and tools at their disposal than non-state actors. Commanders should expect that the most effective hostile activities in cyberspace originate from states. States often undertake more long-term strategic planning; through legislation, states will be able to perform actions illegal to ordinary citizens and can thus act more freely; states often have more financial resources at their disposal; and states often have better chances of affecting, collaborating with or controlling access-facilitating companies (e.g. ISPs). Hence, they can conduct more advanced and complex CO.

Some states use non-state actors to conduct CO, e.g. to be able to deny having been involved in the CO. The rationale behind this can be to avoid military, cultural, political or financial consequences, as these activities may break national, legal, ethical, cultural or diplomatic rules and norms. Denial can also be an attempt to conceal the state's own ability to operate in cyberspace.

Hostile Non-State Actors

Non-state actors may concur with the policy of a state and conduct activities in cyberspace supporting this policy. Such concurrency can be more or less apparent, and the activities conducted can support the state to a larger or lesser degree.

Non-state actors also include insiders, terrorists, hacktivists and criminals posing a threat to others' freedom of movement and action in cyberspace.

The concept hacktivist covers individuals performing (political) activism through hacking.

Insiders are individuals with legitimate access to ICT systems, who intentionally, by accident or as a result of manipulation or deception perform activities which pose a threat to the confidentiality, integrity or availability of these systems.

3.1.6. Neutral Actors

Neutral actors are actors who are not party to the conflict of which the operation is a part.

Neutral actors can be found throughout cyberspace. And as not all layers of cyberspace have a geographical location, it can be difficult to determine which parts of cyberspace are used by or belong to neutral and outside parties.

It is not always possible to control the way data flows through cyberspace. An actor would remain neutral even though an attack of which the neutral actor is unfamiliar is routed through their part of cyberspace.

Considering the rapidly increasing utilisation of cyberspace, including e.g. the Internet, a given operations area should be expected to host a number of neutral actors, including civilians and organisations.

3.1.7. Influence from Other Operational Environments

Operational environments may affect each other. CO may affect and be affected by land, air and the electromagnetic and maritime environments. The overall operational environment of a given operation is often comprised of more than one environment, and CO are therefore rarely isolated events.

When analysing the operational environment in cyberspace, the commander should be aware of the contact points and dependencies between cyberspace and other environments. Points of contact with the physical layer may include generators, coolers in server rooms etc. Points of contact with the logical layer may include procedures for system updates, installation and distribution of applied applications, users' access to installing or changing software or to connecting external equipment (e.g. own mobile phone) etc. Points of contact with the cyber-persona layer may include the link between a physical identity and a cyber-persona. It may also be the person's access to an email account, user account or social media profile.

Weaknesses and vulnerabilities are most apparent at contact points. E.g. a system update of a critical entity in cyberspace delivered by mail on CD-ROM constitutes a serious exploitable weakness.

The commander should consider:

- Which contact points and dependencies exist between own cyberspace and other operational environments?
- Which contact points and dependencies in the adversary's cyberspace may be exploited in connection with OCO?

3.2. Errors and System Breakdowns

System errors may occur as a result of insufficient maintenance, improper use, power cuts, physical conditions (e.g. superheating), programming errors etc. Errors can threaten the confidentiality, integrity and availability of systems.

System breakdowns may expose vulnerabilities, and these must be handled immediately upon acknowledgement, as they may be used by a hostile actor to e.g. gain access to the system and connected systems.

It is often the responsibility of an IT-department within an organisation that is responsible for restoring the functionality of the system, and these activities may be performed outside the realm of CO.

However, the commander should be aware that incidents resembling errors and system breakdowns might be the result of hostile activities in cyberspace. This possibility should always form part of the commander's assessment of the cause of the incident.

Part II: Principles for CO

4. CO

CO are defined as: **military activities in or through cyberspace which, delimited in time and space and through application of cyberspace capacities, intend to achieve military objectives.**

Military activities are activities conducted under military command.

Cyberspace capacities are military capacities capable of operating in or through cyberspace in order to conduct CO.

CO always involve activities at the logical layer through insertion of data and/or code in cyberspace. Military activities affecting cyberspace without the use of data or code are not considered CO. An air attack on a data centre does not constitute CO, while an attack on a plane via the logical layer of cyberspace does.

CO can affect all three layers of cyberspace and ultimately contribute to creating effects outside cyberspace, including e.g. physical and cognitive effects.

CO can support and include all forms of combat, including defence, attack and delaying operations as well as contribute to intelligence gathering, surveillance and reconnaissance in connection with operations in cyberspace as well as in other operational environments.

CO are divided into OCO and DCO. What distinguishes offensive from defensive CO is whether use of force is applied.

The use of force in cyberspace means activities that change the adversary's cyberspace or the functionality of the adversary's entities in cyberspace.

DCO are defined as **CO, which, without use of force, intend to maintain or re-establish own freedom of movement and action in cyberspace.**

Freedom of movement and action is the ability to control and utilise the individual parts of the three layers of cyberspace. Hostile activities and other threats can reduce own freedom of movement and action.

DCO are activities intended to counter the adversary's attempt to create offensive effects.

DCO does not cover standard CS, which forms part of ICT operations and which on a daily basis is performed by the responsible authorities either centralized or decentralized.

OCO are defined as: **CO intending to use force in or through the adversary's part of cyberspace.**

Thus, CO cannot affect the adversary's cyberspace without the use of force. CO that change the adversary's cyberspace should thus be considered OCO. OCO thus also involve CO that use force with a view to defend.

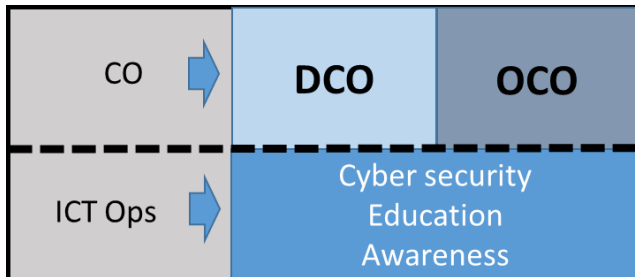


Figure 5, Delimitation of CO

4.1. Roles and Responsibilities

CO are planned at the operational level; the process is described in annex A.

4.1.1. Role of the Tactical Level in CO

Operational staff and units should expect to support CO. They should all expect to plan and conduct capacity development, education and operational activities relevant to CO. They should all include the opportunity to receive CO support, and they may all be exposed to attacks and other impacts from hostile CO. At the tactical level, it is therefore important to be familiar with the effects of CO and how CO support and are integrated in the operations.

At the tactical level, it is important to consider how the individual unit or type of weapon can integrate own operations with CO in the best possible way, both as supporting and as supported. Some units, e.g. an EW unit or special forces, may be particularly useful for connecting with targets in cyberspace or for contributing to relevant reconnaissance in relation to units and activities in cyberspace. Other units or missions will benefit from support from own CO. These potential benefits must be identified.

To support the integration of CO with other military operations, one or more Cyber Liaison Officers (CLO) may be appointed to the tactical commands and headquarters based on concrete assessment. CLO advise the commander and act as point of contact with the CNO Capacity.

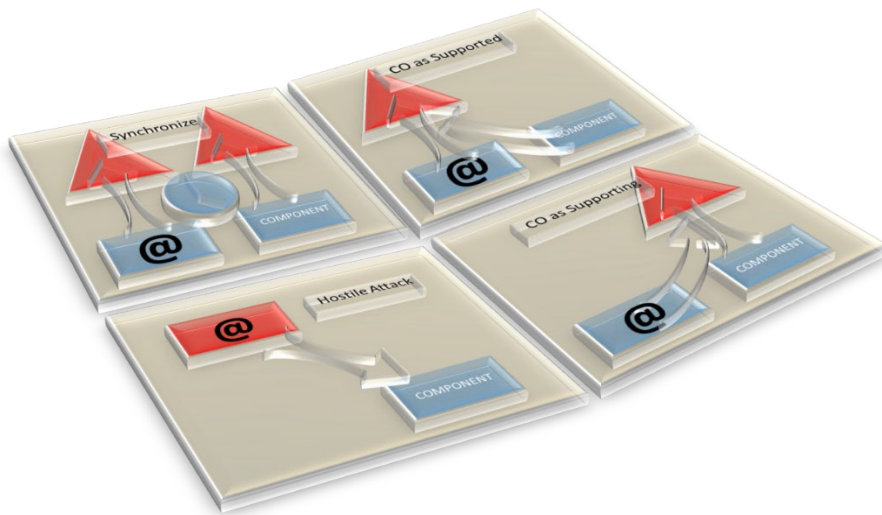


Figure 6, Role of the tactical level in CO

Mission Assurance

At the tactical level, procedures and concepts must be established to ensure that the units can operate while affected by threats from cyberspace, regardless of whether these are errors and system breakdowns or hostile OCO. These procedures and concepts contribute to strengthening the robustness of the units to threats from cyberspace and must be adapted to the units' equipment, functionality, state of readiness and mode of operation.

It must be expected that own entities in cyberspace, even with the best protection, may be affected by incidents changing or limiting their functionality in full or part. The commander should establish a comprehensive picture of the units' contact points with cyberspace, as this is often where incidents in cyberspace turn into actual threats to the system and its use. Points of contact can e.g. be equipment comprising an entity at the physical layer of cyberspace, but may also include contact points with the logical layer (e.g. use of a computer programme) and the cyber-personal layer (e.g. the email account of a commanding officer) of cyberspace.

For a unit to function, even with a high level of threat in cyberspace, it must take two aspects into account:

1. Building redundancy.
2. Building robustness.

Building Redundancy

The use of cyberspace and not least dependence on cyberspace constitutes a vulnerability, and thus the balance between utilisation, dependence and the security level must be constantly balanced. A unit whose work to a large extent depends on cyberspace will

need to maintain a similarly high level of security, which may be both cost-intensive and limit the unit's freedom of movement and even its operations.

Even though it can lead to reduced operating speed and efficiency, a unit must be able to function with limited or no use of cyberspace. It must therefore build redundancy in to the operations, which may involve establishing procedures and methods that do not depend on access to cyberspace.

PACE:

Supported by the principles of PACE, critical systems can build on four levels of redundancy: 1: **P**Primary system, 2: **A**lternate system, 3: **C**ontingency system and 4: **E**mergency System. Here 'system' may comprise physical equipment (e.g. a communications system) as well as procedures.

Building Robustness

Robustness in cyberspace may be established through the use of the five core functions: identify, protect, detect, respond, recover.²⁰

1. Identify

Identify the unit's critical systems with entities in or dependencies on cyberspace and determine how attacks on or errors in these systems affect the unit's efficiency.

2. Protect

The systems must be protected as well as possible in consideration of the balance between application, dependence and security. Considerations on 'security' must also include cost assessments in relation to the level of security, as the costs of protecting *everything from everything* are often very high. These considerations concern physical security as well as security in cyberspace. Even though other authorities may be responsible for parts of the security, local systems or practical issues may make it necessary to take extra protective precautions.

3. Detect

Incidents, including hostile OCO, reducing the functionality of entities in cyberspace are not necessarily visible. E.g. a radar monitor may show an empty airspace, either because it is empty or because the system is not working properly. For all systems, it must be determined how incidents are acknowledged and how the functionality of the system can be verified.

²⁰ The functions are based on US NIST Cybersecurity Framework: National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1, 2018.

4. Respond

Procedures for responding to incidents must be established, communicated and trained. Such procedures may e.g. include plans for Emission Control (EMCON), Information Control (INCON) and transition to alternative systems. The procedures must be adapted to local conditions. For some systems and situations, a procedure can be to shut down the system completely. Other situations call for continuing to use the system, e.g. in order to observe further hostile activity. Depending on the nature of the incident, it may be necessary to coordinate the response with the CNO Capacity, possibly in order to conduct further CO.

5. Recover

Recovery of the system may involve reinstalling the system, update, patching, replacement, changing system instructions and procedures etc.

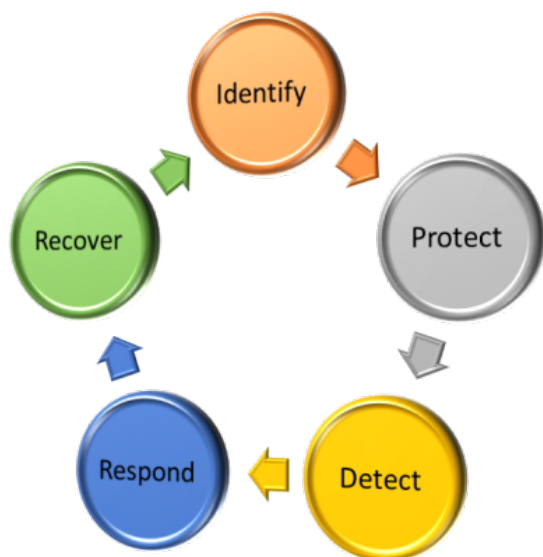


Figure 7, Core functions in building robustness

5. Commander's Considerations

Regardless of whether the commander holds the main responsibility for a joint military operation, is the person responsible for deployment of the CNO Capacity or does not form part of the CNO Capacity (e.g. a force commander), the commander must be familiar with the application of CO in order for these to form part of his considerations.

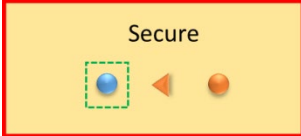
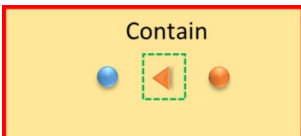
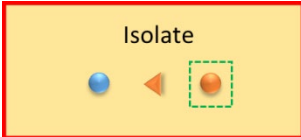

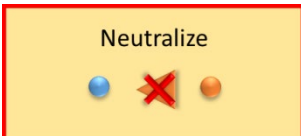
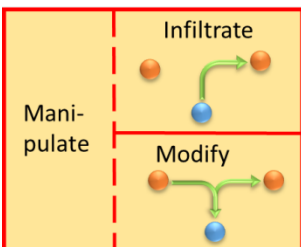
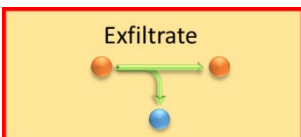
The considerations of the commander can be divided into considerations relating to, respectively:

1. Effects in cyberspace.
2. Joint functions.
3. Principles of operation.

5.1. Effects in cyberspace

CO planning builds on the following effect terms referring to effects that CO can create in or via cyberspace. These effects contribute to creating tactical, operational and strategic effects leading to the achievement of military objectives.

Effects created through OCO may be comparable to the effects of kinetic attacks, though without necessarily damaging the target permanently, as they may be reversible.

Secure	Securing confidentiality, integrity and availability in specific parts of cyberspace from hostile CO.	
Contain	Stopping further contamination by containing harmful data or code.	
Isolate	Cutting the adversary off from his deployed code, thus preventing the attacker from interacting with the code and thus also the affected system or network.	
Deceive	Countering possible attacks by changing cyberspace in order to make sure the attacker steers clear of critical systems and forces.	
Neutralise	Neutralising harmful code by making it incapable of affecting the part of cyberspace used by own forces.	
Manipulate	This effect consists of the subgroups infiltrate and modify.	
Infiltrate	Transferring data and code to the adversary's systems or networks.	
Modify	Modifying data or code in the adversary's systems or networks.	
Exfiltrate	Collecting information by compromising the adversary's systems and networks.	

Deny	This effect consists of the subgroups degrade, disrupt and destroy.
Degrade	Reducing the adversary's ability to use his own entities in cyberspace.
Disrupt	Disrupting the adversary's ability to use his own entities in cyberspace within fixed timespans.
Destroy	Destroying the adversary's entities in cyberspace completely and permanently. This effect is not reversible.
Recover	Recovering the functionality of affected systems and networks, including removing or reducing the effects of hostile attacks, e.g. by restoring data.

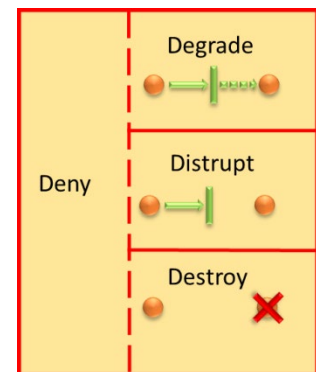


Figure 8, CO effects

5.2. Joint Functions

This section outlines joint functions in relation to CO. This includes how CO support the joint functions and the principles of operation at the tactical level. The purpose of the section is to support the CNO Capacity's planning and implementation of CO as well as the integration of CO on all levels.

Joint functions refers to joint principles which outline the main elements that must be taken into account to integrate, synchronise and implement CO.²¹

5.2.1. Fires

In this doctrine, a cyber weapon is defined as: **computer code applied to create the desired effect on the target**. Weapons deployment is the moment the code is deployed against the adversary's part of cyberspace. The effect of cyber weapons can be both physical and virtual. The effect may be brief, long-term or permanent, and the weapons design may include a delay causing the effect to be created a long time after the weapon has been deployed.

Activities in cyberspace can affect the actual operational environment and not just the entities and actors present in the environment. In other words, it is possible to change the behaviour and appearance of parts of cyberspace. This can be done by affecting the way data is distributed on computer networks, changing computers' interpretation of data and instructions, reducing a system's ability to process data requests etc.

²¹ NATO, *Allied Joint Doctrine for Operational-Level Planning* (unclassified), doc. no. AJP-5, June 2013.

The design of cyber weapons must ensure, to the greatest extent possible, that it cannot be compromised or copied after utilisation and ultimately be turned against own forces. Prior to weapons deployment it is important to ensure that own and allied operations and units are not affected unnecessarily. CO must therefore, depending on the circumstances, be coordinated with other operations and activities, including activities in the EME.

Cyber weapons can create strategic effects (e.g. impact on critical infrastructure), operational effects (e.g. disintegration of the adversary's C2) and tactical effect (e.g. neutralizing weapons systems). The objective of fires in cyberspace is to affect the adversary capability, will and understanding.

Some effects are comparable to the effects of conventional weapons, and in some cases CO can thus replace or support the deployment of physical weapons.

Cyber weapons with reversible effect can be particularly attractive with regard to subsequent rebuilding.

Cyber weapons are deployed in defence, attack, supported and supporting roles. Due to the complexity and opacity of cyberspace, developing cyber weapons requires thorough analysis of their impact and effect in the specific part of cyberspace they are to be deployed in. The risk of undesired effects must be mitigated, and a Collateral Damage Estimates (CDE) must be made.

Effective cyber weapons are rarely off-the-shelf items. Establishing access and developing cyber weapons designed to attack a specific target and create a given effect is usually so complex and resource demanding that it cannot be done by the unit and at the time where it is to be deployed. Therefore, cyber weapons are most often deployed from the CNO Capacity via the CLO. The commander should be aware that establishing a basis for developing and using cyber weapons can take months.

Prior to the deployment of a force contribution, it is in rare instances possible to prepare and deploy cyber weapons that can be delivered during the force contribution. The commander may also be tasked with synchronising own fires with the deployment of cyber weapons.

5.2.2. Manoeuvre

Manoeuvres are used to gain military advantages over the adversary and to affect the adversary's understanding of the situation, disrupt their cohesiveness in battle and to undermine their will to fight. Manoeuvres can be carried out at all layers of cyberspace. Manoeuvres in cyberspace are used in coordination with the deployment of cyber weapons.

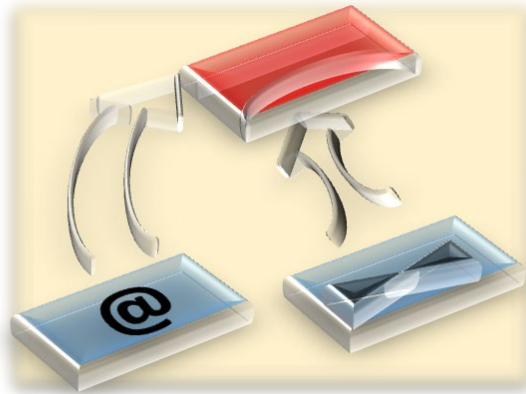


Figure 9, Synchronised manoeuvres

At the logical layer of cyberspace, it is possible to achieve a very high degree of manoeuvrability, as distances and time are not limiting in the same way as in the physical spaces. Manoeuvres can be performed fast and with a greater reach. Manoeuvres can utilise the potential of anonymity in cyberspace to strengthen flexibility, agility, concealment and cover. In some cases, though, it is necessary to manoeuvre in physical space to access non-connected parts of cyberspace.

Manoeuvres in cyberspace can take place independently of physical manoeuvres, but can also be conducted in parallel with physical manoeuvres, e.g. during an attack, where the target is engaged with kinetic weapons as well as attacks through cyberspace. For some types of CO, it is not possible to practise the deployment of a specific cyber weapon or to test its effect prior to the operation. This could be because the operation makes use of technology or techniques that only work on the specific target or whose effect would be reduced should the cyber weapon become known.

Defensive manoeuvres in cyberspace include manoeuvres intending to create:

- Cover (e.g. establishing a firewall or conducting focused data traffic analysis).
- Concealment (e.g. introducing proxy servers or in some other way concealing the layout of own cyberspace).
- Distance between oneself and the adversary by denying adversary the opportunity to connect physically or logically with parts of their own cyberspace (e.g. disconnecting or separating connected systems).

5.2.3. C2

Effective C2 is necessary for planning, synchronising and implementing CO. As CO can create operational effects outside cyberspace, CO must be coordinated and synchronised with other activities and operations.

It is vital that C2 at all levels is characterised by a high degree of resilience and redundancy with regard to impact from cyberspace, as offensive capacities of hostile actors must be taken into account. C2 information systems (C2IS) must above all be protected by a robust defence capable of denying hostile CO. At the same time, C2IS must to the greatest extent possible be able to continue to support C2, even during hostile attacks through cyberspace.

Hostile CO can come without warning and create great effects, even on a well-defended network. Deny effects can side-line computer networks for a longer period of time. However, other hostile effects can also cause networks or parts of networks to be unusable, e.g. as a result of security shutdowns, updates, reinstallation etc.

Commanders should include in their planning hostile actors' capacity to create effects in cyberspace limiting the use of C2IS. This should be based on a risk assessment.

The result of a risk assessment may be initiatives ensuring that C2 works without freedom of movement and action in cyberspace. Ultimately, the commander's C2 may therefore have to contain a sufficient, analogue alternative to the cyberspace-dependent C2IS.

C2 and C2IS robustness and the ability to support own operations, even when faced with hostile offensive effects, can be strengthened through exercise and training.

5.2.4. Intelligence

CO depend on preceding intelligence gathering both in and outside cyberspace.

The necessity hereof is proportional to the degree of complexity of a cyber weapon. The development of cyber weapons designed to engage a specific target is often based on information about the target that is not readily available. As not all parts of cyberspace are connected, it may be necessary to conduct intelligence activities and/or special forces operations to establish connections to a target.

Intelligence collected through cyberspace may be used to support CO as well as other operations at all levels. Analysis of relevant parts of the operational environment, including cyberspace, must always precede the planning of military operations.

Cyberspace can support intelligence gathering disciplines such as SIGINT, IMINT, OSINT and HUMINT. Cyberspace can provide access to targets that would otherwise have been beyond reach.

Information about the parts of cyberspace that are controlled by an adversary can contribute with important information about the adversary, including his organisation, C2, C2IS, plans, capabilities etc.

Activities in cyberspace can support Joint Intelligence Preparation of the Operational Environment (JIPOE).

5.2.5. Information

CO and IA must be coordinated and synchronised to ensure that they do not affect each other negatively. When planning CO, it must be considered whether the operation might have a negative effect on strategic communication (STRATCOM).

Activities in cyberspace may, just like physical activities, affect the information environment and thus the will, understanding and ability at strategic as well as operational and tactical levels. The commander should ensure that activities in cyberspace have been analysed to identify potential desired and undesired side effects in the information environment.

In addition, the commander should be aware that own forces may be affected through cyberspace by information and harmful activities in the information environment that are not readily visible. This may be the adversary's attempt to intimidate, provoke, confuse or in different ways affect own forces.

5.2.6. Sustainment

CO can contribute to establishing and maintaining the necessary level of functionality and security in cyberspace. The capacity for sustainment in cyberspace to a high degree builds on effective ICT management and a well-developed cyber defence.

Digitisation of military logistics, maintenance, staff and health systems etc. causes these systems to depend to a large extent on freedom of movement and action in cyberspace. Just like C2IS, the systems must be resilient, redundant and, to a sufficient extent, be able to work without access to cyberspace.

5.2.7. Force Protection

CO may be used to secure own freedom of movement and action in cyberspace as well as maintain the efficiency of own forces. Information collected through cyberspace, e.g. concerning the adversary's intentions, means, methods and actions in and outside cyberspace, may contribute to strengthening the security of own units.

DCO may include additional systems vulnerability analyses contributing to Force Protection (FP) in relation to military installations, facilities and equipment, including weapons systems.

Force protection is not just a matter of protecting the staff from direct threats such as identity theft, phishing etc. FP is also about protecting servers and databases containing information on military personnel to prevent these data from being misused, e.g. to discredit, misinform or threaten the staff, e.g. in order to subvert the morale.

5.2.8. Civil-Military Cooperation

A large part of the physical layer of cyberspace is owned or run by civilian actors. Cooperation with these actors supports CO. Contact to a local ISP can e.g. make it possible to influence or access otherwise inaccessible parts of cyberspace.

In connection with Civil-Military Cooperation (CIMIC), CO can be used to strengthen civilian actors' CS, which can contribute to building mutual trust and strengthen the cooperation. Civilian actors' level of CS may affect military activities in and outside cyberspace.

It should be considered whether it is necessary or expedient to use DCO to protect the cyberspace of civilian partners. This can e.g. be done by introducing network surveillance or deception into the partner's systems. E.g. well-functioning cooperation can reduce the risk of insider threats and attacks via subcontractors' cyberspace.

5.3. Principles of Operation

Together with other types of military activities, CO are part of the operational planning and implementation of military operations. The overall principles applying to military activities also apply to CO.²²

5.3.1. Unity of Force

Cooperation calls for all military activities to point towards the achievement of military-strategic objectives.

In this regards, CO form a natural part of any operation and can both be supported by and support other military activities. Special operations forces can e.g. support CO by installing technical equipment in the adversary's network, and CO can support an advance of own forces by manipulating the adversary's C2IS.

In some cases, CO represent an alternative to other types of military activities and may be used independently to achieve operational effects, e.g. immobilisation of the adversary's capacities and fighting the adversary's will, capability and understanding. Unity of Force emerge between military instruments of power as well as between military and

²² The principles are described in general in NATO, *Allied Joint Doctrine*, edition E version 1 (unclassified), doc. no. AJP-01(E), February 2017, and Hæren, *Feltreglement I* (unclassified), doc. no. HRN 010-001, June 2016.

state instruments of power outside the military pillar, including financial and diplomatic powers.

Unity of force is strengthened by clear command relations and coordination of activities as well as an overall strategy and shared doctrine, tactics, techniques and procedures. Technical interoperability as well as a high level of education is also important for the unity of force.

Due to the concern for operational security, it is particularly difficult for CO to give units outside the CNO Capacity insight into the planning and implementation of specific activities. Supported units therefore often have to rely on the information received via CLO, including which effects may be available to the force commander. In addition, lack of insight may limit the unity of force through in cyberspace and physical operational environments, respectively.

5.3.2. Mass

The military means available to the commander should be concentrated in time and space. Mass can be established in cyberspace by concentrating force on a single target. An example hereof is DDoS attacks, where the computer power of a large number of attacking computers is directed at a single target causing overload.²³

Another example is when more resources are assigned to CO, e.g. more hackers, in order to launch an attack or have other types of operations support CO.

Establishing mass in cyberspace through various simultaneous CO requires detailed coordination. If possible, the individual CO's effect on each other's functionality should be clarified and tested prior to initiation.

If several CO exploit the same vulnerability in the targeted system, the adversary may prevent further exploitation of the vulnerability after the first attack. In some cases, such preventive measures, e.g. network port disabling, happens automatically and at machine speed.²⁴

Mass can be established via coordination and synchronisation of CO with other activities. CO may constitute a force multiplier, e.g. through manipulation of the adversary's air defence systems, increasing the effect on the target.

²³ Distributed Denial of Service (DDoS) is an attack where a network of computers operated by remote control is engulfed by data traffic, ensuring that the target does not have enough memory, computing power or band width to process the incoming data.

²⁴ Machine speed is the speed at which computers work and data is moved. Complex calculations can take more time, but most information exchanges are almost performed at the speed of light.

5.3.3. Economy of Force

The military resources available to the commander should be used in such a way that they achieve the greatest possible operational effect with the smallest possible effort.

An advantage of CO is that they can create effects without transporting large amounts of equipment to the area of operations. And via CO, a single attack at machine speed can create effects in several parts of cyberspace.

OCO are not necessarily detected by the adversary right away. The target can thus be present in the adversary's cyberspace for a longer period of time and use this presence to create repeated effects using a small amount of resources. If the attack is detected, the defender may have to use a lot of resources to counter the attack and deny the aggressor access, restoring the desired functionality of the attacked system or network and mitigating the long-term effects of the attack.

In principle, developed tactics, techniques, procedures and code can be redeployed in full or part. However, they should be expected to have a limited service life due to the technological development, updates and patching of software. In particular, exploitation of a vulnerability in the adversary's system or network may lead to blocking of the developed exploit and the inability of the exploit in question to be used against the adversary.

The adversary is expected to learn from the applied practice, including applied tactics, techniques, procedures or code. In addition, one should be prepared for the adversary's copying and modification of applied code and ultimately the risk that it may be used against own forces.

Preparation of CO may require a lot of resources and involvement of many military functions and types of weapons. Developing cyber weapons can be a cost-intensive and time-consuming process, and it is therefore important to consider whether it is worth the effort or e.g. conventional weapons could be used instead.

The commander should consider whether CO can replace other activities, e.g. to reduce the wear and tear or release capacities for other assignments.

5.3.4. Freedom of Action

Just like any deployment of force, the use of CO are subject to a series of political, legal and military-strategic limitations ensuring that they take Denmark's political-strategic interests into account. This means that Danish units' operational boundaries may be different from those of foreign units, just as hostile actors may enjoy greater freedom of action than own forces. This also applies to CO, for which reason timely planning and early identification of frameworks and limitations, including Rules of Engagement (ROE) and operational security requirements, are vital with regard to identifying own operational freedom of action.

Freedom to choose the right actions and to act without unnecessary restrictions is a precondition for being able to adjust own cause of action fast and efficiently when facing the adversary.

The authority to launch CO should be assigned to the lowest possible level, as dictated by the circumstances of the given operation and made possible by the demand for control and maintenance of operational security. Delegation of the authority to respond to incidents strengthens the resilience, but presupposes particularly high requirements concerning coordination and communication.

During all CO, a sufficiently high level of supervision with the activity should be maintained to make it possible for the commander to respond to any deviations from the plan, including the opportunity to terminate the activity.

Commanders requesting support from the CNO Capacity should state the desired effect and abstain from imposing on the capacity unnecessary limitations concerning the means to achieving the requested effect.

5.3.5. Objective

CO must, like other operations, have clearly defined and obtainable objectives that fall within the political mandate, the legal framework and the established ROE.

5.3.6. Flexibility

Plans and procedures for CO should be flexible enough to allow for adjustments as a result of unexpected developments and incidents and give the commander maximum freedom of action.

Flexibility is increased by formulating desired effects rather than solution models, through effective use of means of communication, through trust between involved units and by strengthening the situational understanding, which includes establishing and maintaining an up-to-date common operating picture both in and outside cyberspace.

The principle of flexibility may be challenged in connection with CO. Cyber weapons designed to attack specific targets cannot necessarily be adjusted in time and space or directed at other targets.

Similarly, defensive measures cannot necessarily protect against new threats, as new threats may use unknown attack vectors and technology which requires further analysis of the threats and continued development of the defence.

5.3.7. Initiative

Initiative is about acknowledging opportunities when they occur and acting on them to achieve military advantages. Commanders should have enough freedom to show initiative and should motivate subordinates to do the same.

Initiative is also about responding to unexpected incidents and informing the chain of command if the commander does not have the authority or competence to respond to a specific incident. This is particularly important to observe, in respect to a timely identification and response to hostile acts directed at own entities in cyberspace.

Initiative in cyberspace is strengthened actively through use of CO and proactively through cyber awareness, education and training.

CO can contribute to gaining the initiative and maintaining pressure on the adversary, e.g. because CO can:

- Be implemented in periods where physical forces are manoeuvring or reorganizing.
- Be used against targets that are beyond the range of other weapons systems.
- Create friction and inefficiency in the adversary's C2 and thus promote own initiative and battle rhythm compared to the adversary.
- Contribute to changing the adversary's situational understanding and thus cause the adversary to make less effective decisions.
- Conceal own operations and movements, e.g. causing the adversary to use their initiative on decoys or unprofitable targets.
- Neutralise hostile assets that depend on entities in or access to cyberspace.

5.3.8. Offensive

CO should build on a proactive approach to maintain initiative. A defensive and reactive approach to CO is often insufficient due to the speed with which hostile OCO can create effects and due to the unique nature of cyberspace, which makes it possible to conceal future or ongoing attacks.

A proactive approach requires prescience and due care, allowing enough time for planning and preparing CO.

A high operating tempo with regard to CO requires timely involvement of the CNO Capacity and effective use of intelligence capacities in order to gather the necessary information to conduct CO.

The operating tempo can be increased by adopting a forward-looking and proactive approach to identifying possible effects, collecting intelligence on potential targets, planning of CO and obtaining political authorisation.

Opportunities to use CO to support other activities must be identified as early as possible, and the commander should, possibly supported by a CLO, as accurately as possible outline and describe the desired effect.

5.3.9. Surprise

A surprise attack will hit the adversary at a time, place and in a way the adversary is not prepared for.

It is very difficult to identify hostile OCO before they are conducted. And it is difficult to identify advanced attacks even after they have been launched.

Systems and networks contain complex software, making it unlikely that all vulnerabilities can be identified and blocked. CO therefore hold great potential for compromising the adversary's systems and networks, but also a risk that the adversary will compromise own systems and networks.

Activities in cyberspace may be conducted at machine speed and with a high degree of anonymity, which gives the attacker a timely advantage, as the defender will have to acknowledge the attack and identify the attacker before the defender might launch a counterattack.

CO can make use of deception, which may contribute to surprising the adversary. Deception can also be used offensively, e.g. by hiding malware in a an apparently harmless application,²⁵ and defensively, e.g. by use of honeynet.²⁶

5.3.10. Security

Security contributes to creating freedom of movement and action in cyberspace and reduces the adversary's chance of exploiting vulnerabilities.

Security involves balancing security and freedom of movement. In cyberspace it is particularly important to balance security measures and freedom of movement in order to avoid unnecessary deterioration, limitations and resource consumption.

Passive security is based on a premise of strong CS, thorough preparation of activities in cyberspace as well as sufficient surveillance of the part of cyberspace where CO take place.

²⁵ An example is a so-called Trojan horse, which is software the adversary trusts, but which contains hidden harmful code.

²⁶ A honeynet is a false network designed to attract a potential attacker and direct his attention away from the true network.

It is necessary to maintain a high level of operational security, both to protect own forces and systems and to ensure continued effect of security measures and cyber weapons.

Procedures for handling CS breaches should, even for unclassified networks and systems, be classified, as knowledge of such procedures can strengthen the adversary's opportunities to compromise the system or network.

Security involves looking at the other principles from the adversary's point of view in order to identifying own vulnerabilities to hostile activities. This includes the following considerations:

- Expect hostile physical attacks to be supported by cyber attacks.
- Expect cyber attacks to be able to conceal or support other activities – also in other operational environments than cyberspace.
- Use deception to conceal own cyberspace and own offensive and defensive capacities in cyberspace.
- Conceal contact points to own cyberspace, including e.g. the existence of cyber-personas, applied software and protocols and entities in cyberspace.
- If possible, restrain the adversary in an ineffective attack, e.g. by use of deception, and take advantage of the opportunity to understand the adversary's cyber weapons, techniques and tactics.
- Educate and train personnel in responding to hostile activities in cyberspace and in general cyber awareness.
- Establish, as well as possible, a comprehensive common operating picture of relevant parts of cyberspace covering all elements of the operational environment.
- Expect that an immediate common operating picture may be a result of deception on the part of the adversary.
- Establish a particularly high degree of security around C2 as well as techniques and processes to verify C2 confidentiality and integrity.
- Search actively in own cyberspace for vulnerabilities and hostile exploitation hereof, also at a time and in spaces where an attack is not expected.
- Respond to hostile CO by focussing on defensive effects rather than specific methods.

5.3.11. Simplicity

Cyberspace is a complex and opaque operational environment, where contexts and connections can be difficult to work out. This makes it difficult to control the effect of activities implemented. Therefore, it is vital to assign great weight to simplifying orders and plans to prevent them from leading to misunderstanding and confusion.

5.3.12. Morale

Maintaining morale among armed forces may involve maintaining staff access to ICT and the Internet. The principle of security should to the greatest extent possible not limit own and allied forces' access to e.g. communicating with friends and family. Naturally, this also means that the adversary's lines of communication with family and friends, system for payment of wages etc. may represent valuable targets for own and allied forces.

The morale is strengthened by communicating own forces' successful CO and the adversary's unsuccessful CO, making it clear to own forces that their efforts are worthwhile and giving the adversary a sense of their vulnerability and wasted energy. Naturally, such efforts should take into account the operational security (OPSEC), strategic and political considerations etc.

Meeting existing laws for CO and adopting ethical principles where the legislation is unclear or non-existent also contributes to strengthening the morale.

Applied Abbreviations

AJP	Allied Joint Publication
BDA	Battle Damage Assessment
C2	Command and Control
C2IS	Command and Control Information Systems
CDE	Collateral Damage Estimate
CFCS	Centre for Cyber Security
DDDIS	Director of the Danish Defence Intelligence Service
CIMIC	Civil-Military Cooperation
CLO	Cyber Liaison Officer
CNO	Computer Network Operations
CO	Cyberspace Operations
CS	Cyber Security
CyOC	Cyber Operations Centre
DCO	Defensive Cyberspace Operations
DDoS	Distributed Denial of Service
EMCON	Emission Control
EME	Electromagnetic Environment
EMO	Electromagnetic Operation
EMS	Electromagnetic Spectrum
CD	Chief of Defence
DCD	Defence Command Denmark
FP	Force Protection
HUMINT	Human Intelligence
IA	Information Activities
INCON	Information Control
IW	Information Warfare
ICT	Information and Communications Technology
IMINT	Image Intelligence
ISP	Internet Service Provider
JIPOE	Joint Intelligence Preparation of the Operational Environment
LI	Lessons Identified
LL	Lessons Learned
OCO	Offensive Cyberspace Operations
OPG	Operational Planning Group
OPLAN	Operational Plan
OPSEC	Operational Security
ORM	Operational Risk Management
OSINT	Open Source Intelligence
PPP	Private-Public Partnership
RE-TOA	Return Transfer of Authority
ROE	Rules of Engagement
SCEPVA	Sovereign Cyber Effect Provided Voluntarily by Allies
SIGINT	Signal Intelligence
SOP	Standard Operating Procedures
STRATCOM	Strategic Communication
TOA	Transfer of Authority
JDMCO	Joint Doctrine for Military Cyberspace Operations

Definitions in the Doctrine

Cyberspace: **the global volume of entities processing, storing and transmitting digital information and code, regardless of whether they are connected or not.**

- Cyberspace consists of three layers: the physical layer, the logical layer and the cyber-persona layer.
- Cyberspace is a military operational environment on a par with land, sea and air.

Cyberspace operations (CO): **military activities in or through cyberspace which, delimited in time and space and through application of cyberspace capacities, intend to achieve military objectives.**

- What distinguishes offensive from defensive operations is whether use of force is applied in or through the adversary's part of cyberspace.

Offensive cyberspace operations (OCO): **CO intending to use force in or through the adversary's part of cyberspace.**

Defensive cyberspace operations (DCO): **CO, which, without use of force, intend to maintain or recreate own freedom of movement and action in cyberspace.**

Cyber weapons: **computer code applied to create the desired effect on the target.**

Please note that:

- OCO cover all CO that involve changing the functionality of the adversary's part of cyberspace. OCO thus also include these types of operations when conducted with a view to defend.
- The ability to implement OCO is held by the CNO Capacity at the DDIS.
- Coordination, including synchronisation and integration of CO as well as support to and support from CO, is mainly performed through use of CLO.

References

<i>Feltreglement I</i> (unclassified), doc. no. HRN 010-001, June 2016.
Danish Ministry of Defence and Defence Command Denmark, <i>Militærmanual om Folkeret for Danske Væbnede Styrker i Internationale Militære Operationer</i> , 2016.
NATO, <i>Allied Joint Doctrine for Electronic Warfare</i> (NATO RESTRICTED), edition B version 1, doc. no. AJP-3.6, July 2012.
NATO, <i>Allied Joint Doctrine for Information Operations</i> (NATO UNCLASSIFIED), edition A version 1, doc. no. AJP-3.10, December 2015.
NATO, <i>Allied Joint Doctrine for Joint Targeting</i> (unclassified), edition A version 1, doc. no. AJP-3.9, April 2016.
NATO, <i>Allied Joint Doctrine for Operational-Level Planning</i> (unclassified), doc. no. AJP-5, June 2013.
NATO, <i>Allied Joint Doctrine for the Conduct of Operations</i> (unclassified), doc. no. AJP-3(c), February 2019.
NATO, <i>Allied Joint Doctrine</i> , edition E version 1 (unclassified), doc. no. AJP-01(e), February 2017.
NATO, <i>Framework Mechanism for the Integration of Sovereign Cyber Effects Provided Voluntarily by Allies into Alliance Operations and Missions</i> (NATO RESTRICTED), doc. no. MCM-0112-2018, May 2018.
National Institute of Standards and Technology, <i>Framework for Improving Critical Infrastructure Cybersecurity</i> , version 1.1, 2018.
Defence Command Denmark, <i>Bestemmelse for Behandling af NATO AJP Inden for Værnsfælles Forsvarskommandos Område</i> (unclassified), doc. no. VFKBST U.210-0, November 2011.
Defence Command Denmark, <i>Standardiseret Operationsprocedure for den Operative Planlægningsgruppe</i> , Defence Command Denmark, 1 August 2017.

Figures

Figure 1, The three layers of cyberspace	7
Figure 2, Cyberspace and the other environments	9
Figure 3, Physical and cyberspace connections.....	10
Figure 4, Coordination with allies and collaborators	13
Figure 5, Delimitation of CO	19
Figure 6, Role of the tactical level in CO.....	20
Figure 7, Core functions in building robustness	22
Figure 8, CO effects	24
Figure 9, Synchronised manoeuvres	26

ANNEX B SUMMARY OF CONSIDERATIONS ON JOINT PLANNING AND IMPLEMENTATION OF CO

Considerations Relating to Joint Functions

Function	Considerations
Fires	<ul style="list-style-type: none"> • Cyber weapons create offensive effects. • Cyber weapons are rarely off-the-shelf items. Some have to be developed, which, depending on the degree of complexity of the weapon, can take from weeks to years. • The design of cyber weapons can ensure that effects are delivered a long time after deployment. • It should not be possible for the adversary to contain and analyse deployed cyber weapons. • Deployment of cyber weapons should be coordinated with other activities, including activities of allies or partners. • Cyber weapons can create strategic, operational and tactical effects. • The design of cyber weapons can ensure that effects hereof are reversible, which may be attractive with regard to subsequent rebuilding. • Cyber weapons can be used in defence and attack. • Cyber weapons can be used in a supporting or a supported role. • The CNO Capacity may provide a catalogue of possible effects achievable through CO.
Manoeuvre	<ul style="list-style-type: none"> • Manoeuvres can take place at all layers of cyberspace. • Manoeuvres in cyberspace can be carried out independently of manoeuvres in physical space, but may also be synchronised with these. • Manoeuvres in cyberspace are not necessarily limited by speed and geographical distances. • It can be necessary to manoeuvre in physical space in connection with CO, e.g. to reach non-connected parts of cyberspace. • Fire and manoeuvre can take place across physical space and cyberspace.
C2	<ul style="list-style-type: none"> • C2 is necessary for CO to be effective. • C2 can be incorporated into a cyber weapon. • C2 and C2IS must be protected against hostile CO. • Most C2IS depend on cyberspace – and dependencies and thus potential vulnerabilities can be found at all layers. • C2 must be able to function without freedom of movement and action in cyberspace – and ultimately without use of cyberspace. • There should be analogue alternatives to digital C2IS.

Intelligence	<ul style="list-style-type: none"> • Intelligence is a precondition for effective CO. • The need for intelligence increases with the complexity of CO. • Intelligence supporting CO can be collected in as well as outside cyberspace. • Intelligence from and about cyberspace can support the planning of activities outside cyberspace. • Cyberspace can provide access to intelligence collection about targets beyond geographical range. • Knowledge about structures and context in the adversary's cyberspace may reveal information about how the adversary is organised including information about the adversary's planning and capabilities. • Activities in cyberspace may support JIPOE.
Information	<ul style="list-style-type: none"> • Cyberspace is a subset of the information environment. • CO and IA should be coordinated and synchronised. • CO may affect STRATCOM. • CO can affect the adversary's will and understanding. • The effect of CO must be analysed in detail to identify undesired side effects. • The adversary may use cyberspace to affect the information environment – this includes affecting own situational understanding and provoking or intimidating own forces.
Sustainment	<ul style="list-style-type: none"> • Cyber security, cyber defence and effective ICT operations support sustainment in cyberspace. • Sustainment in other operational environments than cyberspace often depends on freedom of action in cyberspace, e.g. in connection with logistics, personnel and health systems.
FP	<ul style="list-style-type: none"> • Information about activities in cyberspace may strengthen own security. • DCO, e.g. in the form of vulnerability analyses, contribute to FP. • Hostile CO may directly threaten personnel and operations, e.g. identity theft, phishing etc. • Hostile CO may indirectly threaten personnel and operations, e.g. if the adversary gains access to sensitive personal data.
CIMIC	<ul style="list-style-type: none"> • A large part of cyberspace is owned or run by civilian actors. • Cooperation with civilian actors (e.g. an ISP) may improve own opportunities to create effects through CO. • CO may secure civilian parts of cyberspace, among other things with in order to secure civilian actors' free communication or to reduce the effects of hostile IA in cyberspace.

Considerations Relating to the Principles of Operation

Principle	Considerations
Unity of Force	<ul style="list-style-type: none"> • Clarify the opportunity or need to support CO with other types of operations. • Identify the opportunity to support other types of operations through CO. • Clarify the opportunity to substitute physical effects with CO effects. • Inform, in consideration of e.g. operational security, about CO options and possible effects. • Strengthen knowledge about CO doctrine. • Strengthen communication between the CNO Capacity and other capacities. • Synchronise CO with operations and activities in other operational environments.
Mass	<ul style="list-style-type: none"> • Focus the effort on a single mission in time and space. • Build striking power in each individual attack. • Allow other types of operations to support CO. • Exploit vulnerabilities in the adversary's systems at the time and place where it will have the greatest effect, as the vulnerability may be closed once the adversary becomes aware of the attack. • Use support from CO as a force multiplier in connection with operations in the physical operational environments.
Economy of force	<ul style="list-style-type: none"> • Utilise CO potential to create effect without having to move equipment or personnel to an operation area. • Utilise CO potential to create effect and attack several targets simultaneously with the same weapon – without being limited by physical distances. • Utilise CO potential to relieve units operating in physical operational environments. • Build presence in the adversary's parts of cyberspace in order to create repeated effects using few resources. • Avoid exposing methods and exploited vulnerabilities. • Determine whether it is worth the cost and time to develop a complex cyber weapon or if conventional weapons should be used instead.
Freedom of action	<ul style="list-style-type: none"> • Understand the political, legal and military-strategic implications of the use of CO. • Understand the adversary's approach to the above. • Delegate the implementation of CO and cyber weapons to the lowest possible level. • Ensure that own forces focus on and train for redundancy and robustness. • Incorporate control and surveillance functions into CO, making it possible to adjust or terminate them.

	<ul style="list-style-type: none"> • Plan for effects rather than for methods.
Objective	<ul style="list-style-type: none"> • Establish clear objective for CO.
Flexibility	<ul style="list-style-type: none"> • Plan CO with flexibility in mind, as the operational environment is dynamic and opaque. • Maintain an up-to-date common operating picture. • Strengthen the communication between commanders, CLO and the CNO Capacity. • Be aware that cyber weapons are often designed for specific targets and therefore cannot necessarily be adjusted in time and space.
Initiative	<ul style="list-style-type: none"> • Build and train own readiness to face hostile activities in cyberspace. • Strengthen own cyber awareness. • Use CO to cripple and delay the adversary's C2 structure. • Use CO to affect the adversary's understanding. • Use CO to neutralise hostile assets that depend on cyberspace • Conceal own movements and activities in cyberspace to make them difficult for the adversary to acknowledge. • Exploit the fact that CO may be implemented in periods otherwise dedicated to reorganizing. • Exploit the fact that CO can be used on targets that are beyond the range of other types of weapons.
Offensive	<ul style="list-style-type: none"> • Incorporate CO into the planning at as early a stage as possible to allow for time to prepare potential effects and cyber weapons. • Due to the time it takes to develop effects and cyber weapons, it may be profitable to launch the development hereof before other operations and activities are planned.
Surprise	<ul style="list-style-type: none"> • Utilise the potential to deliver effect at machine speed. • Utilise the potential to deploy offensive capacities at a great geographical distance from the target. • Utilise the potential to conceal own activities in the adversary's part of cyberspace. • Use the advantage of being able to choose the time and place of an attack. • Use all layers of cyberspace to create deception and confusion prior to deployment of a cyber weapon.
Security	<ul style="list-style-type: none"> • Maintain an appropriately high level of operational and information security. • Maintain an appropriate level of physical security for own entities in cyberspace. • Protect information about procedures in connection with security breaches, system errors and hostile CO.

	<ul style="list-style-type: none"> • Monitor relevant parts of cyberspace. • Determine how the parts of cyberspace that are vital to own operations, but run by civilian actors can be secured. • Look at the other principles from the perspective of the adversary, and identify own vulnerabilities in cyberspace to hostile activities as well as activities in other operational environments. <ul style="list-style-type: none"> ◦ Expect hostile physical attacks to be supported by cyber-attacks. ◦ Expect cyber-attacks to be able to conceal or support other activities – also in other operational environments than cyberspace. ◦ Use deception to conceal own cyberspace and own offensive and defensive capacities in cyberspace. ◦ Conceal connections to own cyberspace, including e.g. the existence of cyber-personas, applied software and protocols and entities in cyberspace. ◦ If possible, restrain the adversary in an ineffective attack, e.g. by use of deception, and take advantage of the opportunity to understand the adversary's cyber weapons, techniques and tactics. ◦ Educate and train personnel in responding to hostile activities in cyberspace and in general cyber awareness. ◦ Establish, as well as possible, a comprehensive common operating picture of relevant parts of cyberspace covering all elements of the operational environment. ◦ Be aware that the immediate operating picture may be a result of deception on the part of the adversary. ◦ Establish a particularly high degree of security around C2 as well as techniques and processes to verify C2 confidentiality and integrity. ◦ Search actively in own cyberspace for vulnerabilities and hostile exploitation hereof, also at a time and in spaces where an attack is not expected. ◦ Respond to hostile CO by focussing on defensive effects rather than specific methods.
Simplicity	<ul style="list-style-type: none"> • Aim for simplicity in planning, as small variations in implementation can result in great differences in the effect of activities, due to the complex and opaque nature of cyberspace.
Morale	<ul style="list-style-type: none"> • Allow personnel the greatest possible access and use of cyberspace, while taking security considerations into account. • Utilise opportunities to demoralise hostile personnel by affecting their access to cyberspace and e.g. the functionality of the adversary's administrative systems. • Communicate own successes in cyberspace, while taking into account the other principles. • Comply with international law and ethics when conducting CO.

ANNEX C SUMMARY OF THE COMMANDER'S CONSIDERATIONS ON INTEGRATING AND SYNCHRONISING OWN OPERATIONS WITH CO

The roles of the Tactical Level in CO

- The tactical level should expect to integrate and synchronise with CO.
- The tactical level can support or receive support from CO.
- The tactical level communicates with the CNO Capacity mainly through CLO.
- The tactical level must identify contact points to and dependencies on cyberspace to identify vulnerabilities.
- The tactical level should conduct risk assessments with regard to the above.
- The tactical level should develop own plans and procedures that ensure the ability to operate faced with threats and hostile activities from cyberspace. This involves:
 - Building redundancy, optionally with the help of 'PACE'.
 - Building robustness, optionally through the use of the five core functions: identify, protect, detect, respond and recover.

Principles of Operations in Connection with Integrating and Synchronising with CO

Principle	Considerations
Unity of Force	<ul style="list-style-type: none"> • Identify the ways to support CO. • Identify the opportunities to receive support from CO. • Identify the benefits of replacing physical effects with CO effects. • Strengthen own knowledge about CO opportunities and effects. • Strengthen own knowledge about CO doctrine. • Ensure reliable communication with the CNO Capacity through CLO.
Mass	<ul style="list-style-type: none"> • Use support from CO as a force multiplier in connection with operations in the physical operational environments.
Economy of force	<ul style="list-style-type: none"> • Utilise CO potential to create effect without having to move equipment or personnel to an operation area. • Utilise CO potential to relieve units operating in physical operational environments. • Expect that the development and deployment of a complex cyber weapon may take a long time compared to creating effects using a conventional weapon.
Freedom of action	<ul style="list-style-type: none"> • Plan on effects rather than methods to give the CNO Capacity freedom of action with regard to how effects are created.
Objective	<ul style="list-style-type: none"> • When requesting CO effects, clearly describe the purpose of the effect.

Flexibility	<ul style="list-style-type: none"> • Maintain an up-to-date common operating picture, which includes actors and threats in cyberspace. • Strengthen the communication between commanders, CLO and the CNO Capacity. • Be aware that cyber weapons are often designed for specific targets and therefore cannot necessarily be adjusted in time and space.
Initiative	<ul style="list-style-type: none"> • Build and train readiness to face hostile activities in cyberspace • Strengthen own cyber awareness. • Explore the possibility of receiving support from CO to cripple and delay the adversary's C2 structure. • Explore the possibility of receiving support from CO to influence adversary's situational understanding. • Explore the possibility of requesting CO to neutralise hostile assets that depend on cyberspace. • Explore the possibility of receiving support from CO to maintain pressure on the adversary in periods dedicated to reorganizing. • Explore the possibility of receiving support from CO to affect targets that are beyond the range of own weapons. • Limit the adversary's chances of acquiring knowledge of the use of contact points and dependencies on cyberspace.
Offensive	<ul style="list-style-type: none"> • Identify in the planning as early as possible the possibility of integrating own operations with CO, including specific CO effects that may support own activities.
Surprise	<ul style="list-style-type: none"> • Explore the possibility of receiving support from CO to conceal or cover own activities in cyberspace as well as in physical space.
Security	<ul style="list-style-type: none"> • Maintain an appropriately high level of operational and information security. • Maintain an appropriate level of physical security for own entities in cyberspace. • Protect information about procedures in connection with security breaches, system errors and hostile CO. • Monitor relevant parts of cyberspace. • Determine how the parts of cyberspace that are vital to own operations, but run by civilian actors can be secured. • Look at the other principles from the perspective of the adversary, and identify own vulnerabilities in cyberspace to hostile activities as well as activities in other operational environments. <ul style="list-style-type: none"> – Expect hostile physical attacks to be supported by cyber attacks, and identify dependencies and contact points with cyberspace.

	<ul style="list-style-type: none"> – Expect cyber attacks to be able to conceal or support the adversary's physical activities and operations. – Camouflage contact points to and dependencies on cyberspace, including e.g. the existence of cyber-personas, applied software and protocols as well as entities in cyberspace. – Upon indication of hostile OCO, immediately coordinate response actions with the CNO Capacity. – Educate and train personnel in responding to hostile activities in cyberspace and in general cyber awareness. – Contribute, where possible, to the recognized picture of cyberspace supported by CLO. – Be aware that the immediate operating picture may be a result of deception on the part of the adversary. – Establish a particularly high degree of security around C2 as well as techniques and processes to verify C2 confidentiality and integrity. – Search actively in own cyberspace for vulnerabilities and hostile exploitation hereof, also at a time and in spaces where an attack is not expected. – Respond to hostile CO by focussing on defensive effects rather than specific methods.
Simplicity	<ul style="list-style-type: none"> • Aim for simplicity in planning, as small variations in implementation can result in great differences in the effect of activities, due to the complex and opaque nature of cyberspace.
Morale	<ul style="list-style-type: none"> • Allow personnel the greatest possible access and use of cyberspace, while taking security considerations into account. • Explore the possibility of demoralising hostile personnel by affecting their access to cyberspace and e.g. the functionality of the adversary's administrative systems. • Communicate own successes in cyberspace, while taking into account the other principles. • Use cyberspace to share information about successes in other operational environments.

ANNEX D PHASES OF OCO

OCO can be divided into four main phases:

4. Preparation.
5. Access.
6. Presence.
7. Effect.

1. Preparation

Preparation involves building sufficient knowledge of the target to design and develop an effective cyber weapon and to identify the vulnerabilities that may provide access to the target.

Knowledge of the target may be obtained via intelligence gathering, surveillance and reconnaissance and may include information from open as well as closed sources. Preparation should, if possible, involve tactical and technical training, e.g. in the form of a test on a copy or simulation of the actual target.

2. Access

Sometimes it is possible to use a widely available or previously developed cyber weapon which utilises known vulnerabilities and provides access to the target. However, it is often necessary to adjust such weapons, or to develop new ones to gain access to the specific target.

Access to targets and utilisation of vulnerabilities may require manoeuvres in cyberspace as well as in physical space.

3. Presence

Once a vulnerability has been utilised to gain access to a target in cyberspace, it must be ensured that the target is accessible, at least until the planned effects have been delivered.

In some cases, it can be a good idea to maintain presence in a target system after the effects have been delivered, e.g. in order to ensure that the target is open to future effects or to conduct BDA.

Building presence in a computer system may involve further escalating one's privileges in the system, e.g. by taking over legitimate users' access to the system. Escalation and expanded presence in a target must not involve risks of being detected.

4. Effect

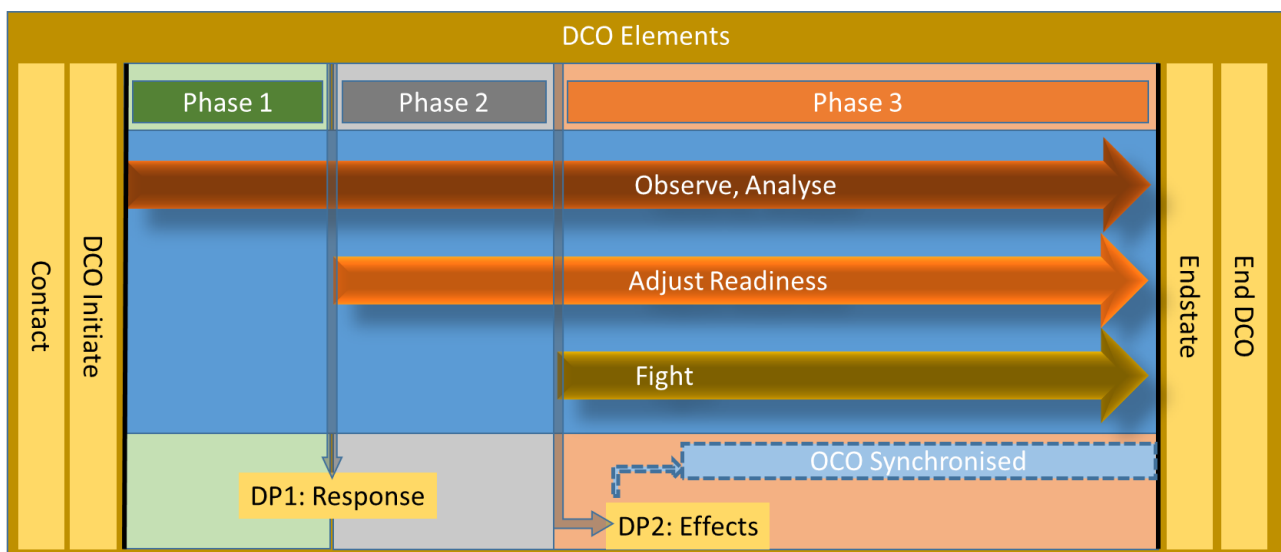
Achieving a specific effect may require continued communication with a deployed cyber weapon and thus establishing a virtual bridgehead on the attacked system and a secure communication channel. The creation of effects may be controlled in time, e.g. by programming a delay into the cyber weapon's execution of specific commands or by dividing the offensive operation into phases.

ANNEX E PHASES OF DCO

DCO are launched to counter hostile activities in cyberspace in order to secure or maintain own freedom of movement and action in cyberspace.

DCO can be divided into three main phases with intermediate decision points. The phases can last from seconds to days, depending on the nature of the hostile activities. The overall DCO process looks as follows:

1. Contact.
2. Initiation of DCO.
3. Phase 1: Observe and analyse.
4. Decision point 1: Response.
5. Phase 2: Observe, analyse, adjust readiness.
6. Decision point 2: Effects.
7. Phase 3: Observe, analyse, adjust readiness, fight.
8. Desired endstate.
9. End DCO.



1. Contact

Contact in cyberspace may be an observation of a hostile (or suspected hostile) activity in own cyberspace (e.g. OCO) or attempts or preparations to that end. Contact can e.g. be an indication of a foreign presence in own cyberspace or recognized hostile effects. Contrary to most kinetic effects, certain effects may have existed in cyberspace for a long time before they are detected.

2. Initiation of DCO

DCO is initiated on the basis of contact. Initially, initiation consists of placing responsibility for the DCO in question. If there are no deviations from Standard Operating Procedures (SOP), initiation consists only of an initiation order.

3. Phase 1: Observe and Analyse

This phase focusses on intelligence, surveillance and reconnaissance. No or few activities in this phase can affect the adversary and their activities. The purpose of the phase is to:

- Verify hostile activities, ensuring that these activities are not indeed other types of effects, attacks, errors or breakdown.
- Limit the adversary's opportunities to conduct intelligence, surveillance and reconnaissance.
- Gather as much information as possible on the hostile activities, creating a basis for decision point 1 below, including:
 - Registered activities and effects.
 - Timespan of activities and effects.
 - Applied method and technique.
 - Activities' attack vector and possibly their origin.
 - Complexity of the activity.
 - Exploited vulnerabilities.
- Identify other entities, if any, with the same vulnerabilities, which therefore may be under attack or in risk hereof.

4. Decision Point 1: Response

This decision point marks the transition from phase 1 to phase 2 and contains a presentation of information gathered at phase 1 and a decision concerning activities to be included in phase 2. The first and main decision is the extent to which one should adjust one's use of or stop using entities affected by hostile activities, as it can be beneficial in some cases to conceal from the adversary that the attack has been detected.

5. Phase 2: Observe, Analyse, Adjust Readiness

This phase should limit the effect of the hostile activities. The focussed intelligence, surveillance and reconnaissance continues, while activities intended to affect the adversary and his activities are conducted. These activities aim to the greatest extent possible and in consideration of decision point 1 to reduce the risk facing own forces by reducing:

- Own faith in affected entities.
- Own use of affected systems.
- The adversary's freedom of movement.

These limitations are achieved through a combination of informing, system shutdown and implementation of prepared procedures, e.g. launch of INCON plans and transition to redundant, alternative or emergency systems and procedures.

6. Decision Point 2: Effects

This decision point marks the transition from phase 2 to phase 3. Based on observations and the effect of readiness adjustments, the desired defensive effects are selected and prioritised. In addition, the resources, including units and personnel, intended to create the effect are identified.

The criterion for success for DCO is identified and presented as a desired endstate. The effects describe the impact imposed on the adversary. The endstate is formulated as the desired outcome of the effects.

Depending on the complexity of the operation, this decision point may include planning of deployment and synchronisation of more effects, possibly in several lines of effort.

If the response to hostile activities is OCO, OCO are divided into phases which are synchronised and coordinated with the continued activities in DCO phase 3.

7. Phase 3: Observe, Analyse, Adjust Readiness, Fight

This phase includes delivery of the defensive effects and ends once the desired endstate has been achieved. Phase 3 may be synchronised with own OCO.

Intelligence, surveillance and reconnaissance continue, while the actual battle is conducted as a combination of delivery of defensive effects and continued readiness adjustment. The battle should thus be considered a combination of fire and movement, where fire represents the deployment of defensive effects and manoeuvre the continued readiness adjustments. These adjustments can be considered defensive manoeuvres and, during battle, aim to conceal and create cover and create distance.

Conceal: Conceal own manoeuvres, actions and entities at all three layers of cyberspace, e.g. through INCON, use of proxy servers, changing network configurations etc.

Create cover: Protect own entities against the effect of hostile OCO, e.g. through patching of systems, configuration of firewalls etc.

Create distance: Ensure that vulnerable entities in cyberspace are no longer within reach of the adversary, e.g. by switching off systems and moving vulnerable data and processes to non-attacked systems etc.

Please note that the above defensive manoeuvres may also contribute to creating defensive effects.

8. Desired Endstate

Achievement of the criterion for success for DCO, defined at decision point 2, marks the end of DCO.

9. End DCO

Once the desired endstate has been achieved, the DCO in question are terminated. A debriefing is conducted in order to identify the consequences of the hostile activity as well as Lessons Identified/Lesson Learned (LI/LL).

Subsequently, LI/LL are handed over to relevant units and authorities.

ANNEX F RELATIONS TO NATO DOCTRINE FOR CO

This annex will be added once the NATO Allied Joint Publication 3.20 Doctrine for Cyberspace Operations has been released.