CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Teaming up in Cyber Command: the preparation process

Michael Widmann, Henrik Paludan Beckvard, Federico Clemente & Marcel Scherrenburg

NATO CCDCOE & NATO C2COE

Tallinn 2019

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 21 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the *Tallinn Manual 2.0*, the most comprehensive guide on how international law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise, Locked Shields. Every spring the Centre hosts in Tallinn the International Conference on Cyber Conflict, CyCon, a unique event joining key experts and decision-makers of the global cyber defence community. As of January 2018, CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

The Centre is staffed and financed by its member nations – to date, Austria, Belgium, Bulgaria, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Norway, Poland, Portugal, Rumania, Slovakia, Spain, Sweden, Turkey, the United Kingdom and the United States. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

NATO C2COE

NATO Command and Control enables NATO to orchestrate its international means and capabilities. The NATO Command and Control Centre of Excellence works on 'Catalysing C2', which means that it researches, publishes and experiments & evaluates on specific C2 topics. These topics include C2 processes and structures, human factors such as leadership, and information & knowledge management. The NATO C2COE is an 'Agent of Change'; as such, it supports ACT with the transformation of NATO, specifically on Command and Control.

The NATO C2COE mission is to support NATO, nations and international institutions and organisations with subject matter expertise on Command and Control. The main level of interest is C2 at the Operational level.

The Netherlands is the so-called 'Framework Nation' of the NATO C2COE, providing the centre with infrastructure, support resources and the main manning body. The NATO C2COE is also reinforced by six 'Supporting Nations': Germany, the United States, Estonia, Slovakia, Spain and Turkey. Our SMEs are staff officers from various military backgrounds and all service branches are represented within the centre.

www.c2coe.org

Disclaimer

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence and the NATO Command and Control Centre of Excellence (the Centres). It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centres may not be held responsible for any loss or harm arising from the use of the information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation.

Table of Contents

1. Introduction 5

2. Aim 6

3. Management functions 6

4. Elements to enhance the management functions in the design phase of creating a Cyber Command 9

4.1 Connecting 9

4.2 Collecting phase: sensing 9

4.3 Collecting phase: processing 10

4.4 Decision-making phase: sense-making 11

4.5 Decision-making phase: deciding 11

4.6 Effecting phase: acting 11

4.7 Effecting phase: assessing 12

5. Thoughts on how to enhance cooperation 12

6. Conclusions 14

References 16

Abbreviations 16

1. Introduction

Protecting cyberspace is different from protecting terrestrial borders, territorial waters or national airspace. An attack in and through cyberspace may be swift, may be varied in scope, and may occur over vast geographic distances. Incidents may not be constricted by national borders nor abide by the divide between civilian and military institutions.

Societies are more effective in the cyber domain when they increase collaboration between industry (with its innovation and development of cutting-edge technology), academia, civil society and the military. This collaboration needs to be established through mutual coordination and based on demonstrated loyalty. National strategies should call for setting up and strengthening information-sharing mechanisms to enable the exchange of actionable intelligence and threat information between and amongst the public and private sectors.

Cyber threats or incidents are often handled nationally by Computer Emergency Response Teams (CERTs) or a national cyber command, in many cases without information regarding the incident being shared. As much of the critical infrastructure which may be attacked in and through cyber is dual-use (military and civilian), nations need to define this infrastructure and who, in case of a cyber-incident, has the responsibility for protecting it.

The lack of timely exchange of information between nations substantially impairs decision-making to deal with both incidents and attacks in and through cyberspace. The coordination needed to conduct defensive cyber operations (DCO) effectively within an alliance of countries, such as NATO or the EU, requires a broad consensus on how to exchange information.

Countries need to recognise state interdependencies; but having adequate capacities to deal with threats in and through cyberspace is crucial for all governments, especially within the most technologically developed countries. These capabilities should be translated into skills that would allow monitoring of cyberspace, predict cyber operations of potential adversaries, and react appropriately and rapidly to neutralise the effects of any malicious incidents, including attacks, in and through cyberspace.

To manage a timely and effective cyber response, we look at the military world, in which command and control (C2) is considered an essential element to be successful in achieving the assigned goals and tasks.

> ‘No single activity in war is more important than command and control. Command and control by itself will not drive home a single attack against an enemy force. It will not destroy a single enemy target. It will not affect a single emergency resupply. Yet none of these essential warfighting activities, or any others, would be possible without effective command and control. Without command and control, campaigns, battles, and organized engagements are impossible, military units degenerate into mobs, and the subordination of military force to policy is replaced by random violence. In short, command and control is essential to all military operations and activities.’[1]

[1] Marine Corps Doctrinal Publication # 6. Command and Control, p 35. Headquarters United States Marine Corps, Washington, D.C. 1996. https://www.marines.mil/Portals/59/Publications/MCDP%206%20Command%20and%20Control.pdf, 18 April 2019

With the growing use of technology, command and control has evolved.[2] Machine learning and artificial intelligence (AI)[3] are reasonably good for uniform standard tasks and may, for instance, help with cyber threat detection and response. Still, the human factor cannot be ignored and it is necessary to allocate the resources to have human beings monitor automated responses and thus execute command and control.

2. Aim

The aim of this paper is to aid policy- and strategic-level decision-makers to ensure that their respective cyber policies, management-structures and management-processes are focused on enabling data-driven and timely decisions when faced with cyber incidents. Additionally, the paper seeks to show that by strengthening national efforts in this regard, cooperation between like-minded states may be enhanced.

The scope of the paper is to portray possible means of designing enhanced management processes for DCO. The target audience is decision-makers who may not already have an in-depth knowledge of the cyber domain.

3. Management functions

Command and control is a 'set of organisational and technical attributes and processes [... that] employs human, physical, and information resources to solve problems and accomplish missions'[4] in order to achieve the goals of an organisation or enterprise.

The concept of 'C2', as it is commonly called in military jargon, could be considered analogous to that of management. The obviousness of treating C2 as one function becomes apparent in the context of management theory. We are used to 'management' as one term which cannot be divided; the same applies to C2. There are a number of sources that compare the two and see C2 as simply being equivalent to management.[5] As early as in 1975, a technical report considered military command and control to be the same as civilian management: 'Outside of the element of personal risk, there are no significant functional differences between military and civilian management. Differences are of degree and not of kind.'[6] However, this is an important distinction; in addition to the danger to life, C2 also has to deal with the use of (controlled) violence.[7]

So, although as a term 'C2' is the military[8] equivalent of the civilian 'management', rather than making C2 obsolete – because an appropriate term already exists – there is actually a strong reason to keep it as a separate expression, because it distinguishes military management, which contains the possible

[2] When speaking of C2 in this paper, the concept implies the more comprehensive Command, Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance (C4ISR).

[3] Artificial intelligence (AI) is a broad concept which essentially covers the aspect of machines performing human tasks. Machine learning (ML) is a subset of AI whereby algorithms are used for a computer to make predictions or decisions without being explicitly programmed to perform these tasks.

[4] Vassiliou, Marius, David S. Alberts, and Jonathan R. Agre (2015). 'C2 Re-Envisioned: the Future of the Enterprise', CRC Press; New York; p. 1.

[5] 'Understanding Command and Control' Alberts & Hayes 2006: 32; 'That! – Command and Control in the Post-Industrial Age' Essens, de Spiegeleire, Treurniet, & Spaans, 2010: 45; 'Review of Command and Control models and theory' Crumley & Sherman, 1990: 3-4, with references to other authors.

[6] Finley, Muckler, Gainer, and Obermayer, 1975: 15.

[7] 'The legal authority assigned to a nation's military goes well beyond that of any other private or government organisation; it includes the use of controlled violence', Canadian Air Force Leadership and Command: The Human Dimension of Expeditionary Air Force Operations. English & Westrop 2007: 120.

[8] Besides other uses, the term 'command and control' is in use in computer security (C&C, www.qinetiq.com/cyber), and in environmental matters (CAC, www.epa.gov), however, in this study C2 is used only to express the phenomena that belong to the military context.

use of violence and danger to life, from civilian management, which normally does not. Management is thus a term with special meaning, and so is C2 (See Figure 1).

Meaning of the function	**Running an organisation**	
Term used to address the function	**Command and control**	**Management**
Peculiarity of the function	*Contains danger to life and controlled use of violence*	*Applicable to every organisation*
Domain where applied	**Military Domain**	**Civilian Domain**

FIGURE 1: COMMAND AND CONTROL VERSUS MANAGEMENT

This paper deals with the term 'Command and Control' or 'C2' as a compound word with a single meaning. In the Oxford English Dictionary, the meaning of C2 is presented as if it was one compound word: 'the running of an armed force or another organisation'. The same source explains 'management' as 'the process of dealing with or controlling things or people', the management theory supports the idea that this also means running of an organisation.

Once the equivalence of C2 and management has been clarified, it has to be pointed out that systems for managing cyber operations are, by nature, complex and are not limited to the digital domain. Cyber also affects the social or human domain. Creating an adequate cyber structure and cyber response process requires a comprehensive approach in multiple domains. As with all complex system implementations, the project approach can be divided into four major steps (see Figure 2: Project management process):

1. **Awareness**: create a sense of urgency for the stakeholders, define the required end-state and create a rough outline of the processes.
2. **Design**: develop an interoperable blueprint program, define system architecture, organise skills and knowledge.
3. **Implement**: realise the designed process, optimise the processes, building in-depth knowledge, and validate the system.
4. **Cooperate**: expand the boundaries of the system to partner nations and establish interoperability.

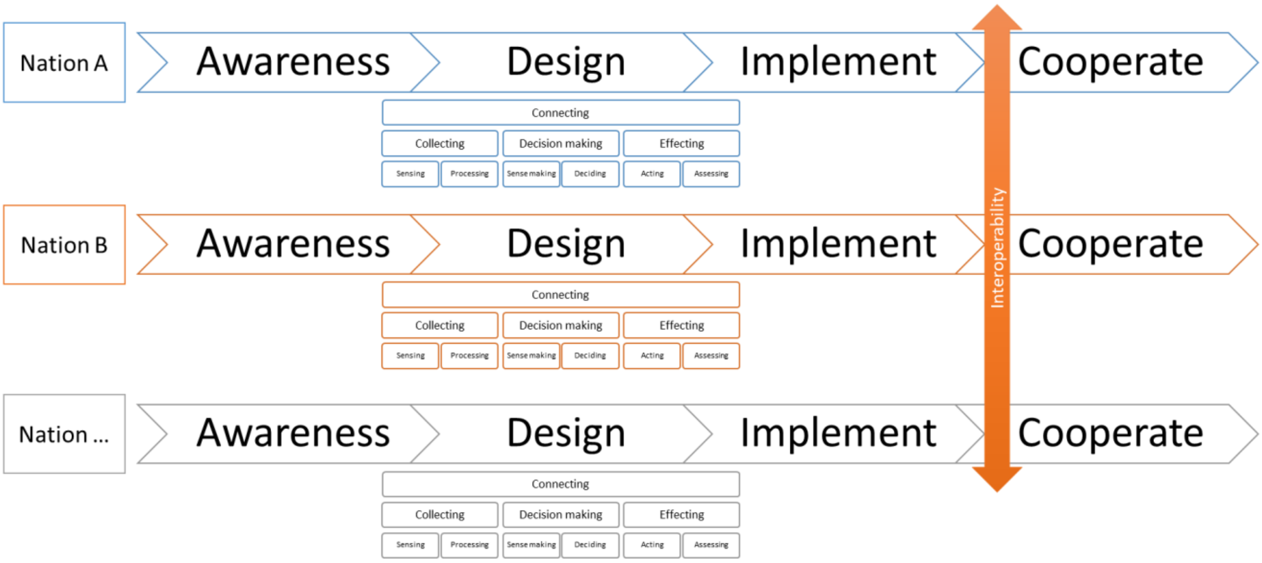

FIGURE 2: PROJECT MANAGEMENT PROCESS

This paper will focus on the design phase of the project management process and, to a lesser degree, on the cooperation phase (which links up to the awareness phase). This paper will not look into the awareness phase beyond emphasising that continuous and comprehensive awareness of the strategic environment is crucial for information superiority. Also, the implement phase will not be dealt with further than to highlight the obvious, that the design needs to be properly implemented in order to function.

During the design phase, nations should have substantial knowledge of transboundary cooperation and use of tools. Some nations may not be able or willing to undertake all elements in the design phase themselves.

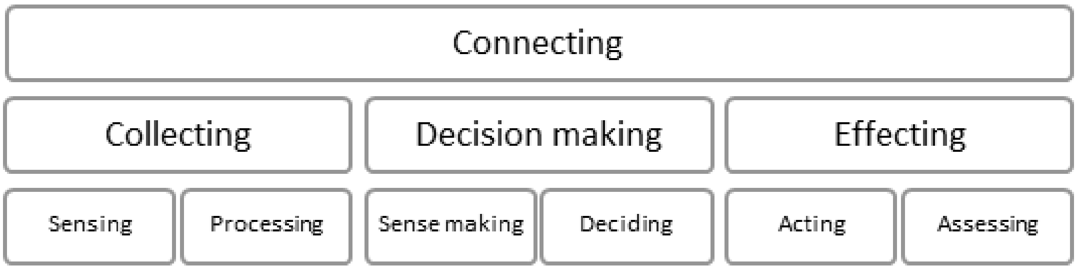

Figure 3: Detail of the design phase

The design phase is critical for future success. To ensure interoperability during the cooperation phase, a standardised approach is required. A possible model, based on best practice knowledge, is the C2 model described by NATO's Allied Command Transformation (ACT) in the C2 Capstone Concept.[9] This model defines four phases within the C2 process: *Connect*, *Collect*, *Decide* and *Effect*.

The first phase is *connecting*. It is the central and principal phase without which C2 is not possible. It seems obvious, but sometimes one forgets just how important it is. Without the ability to receive information from the outside and to send orders to those who must perform the actions, command and control cannot exist. The connection must materialise, not only with the use of communication means (computers, telephones, email, videoconference, etc.), but also with the exchange of liaison officers.

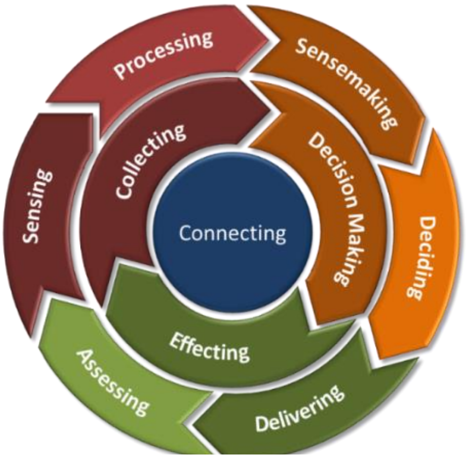

Figure 4: Command and Control cycle according to the ACT C2 Capstone document. The inner ring shows the C2 phases and the outer ring shows the functions/activities

The second phase is *collecting*. During the collection phase, data is gathered to elaborate on the information that will allow a later understanding of the situation. To be able to carry out these actions, sensors and data analysis capacity are needed. This data processing capacity must be adequate to analyse, within a reasonable time, the data obtained. The sensors must be deployed correctly and directed adequately to get the information needed and filter it from less relevant data. In some cases, artificial intelligence may be a great support in this process, by having machines imitate cognitive human problem-solving and conduct the filtering faster than humans.

The third phase is *decision-making*. This phase aims to obtain the maximum situational awareness possible and make timely decisions. It seeks to present the reality of the event so that the decisions made are based on verifiable facts. Visualisation of that

[9] https://tide.act.nato.int/tidepedia/index.php/ACT_C2_Focus_Area_-_Capstone_Concept, 14 May 2019.

information is crucial when a human decision has to be made. In some cases, only machines will be able to understand the changing environment rapidly enough and be ready to make a decision in accordance with the information.

Finally, the fourth phase is *effecting*. The effecting phase aims at executing the actions decided in the previous phase and assessing whether they have been adequate and have created the desired effects. In this phase, the suitable tools and actors are needed to achieve the desired effects. The quality and speed of the response influences the entire decision-making process. If the answer is slow, it takes longer to produce the desired effect, which again influences the decision-making cycle.

4. Elements to enhance the management functions in the design phase of creating a Cyber Command

How should the elements in the command and control cycle shown in Figure 4 be made functional? NATO ACT has made a *C2 SWOT Analysis* of the elements to highlight the strengths/opportunities and weaknesses/threats for each.[10] Based on the *C2 Capstone Project*, this section looks at some of the actions derived therefrom,[11] which NATO, Nations, Partners and organisations may implement in order to enhance the management functions in the *design* phase shown in Figure 3.

4.1 Connecting

As illustrated by Figure 4, *connecting* is the lynchpin of the command and control cycle through which the three interlocking phases of *collecting*, *decision-making* and *effecting* take place. Connecting means something more than just electronically connecting the decision-maker with the subordinates. More broadly, it means connecting with the surroundings. Subordinate, lateral and superior levels, relevant actors in cyberspace policy, other decision-makers and main stakeholders have to be connected together. This connection will allow information sharing and dissemination of orders. It will facilitate the necessary situational awareness and understanding of the different actors to coordinate and unify their efforts.

Therefore, the first thing when creating or assessing a Cyber Command is to define the elements which have to be connected and how to connect them. It is crucial to develop an information exchange matrix (IEM) or a similar system and not to forget to include the use of liaison officers when two important system elements have to be closely coordinated. The IEM must be exhaustive and should include access to databases, emails, VTC, (protected) websites and liaison officers.

Naturally, when creating the IEM, important interoperability issues will arise. It is, therefore, necessary to decide on the communication system, standards and procedures to be used and the responsibilities for providing and maintaining the connection and the service management. It should also not be forgotten that the user has to adapt to the requirement and the responsibilities to make that connection happen.

4.2 Collecting phase: sensing

The first element in the *collecting* phase is *sensing*. Essentially, sensing is picking up data and potential or actual network threats. With the Internet of Things (IoT), there is a lot to monitor and high-volume,

[10] https://tide.act.nato.int/tidepedia/index.php/C2_SWOT_Analysis, 14 May 2019.
[11] https://tide.act.nato.int/tidepedia/index.php/ACT_C2_Focus_Area_-_Capstone_Concept, 14 May 2019.

high-velocity and high-variety information may lead to big data challenges. However, the sensing technology is quickly developing and autonomous systems, cognitive computing and AI are being employed and will no doubt play an increasingly important role in sensing, thereby identifying and mitigating threats to the network. By connecting sensors and sharing information between entities, the defence against any threats posed in or through cyberspace may be strengthened.

In a simple form, sensors may be a firewall installed for protecting computers or a network. The firewall will analyse packet headers and reject those that do not fit a pre-defined policy based on protocol type, source address, destination address, source port, and destination port. Packets not fitting the policy will be caught by a filter, from which it may be possible to see who sent the packet and a simple sensing is thereby conducted.

In the cyber domain, setting up intrusion detection systems (IDS) will assist sensing by monitoring what is happening within a network and giving an alert. For instance, a signature-based IDS is designed to monitor information coming to the network and to compare it with signatures or attributes from known malicious threats or anything out of the normal picture for the particular network. The difference between an ordinary firewall and an IDS is that the latter will also look at the packet payload and not only the header. Colloquially, such systems may be classified as network intrusion detection systems (NIDS) or host-based intrusion detection systems (HIDS). Both NIDS and HIDS are passive, as they only give a warning but take no action.

An intrusion prevention system (IPS) will further be able to take pre-defined action against the intrusion, typically by blocking any further traffic from a particular IP-address or user. These active systems may also be network intrusion prevention systems (NIPS) or host-based intrusion prevention systems (HIPS).

To sense who is trying to get into a system, so-called honeypots may also be laid out, looking like the system they are trying to protect but in reality being nothing but a decoy. The purpose of a honeypot is to entice hackers into a trap to reveal themselves and the methods they use to gain access to a system.

With the rollout of 5G, many devices will be interconnected and the amount of data to sense will increase dramatically, potentially leading to big data challenges. At the same time, however, the latency (speed) of 5G should enable us to process more data.

4.3 Collecting phase: processing

The second element of the *collection* phase is *processing*. That which has been sensed needs to be processed into data, which may be analysed to create the situational awareness needed for decision-making. Data collection management and data processing support situational awareness and decision-making. The data generated by, for instance, the NIDS (generally, malicious activity or violation of the network) will be reported to an administrator or collected centrally using a security information and event management (SIEM) system, combining data from multiple sources and filtering out malicious activity. In most cases, to be effective a SIEM system will have to be custom-built for the network on which it is being applied.

Creating strategic situational awareness and an effective decision-making process is crucial to responsiveness, not least at the political level both nationally and within an alliance such as NATO or the EU. The element of *processing* is a prerequisite for both sense-making and deciding. With an ever-increasing amount of data, it is necessary to employ AI-technology, adaptive algorithms and predictive searches in the processing of data. Human thinking will still be required and cannot be factored out, but for processing large quantities of data, machine learning (ML) will likely be increasingly used. As one form of AI, ML may be described as machines learning from their own experience to recognise patterns, by using examples rather than by programming. Using ML, it may be possible to drastically reduce both the effort and time in processing data and helping make sense of it.

4.4 Decision-making phase: sense-making

The first element of the *decision-making* phase is *sense-making* – understanding the processed information and creating situational awareness. As with the processing of the data, emerging technologies such as analytics, adaptive algorithms, predictive search, AI and human cognition enhancers provide unprecedented opportunities to enhance the analysis work in this area.

With constantly changing threats, it is essential that decision-makers have continuous strategic awareness and are both trained and exercised to react swiftly to an event so that decision superiority may be maintained or quickly regained. To aid human cognition, for instance with regression analyses or the prediction of all possible paths of an attack that has occurred, ML may be employed.

Humans understand differently and often a variety of ways of portraying of information will be needed in order to have everyone on the same page and making (the same) sense of the processed data. In this regard, visualisation may be a great help for decision-makers in illustrating and communicating the 'so what' of a given scenario – its implications and possible solutions.

An essential element for success is that information is shared both between entities within a nation and between nations. The willingness to share information is based on trust and this must be forged in peacetime if we are to have 'zero-day' readiness and responsiveness. Thoughts on how to further improve and develop cooperation will be explored in section 5, the *team of teams* approach.

4.5 Decision-making phase: deciding

There seems little doubt that computer-aided decision-making tools will be more widely used for making decisions more quickly and with fewer staff members. Factors such as restraints, constraints, logistics and time may be run through a program and aid decision-making, but most systems will still have a person in the loop to be able to override a computer-made decision if needed. Computer-aided decision-making may provide both knowledge and decision superiority, but the C2 capacity to bridge the gap of both collecting information and ensuring political consultation, thus enabling decision-making in a complex environment in a timely manner, presents a significant challenge.

Flatter C2 structures and quicker decision cycles will also need to be put in place in order to be both fast and flexible enough to counter attacks in and through cyberspace, where time is often a critical factor. The combination of centralised intent with decentralised execution is not a new concept, but is rarely implemented. Thoughts on this will be dealt with in Section 5 below.

4.6 Effecting phase: acting

The first element of the *effecting* phase is *acting,* which is countering or delivering lethal and non-lethal effects through cyber. Essentially, you may be able to achieve the same effects through cyber as you may through kinetic means. In this case, effecting refers to all manual, semi-automated and automated, political, military, economic, social and information capabilities required to deliver effects and achieve execution superiority. Acting (or reacting) refers to delivering (or countering) these effects. At the tactical level a cyberspace capability may be described as a device, computer program or technique, including any combination of software, firmware or hardware, designed to create an effect in or through cyberspace.[12] At the operational level, the focus will invariably be on the effects which may be delivered through cyber weapons. There is as yet no uniform definition of what constitutes a cyber weapon, but

[12] US Joint Publication 3-12 Cyberspace Operations, 8 June 2018, I-4 - https://fas.org/irp/doddir/dod/jp3_12.pdf, 24 April 2019.

for the purpose of this paper it may be defined as 'software and IT systems that, through ICT networks, manipulate, deny, disrupt, degrade, or destroy targeted information systems or networks'.[13]

As with all operations, the speed and time with which you are able to act (or react) vis-à-vis the opponent may provide execution superiority. Regarding the cyber domain, experts and officials agree that the speed of attacks and their sophistication has changed dramatically. Another vital difference lies in their diversity.[14]

Although the scope of this paper is cyber defence, it is worth mentioning the old adage that 'the best defence is a good offence' and, consequently, many countries also possess offensive capabilities. It is important to be aware that a cyber weapon is not the same as kinetic ordnance, although the effects may be similar. Once a cyber weapon has been used it cannot, in most cases, be reused. Depending on the target, an attack in and through cyberspace may therefore not always be initiated as quickly as an attack through kinetic means. For such an attack to be effective, meticulous planning must be conducted, often with years of intelligence preparation and weapon development. In cyber defence, much, therefore, relies on *sensing* the preparations of an opponent.

4.7 Effecting phase: assessing

The second element of the *effecting* phase is *assessing*. Assessing refers to measuring the effectiveness of the intended effect and to determine possible un-intended consequences. Coordinating and controlling effects is a crucial C2 function to ensure that all effects are optimised and synchronised to maximise the outcomes and minimise any collateral damage.

In the cyber domain, assessing is to a large extent done by monitoring whether the targeted system is still up and running, or whether a capability of the opponent is still a threat to your own network systems. If the attack in and through cyberspace has had an effect in another domain, this may also be observed through the same means as is used for assessment within that domain.

Apart from *detecting* an attack in or through cyberspace, the incident may be *assessed* by looking at how well it was *redirected* (deterred, diverted or deceived), *obviated* (prevented or pre-empted), *impeded* (degraded or delayed), *limited* (contained, curtailed and/or how quickly one was able to expunge or recover) or *exposed* (analysed and publicised).[15] As *assessing* is partly done through *sensing,* the C2 cycle is thereby completed.

5. Thoughts on how to enhance cooperation

At the Warsaw Summit in July 2016, NATO reaffirmed its defensive mandate and recognised cyberspace as a domain of operations which must be defended as effectively as the air, land and sea domains. With this increased focus, cyber defence is now one of the areas of strengthened cooperation between NATO and the EU. As part of the two organisations' increasingly coordinated efforts to counter hybrid threats, NATO and the EU share information between cyber crisis response teams and exchange best practices.[16] Countries outside NATO and the EU which share the same values and common

[13]What are Cyber Weapons?: Some Competing Definitions https://www.lexology.com/library/detail.aspx?g=65179269-c85e-4253-a9a3-5d9ba1c9c906, 24 April 2019.

[14] NATO: changing gear on cyber defence - https://www.nato.int/docu/review/2016/Also-in-2016/cyber-defense-nato-security-role/EN/index.htm, 24 April 2019.

[15] See *Characterizing Effects on the Cyber Adversary,* MITRE TECHNICAL REPORT MTR1 3 04 3 2 available on https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf, 15 April 2019.

[16] NATO Cyber Defence Factsheet, February 2019 - https://www.nato.int/.../20190208_1902-factsheet-cyber-defence-en.pdf, 15 April 2019

approaches to cyber defence now see the cyber domain as a priority and have consequently developed (or are in the process of developing) national cyber policies and doctrines.

One way of enhancing cooperation, both nationally (between national organisations) and internationally (between NATO, the EU and eventually like-minded nations) would be to adopt the 'team of teams' approach developed by US General Stanley McChrystal.

To be more effective in combating Al Qaeda, General McChrystal and the Joint Special Operations Task Force in Iraq discarded conventional procedures and reconfigured the task force in the midst of fighting. A network was created that combined transparent communication with decentralised decision-making authority. The walls between silos were removed and leaders looked at the best practices of the smallest units and found ways to extend them to thousands of people on three continents, using technology to establish a oneness that would have been impossible even a decade or two earlier. The task force became a 'team of teams' – faster, flatter, more flexible – and beat back Al Qaeda.[17]

Figure 5 visualises the approach and the differences between traditional command structures and a 'team of teams' construct. The coloured circles represent individual states or entities and the lines between them represent the cooperation (both internally and externally).

Societies we will be more effective when we have greater cooperation between industry (with its innovation and development of cutting-edge technology), academia, civil society and the military within the cyber domain. Such cooperation needs to be based on trust which is established through credibility and demonstrated loyalty. National strategies should call for setting up and strengthening coordination and information-sharing mechanisms to enable the exchange of actionable intelligence and threat information between and amongst the public and private sectors. Malicious incidents, including attacks, in and through cyberspace do not happen in a vacuum: they require funding, information-gathering about the intended victim and careful planning. It is likely that information about such activities will be picked up, but this information is not worth much if it is not shared. Determining how to securely share classified information between like-minded nations in a timely manner will prove a challenge, but the effort must be made.

Handling malicious cyber incidents, especially as they most often fall below the traditional threshold levels of crises and conflict, is often done nationally by the CERTs or a national cyber command, in many cases also without information regarding the incidents being shared.

[17] https://www.mcchrystalgroup.com/insights/teamofteams/, 15 April 2019

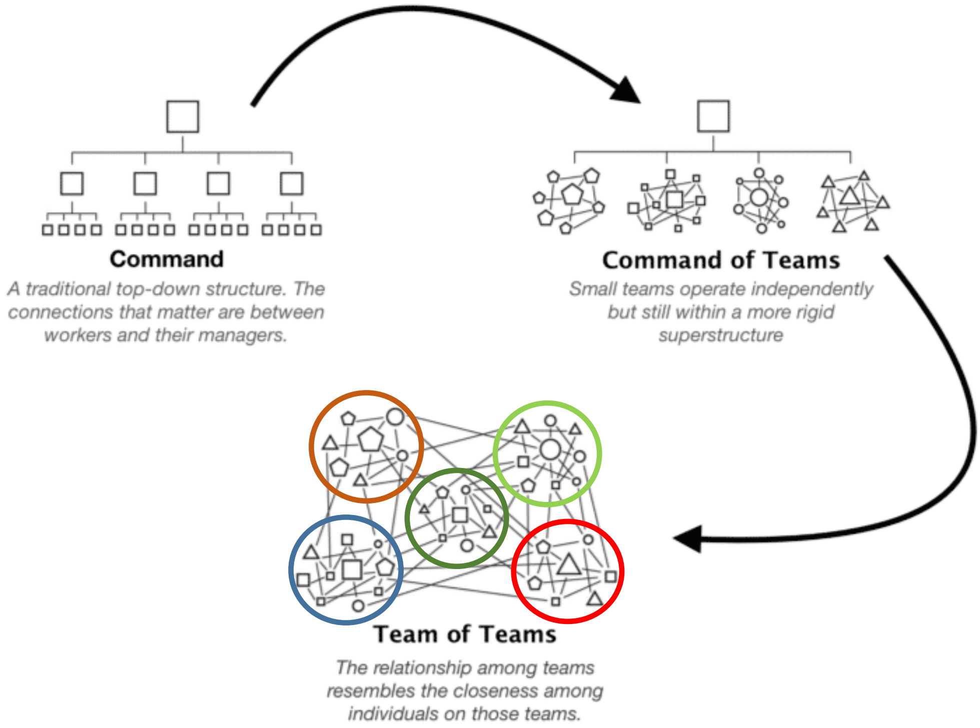
Command
A traditional top-down structure. The connections that matter are between workers and their managers.
Command of Teams
Small teams operate independently but still within a more rigid superstructure
Team of Teams
The relationship among teams resembles the closeness among individuals on those teams.

FIGURE 5: ILLUSTRATION OF THE 'TEAM OF TEAMS'. THE ORIGINAL ILLUSTRATION (WITHOUT CIRCLES) © ORGANIZATIONALPHYSICS.COM

The team of teams approach was seen by McChrystal to be effective for highly specialised teams working together – a scenario not totally remote from national entities working together, or for states working together. In any organisation, either military or civilian, there will be leaders and subordinates; but to be able to act or react swiftly, there is a need for leaders to trust their subordinates and delegate executive powers while still assuming responsibility for the actions taken. General McChrystal identified *shared consciousness* and *empowered execution*[18] as key elements of the team of teams approach. Shared consciousness is a carefully maintained set of centralised forums for bringing people together, and empowered execution is described as a 'decentralised system for pushing authority out to the edges of the organization'.[19] McChrystal names these two elements as key for transforming a task force so that it became 'a single, cohesive unit far more agile than its size would suggest'.[20] He employed the same method against the Taliban in Afghanistan with success and today advocates the idea to the corporate world. In the same vein, such a way of working together could be applied for enhanced cooperation between entities and between states within the cyber domain.

6. Conclusions

Collaboration in the cyber domain is a benefit for nations, and information sharing between public and private sectors is an important enabler. When creating a system to manage cyber operations, nations should focus their attention on the design phase of the project management process. The design should make the system interoperable to cope with the requirement for collaboration between both sectors and

[18] The Key Point - https://thekeypoint.org/2015/11/27/team-of-teams/, 15 April 2019
[19] Ibid
[20] Ibid

countries. This interoperability should be in all phases of the command and control functions (connecting, collecting, decision-making and effecting).

Defining effective information exchange mechanisms, such as an IEM with defined processes, and using liaison elements to link the organisations will enhance trust and provide the basis for connecting well.

The management system needs to be able to sense cyberspace through setting up firewalls, intrusion detection systems and intrusion prevention systems. The use of decoys such as honeypots will facilitate the identification of attacks or potential attacks in and through cyberspace, together with the methods being used to gain access to your network.

Once the sensing is made, there is a need to process all the data. A bespoke Security Information and Event Management system will facilitate the combination of all these data and the identification of malicious activity. To reduce effort and time in processing data and to make sense of it, the use of AI and ML to identify patterns will undoubtedly be helpful, especially when dealing with large amounts of data.

To make sense of all processed data, a good visualisation tool will be required to present the findings to decision-makers who may not have a detailed knowledge of cyber. This tool should include data processed by other connected organisations. To further quick decision-making, a shared consciousness and a flattened decision-making organisation based on centralised intent and decentralised execution is advisable, as this may provide a more flexible and adaptable way to exercise C2.

The effecting phase of the project management process must be able to use effective cyber weapons and remember the adage that ‘the best defence is a good offence’.

If the management system is designed following these principles and nations and societies enhance their cooperation, both internally and externally, using the ‘team of teams’ approach, managing cyber operations may be both faster and better-coordinated.

References

An Analysis and Evaluation Methodology for Command and Control. Finley, Muckler, Gainer, and Obermayer, 1975.

C2 Re-Envisioned: the Future of the Enterprise, Vassiliou, Marius, David S. Alberts, and Jonathan R. Agre, CRC Press; New York, 2015

Canadian Air Force Leadership and Command: The Human Dimension of Expeditionary Air Force Operations. English & Westrop 2007.

Characterizing Effects on the Cyber Adversary, MITRE TECHNICAL REPORT MTR1 3 04 3 2

Marine Corps Doctrinal Publication # 6, Headquarters United States Marine Corps, Washington, D.C. 1996

NATO ACT C2 Capstone Project, Tidepedia

NATO ACT C2 SWOT Analysis, Tidepedia

NATO Cyber Defence Factsheet, February 2019

Review of Command and Control models and theory. Crumley & Sherman, 1990:

Study on the Command and Control: Generating a Conceptual Framework. An unpublished report of the NATO Command and Control Centre of Excellence. Tammistu, R. 2016. Utrecht.

Team of Teams – New Rules of Engagement for a Complex World, Portfolio/Penguin, 2015

That! – Command and Control in the Post-Industrial Age. Essens, de Spiegeleire, Treurniet, & Spaans, 2010: 45;

The Key Point - https://thekeypoint.org/2015/11/27/team-of-teams/

Understanding Command and Control. Alberts & Hayes 2006: 32;

US Joint Publication 3-12 Cyberspace Operations, US Joint Chiefs of Staff, 8 June 2018

Abbreviations

ACT – Allied Command Transformation

AI - Artificial Intelligence

C2 – Command and Control

C4ISR - Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

CERT - Computer Emergency Response Team

DCO - Defensive Cyber Operation

HIDS - Host-based Intrusion Detection

IDS - Intrusion Detection System

IEM - Information Exchange Matrix

IoT - Internet-of-Things

IPS - Intrusion Prevention System

JOA - Joint Operations Area

ML - Machine Learning

NATO – North Atlantic Treaty Organization

NIDS - Network Intrusion Detection System

SWOT – Strengths, Weaknesses, Opportunities, Threats

VTC – Video Teleconference