All about access

Insights from NLD DISS cyber operations and their implications for digital striking power

The authors work for the Netherlands Defence Intelligence and Security Service (NLD DISS) and must therefore remain anonymous for security reasons.

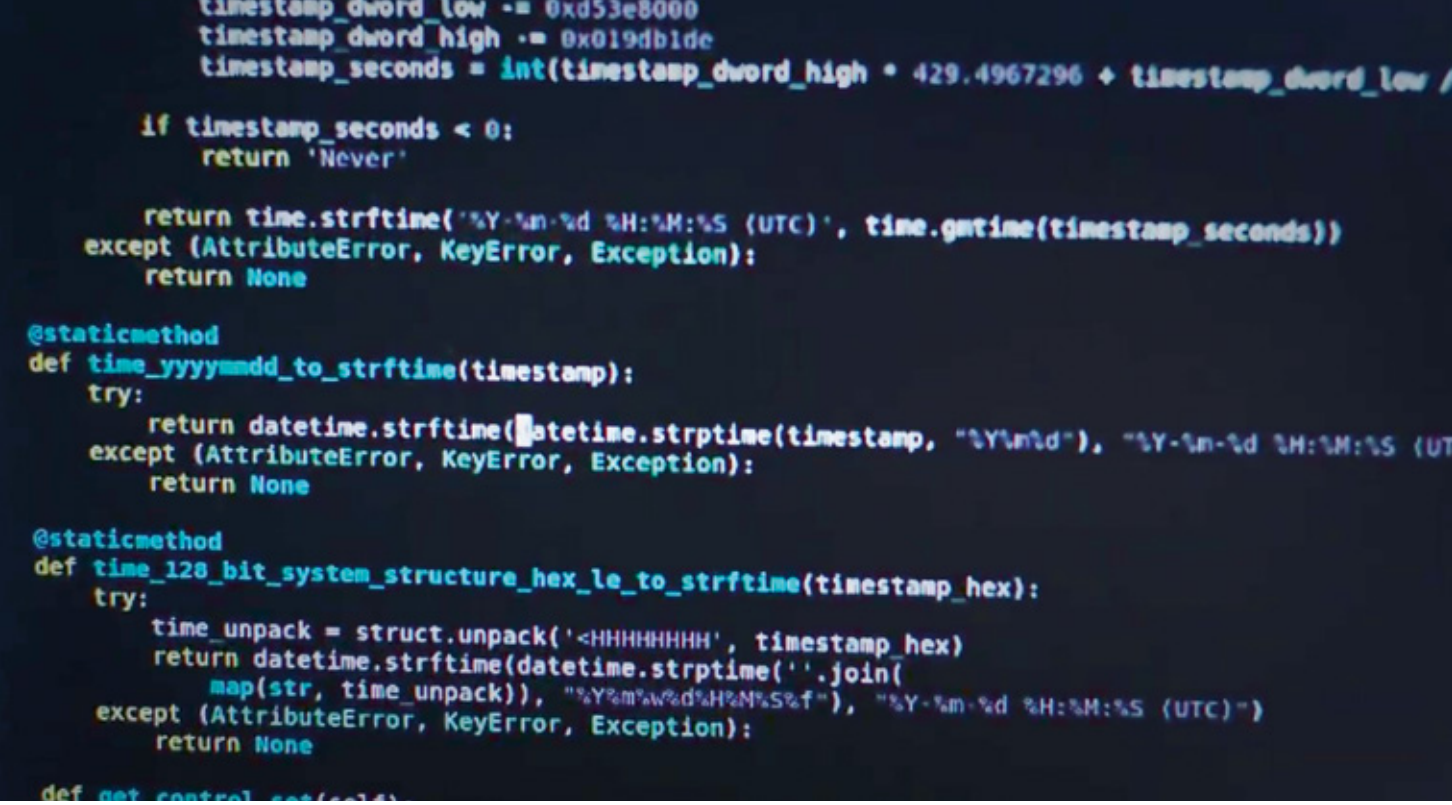
'Never get involved in a land war in Asia, never go against a Sicilian when death is on the line, and never hack the Dutch.'[1]

'Also never give them any excuse to hack you. Just don't f-ck with the Dutch in general.'[2]

Following on from the 2018 Defence Cyber Strategy, the Netherlands Defence Intelligence and Security Service (NLD DISS) and the Defence Cyber Command (DCC) have intensified their collaboration through the creation of cyber mission teams (CMTs). NLD DISS has been intensively engaged in conducting cyber operations for more than a decade, following the publication of the first Defence Cyber Strategy in 2012. Many successes have been achieved over that time and valuable lessons have been learned. These insights have highlighted the benefits of closer collaboration for the further operationalisation of the cyber domain by the armed forces. We would normally only be permitted to share details of our activities among a very select group of people since we are legally obligated to protect our sources and methods. Nevertheless, in this article we would like to share a number of NLD DISS's experiences with conducting cyber operations. As such, we are hoping to contribute to the discussion within the armed forces regarding the conceptual nature of cyber operations and the optimal organisational structure required for conducting them.

This article starts by presenting a number of insights gained from NLD DISS's intelligence-gathering cyber operations in recent years. Based on these insights, a number of implications for other types of military cyber operations are then identified. Finally, these insights and implications are used to outline the model for the new cyber mission teams (CMTs), in which NLD DISS and the Cyber Defence Command now collaborate on the basis of the 2018 Defence Cyber Strategy (DCS2018).
This article aims to highlight the central role played by covert intelligence activities in conducting all types of military cyber operations. We argue that the operational processes and options available are largely defined by the underlying intelligence and access positions.

However, we would like to emphasise that our assertion is not that the right model for all cyber operations lies solely with the intelligence perspective and the CMTs. On the contrary, we are extremely interested in other operational approaches to the cyber and information domains, such as those of the new Cyber and Electro-Magnetic Activities (CEMA) company [3] or the army's Land Information Manoeuvre Centre[4]. More such innovative perspectives are required in order for the armed forces to make optimal use of the many options offered by the



Access positions largely define the operational processes and options available for military cyber operations PHOTO WERKEN BIJ DEFENSIE

cyber and information domain. We believe that a normally closed organisation such as NLD DISS should also contribute to these perspectives.

Six insights from NLD DISS cyber operations

NLD DISS is authorised to penetrate automated devices, in other words to hack networks and systems, under Article 45 of the Netherlands Intelligence and Security Services Act 2017 (*Wet op de Inlichtingen- en Veiligheidsdiensten* 2017 – Wiv 2017), with the aim of obtaining and maintaining the right access to a target in order to fulfil an intelligence need, known as an access position. Such cyber operations are also referred to as Computer Network Exploitation (CNE). These cyber operations are conducted by multi-disciplinary NLD DISS intelligence teams that include personnel from the Joint Sigint Cyber Unit (JSCU), established jointly with the Netherlands General Intelligence and Security Service (NLD GISS). These cyber operations are part of an all-source intelligence process and may be supported with other general and special powers, such as the use of open sources, the deployment of agents and the placing of taps. NLD DISS conducts such operations in order to gather intelligence for investigation orders formulated by the government and the armed forces, and only conducts cyber operations with approval from the Minister of Defence and the independent Review Board for the Use of Powers (TIB) and under the supervision of the Review Committee on the Intelligence and Security Services (CTIVD). We will now present a number of insights that NLD DISS has gained from conducting these types of cyber operations over the years.

1. Cyber operations are always specific

Analogous to the assembly or readying of units for a mission, cyber operations require a solution that is tailored to the specific environment and characteristics of the target or the area of operations. As a general rule, there is no

1 Joseph Menn, 'Twitter Post', Twitter, 16 February 2021. See: twitter.com/josephmenn/status/1361744241291010048.
2 Andy Greenberg, 'Twitter Post', Twitter, 16 February 2021. See: mobile.twitter.com/a_greenberg/status/1361748350039646208.
3 Dutch Ministry of Defence, *Landmacht versterkt met cyber- en elektromagnetische capaciteit* press release dated 9 July 2021. See: https://www.defensie.nl/actueel/nieuws/2021/07/09/landmacht-versterkt-met-cyber--en-elektromagnetische capaciteit.
4 Dutch Ministry of Defence, *Land Information Manoeuvre Centre helpt Defensie anticiperen*, press release dated 16 November 2020. See: https://www.defensie.nl/actueel/ nieuws/2020/11/16/land-information-manoeuvre-centre-helpt-defensie-anticiperen.

CEMA exercise in Marnewaard. Multiple innovative perspectives are required for the armed forces to make optimal use of the many options offered by the cyber and information domains

PHOTO MCD, JARNO KRAAYVANGER

one-size-fits-all solution and no fire-and-forget cyber capabilities are available. A multi-role cyber capability that can be deployed anywhere in the world with small variations in payload is very rare in the cyber domain. This means, in fact, that every operation requires a specific and individually-tailored development process for the required capabilities and attack techniques.

Public debate and literature regarding cyber operations are often focused on specific exploits,[5] malware or other cyber capabilities or attack techniques, since these can be observed and investigated by third parties. In practice, however, such aspects actually only constitute a small part of a cyber operation. If the target is actually revealed to have used a vulnerable version of hardware, software or a service which can be penetrated by an existing capability or attack technique, this generally only works against a single aspect of a single defence shell in a single intermediary step towards a single target or group of targets. A specific cyber capability or attack technique must therefore usually be adapted or combined with a large number of other means, or must be developed from scratch. The notion of generic cyber weapons, which can be deployed against a large number of targets with limited modifications, is therefore largely incorrect and irrelevant in practice.[6]

5 An exploit is a possibility to exploit a software vulnerability

6 P.A.L. Ducheine, 'Defensie in het Digitale Domein' in Militaire Spectator 186 (2017) (4) 164; Thomas Rid and Peter Mcburney, 'Cyber-Weapons', in: *The RUSI Journal* 157 (2012) (1) 6-13; Dale Peterson, 'Offensive Cyber Weapons: Construction, Development, and Employment', in: *Journal of Strategic Studies* 36 (2013) (1) 120-124; E. Tyugu, Situation Awareness and Control Errors of Cyber Weapons, IEEE, 2013, 143-148; L. Arimatsu, A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations, IEEE, 2012, 1-19.

2. Cyber operations often require a complex indirect approach.

In many cyber operations you have to reach the primary target indirectly, via secondary targets,[7] since the primary target often cannot be approached directly. For example, the target may not be directly connected to the internet, or may be so well protected that no opportunity exists to access in that way. Sometimes it is simply the case that technical characteristics such as the IP address are initially unknown or because the precise identity of the target itself is not clear. Obtaining a single access position for gathering intelligence on a primary target, such as a hostile communication system, can thus require a whole host of individual all-source intelligence operations to be conducted against secondary targets. This need for an indirect approach and the fact that several sub-operations have to be combined often renders the operational process extremely complex.

3. Cyber operations are time-consuming

Just as a reconnaissance unit with an unmanned aerial vehicle (UAV) goes through a time-consuming readiness process involving the physical, conceptual and mental components, cyber operations generally also require a long preparation period. As part of such preparations, you have to explore the vulnerabilities in the target's networks and equipment, request the required authorisations, plan and carry out the technical operations, obtain and expand access positions and study the network's or system's configuration. You then have to figure out where the needle in the haystack is that makes the next step of the operation possible or fulfils the intelligence requirement. Due to the above-mentioned need for an indirect approach, this process often runs in parallel, against several targets at the same time.

The numerous steps in this process in combination with the above-mentioned specificity and complexity of cyber operations result in many interdependencies and operational obstacles that, almost by definition, lead to a substantial loss of time. There are always exceptions, though, and sometimes things can be dealt with very quickly if a solid base is already in place.

The notion of generic 'cyber weapons' is largely incorrect and irrelevant in practice

However, most cyber operations take months, if not years to be successfully concluded.

4. Cyber operations require permanently integrated work.

The integration seen at the staff level in mixed military units on missions is also required for conducting cyber operations. Planning, technology, execution and analysis are inextricably linked. For example, legal authorisation to hack on the basis of Article 45 of the Wiv 2017 can only be obtained and retained on the basis of a detailed knowledge of the target, the environment and full understanding of the available technical capabilities. The use of these special powers will only be authorised if the operation is as targeted as possible and the right balance has been struck between necessity, proportionality and subsidiarity. This requires close and intensive technical, analytical and operational collaboration between the departments involved during the planning phase of a cyber operation. This also means that the experience, creativity and long-term deployment of the personnel involved is crucial.

Successful cyber operations therefore rely on intrinsic, implicit knowledge that is only explicitly transferable to a limited degree. Such intrinsic, implicit knowledge includes experience with the historical configuration of the target network or system, the variable data flows within it, the digital behaviour of users,

7 In the Netherlands Intelligence and Security Services Act 2017 (Wiv 2017) this is referred to as a non-target or 'third party'.

the security measures in place within a system and the way in which users communicate.

5. Cyber operations always carry a high political risk factor

In cyber operations there is a high probability that the primary and various secondary targets are located in different places across the globe and use various global flows of communication. This is one of the reasons that multiple supporting cyber operations and other all-source intelligence operations are often conducted at the same time, in different geographical locations and therefore in different national jurisdictions. When hacking networks and systems of primary and secondary targets in various countries, the chance of an unintended spill-over effect is also omnipresent along with the possibility of our covert activities being discovered and digital collateral damage. Given that data and data traffic on the internet and within a target's networks and systems are easily logged and stored, cyber operations can be discovered long after they have concluded ('the internet does not forget').

An NLD DISS intelligence team operates globally in the cyber domain from within the Netherlands, but if discovered, NLD DISS and other Dutch interests can be attacked from anywhere in the world via the cyber domain. For all these reasons there is almost always an associated high politico-administrative risk factor that can appear anywhere in the world and far into the future.

6. Operating covertly is always a necessity

A strong correlation exists in cyber operations, as with some other intelligence sensors, between secrecy and effectiveness since successfully obtaining and maintaining an access position is only possible in practice when the target is unaware of it. An access position can therefore best be compared to a covert special operating forces (SOF) observation post watching a target, for example. If an access point is discovered, it can be relatively easily neutralised by a target.

The relationship between secrecy and effectiveness in a cyber operation or at a covert observation post differs from that of an intelligence sensor, such as a photo reconnaissance satellite or UAV, since adversaries can avoid such sensors by altering their physical movements, although they cannot usually simply disable them in peace time. Public effects can also be created with such intelligence sensors without this negatively impacting the effectiveness of the capability, for example by showing imagery intelligence (IMINT) at a session of the UN Security Council. Such a distinction between effectiveness and secrecy does not exist with cyber operations, since the distance between the intelligence sensor, the access position and the target is almost zero.

Maintaining secrecy is not only necessary for the success of a single current operation, but also for ensuring operational sustainability in the future by protecting your modus operandi. Untraceable or imperceptible operations are also required in order to keep the high politico-administrative risk factor manageable, both in the Netherlands and vis-à-vis foreign partners. Secrecy is therefore of vital importance for operating successfully in the cyber domain.

Seven implications for other military cyber operations

NLD DISS cyber operations are therefore often complex, tailored, time-consuming, politically sensitive and require permanent disciplinary integration and the use of secrecy. These characteristics are not only inherent to cyber operations intended for gathering intelligence (CNE operations), but also to other types of cyber operations targeting extensive or complex targets in various jurisdictions and conducted at distance over longer periods. These characteristics also largely apply to the Computer Network Attack (CNA) operations that fall within the objectives of the Defence Cyber Command. It is also expected that these insights are relevant for cyber operations focused on creating different types of military effects, such as hypothetical cyber-enabled information operations and psychological operations that the armed forces will possibly want to be able to conduct in the future. However, the implications

Obtaining a single access position that can gather information on a primary target may require a whole array of separate all-source intelligence operations on secondary targets

PHOTO: WERKEN BIJ DEFENSIE

of the above insights highlight that such cyber operations differ from traditional physical military operations in a number of crucial ways.

1. Cyber operations revolve around access positions

Just as with kinetic military operations, the effect is key, with the access position dictating the effects that can be achieved with cyber operations. Without access you can't do anything. Access positions are therefore an essential condition when employing cyber operations to achieve an effect. Such effects could include obtaining certain confidential military information from an adversary, deceiving an adversary, or releasing a destructive virus that wipes all the hard drives of an adversary's communication network, thereby rendering the adversary no longer capable of operating. As such, the right access position is key and defines and shapes an operation and dictates which affects can be achieved.

Consequently, offensive cyber operations are first and foremost intelligence operations that are aimed at covertly obtaining an access position. According to various cyber operation models, between 83 and 94 percent of a cyber operation consists of obtaining an access position (CNE operation).[8] The remaining 6 to 17 percent can be differentiated according to the

8 See: Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin, Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains (Washington, D.C., Academic Conferences and Publishing International Limited, 17-18 March, 2011); Marc Laliberte, 'A Twist on the Cyber Kill Chain: Defending Against a Javascript Malware Attack', Darkreading, 21 September 2016. See: www. darkreading.com/ attacks-breaches/a-twist-on-the-cyber-kill-chain-defending -against-a-javascript-malware-attack/a/d-id/1326952; Corey Nachreiner, 'Kill Chain 3.0: Update the Cyber Kill Chain for Better Defense', Helpnetsecurity, 10 February 2015. See: www. helpnetsecurity.com/2015/02/10/kill-chain-30-update-the-cyber-kill-chainfor-better -defense/; Blake D. Bryant and Hossein Saiedian, 'A Novel Kill-Chain Framework for Remote Security Log Analysis with SIEM Software', in: *Computers & Security* 67 (2017); MITRE, 'ATT&CK: Tactics', MITRE. See: www.attack.mitre.org/tactics/ enterprise/; Paul Pols, 'The Unified Kill Chain: Designing a Unified Kill Chain for Analyzing, Comparing and Defending Against Cyber Attacks', Cyber Security Academy, 2017.

desired effect, for example obtaining intelligence, disruption or manipulation (CNA operation).[9] Based on almost 10 years of cyber operations, NLD DISS concurs with these percentages.

2. Access positions are difficult to transfer

A dependence on intrinsic, implicit knowledge means that an NLD DISS intelligence team's CNE access position cannot simply be transferred to an effector wanting to conduct a CNA operation or to take over a CNE operation. The CMTs established under the DCS2018 are seen as a possible solution to this issue. Transfer is complicated however, since this is not a matter of handing over the log-in details and operation of a command and control server (C2 server) used by NLD DISS to penetrate a target network, for example. Such explicit information is only usable in combination with the implicit knowledge of the target and its environment acquired gradually over time. In such a case, the effector is familiar with how the target's network or system is configured and operates, has the necessary experience of covertly operating in this network and understands the wider context and the relationship of the target with secondary targets. Integrated cooperation is necessary for conducting successful future CNE and CNA operations.

3. CNA also requires covert operations

The need for operational methods that are both untraceable and undetectable also applies to those cyber operations intended to cause a noticeable effect, such as CNA. Such methods are even essential for the concept of loud cyber, which has been discussed in literature in recent years.[10] In loud cyber operations, an actor communicates their capabilities for generating an effect in a hostile network, or an actor assumes political responsibility for the effect of an operation. Alternatively, for example, a relatively open threat could be made that the vital infrastructure of another country has been hacked and could be sabotaged.[11] However, the covert nature of the modus operandi employed for obtaining the access position used remains crucial, even if a cyber operation is part of a relatively open military mission. If the direct adversary or a third party with strong SIGINT capabilities gains too much insight in the modus operandi used, this directly impacts the possibility of generating the announced effect, the operational sustainability of other simultaneous cyber operations and the execution of future cyber operations.

At first glance, Distributed Denial of Service (DDoS) operations appear to represent an exception to this rule since the penetration of a target's network or system to obtain an access position is not required. Instead, a target's website or internet connection, for example, can be rendered temporarily unusable by externally bombarding it with massive amounts of data traffic. DDoS operations can therefore be employed quickly and on an ad-hoc basis. However, in order to generate the amounts of data traffic required an actor must either hack a large number of systems of random third parties and bring them together in a botnet[12], or acquire these capabilities from criminal actors or force large telecommunication providers to cooperate. In other words: DDoS capabilities also rest on a number of access positions that must be established through covert intelligence operations.

4 Cyber operations require different planning cycles

In terms of time frame, conducting a complex cyber operation is comparable to conducting a complex long-term military operational deployment. Cyber operations do not have planning cycles equating to hours, days or

9 Pols, 'the Unified Kill Chain'.

10 See for instance: Max Smeets and Herbert Lin, 'Offensive Cyber Capabilities' (Tallinn, NATO CCD COE Publications, 10th International Conference on Cyber Conflict, 2018) 63; Max Smeets, 'The Strategic Promise of Offensive Cyber Operations', in: *Strategic Studies Quarterly* 12 (2018) (3) 100; Herbert Lin, 'Attribution of Malicious Cyber Incidents: From Soup to Nuts', in: *Aegis Paper Series* (2016) (1607) 44; Herbert Lin, 'Still More on Loud Cyber Weapons', Lawfareblog, 19 October 2016. See: www.lawfareblog. com/still-more-loud-cyber-weapons; Timothy M. Goines, 'Overcoming the Cyber Weapons Paradox', in: *Strategic Studies Quarterly* 11 (2017) (4) 86-111, 87-88; Nicole Softness, 'How Should the U.S. Respond to a Russian Cyber Attack?', in: *Yale Journal of International Affairs* 12 (2017) (Spring) 105.

11 David E. Sanger and Nicole Perlroth, 'U.S. Escalates Online Attacks on Russia's Power Grid', *The New York Times*, 15 June 2019.

12 A botnet is a group of hacked systems (bots) that an actor can control as a whole, for example to conduct a DDoS operation.

weeks. Following the time-consuming readiness and deployment process, a submarine can manoeuvre in an area of operations in a relatively short space of time and disable a range of targets there. In cyber operations, such deployment is barely conceivable. Cyber operations can only produce an effect in a time frame comparable to that of a readied and deployed physical weapons system when an advanced access position has already been achieved beforehand. However, the 'before the event' element is generally so time-consuming that this is better compared to the execution of the logistical, legal and operational planning and training process that starts months in advance of getting the submarine into the area of operations at the right time.

The covert nature of the modus operandi used for gaining access positions remains crucial.

5. Cyber operations exceed normal military mandates

The above-mentioned implications mean that cyber operations, in terms of both time and space, can best be compared with a complex long-term military operational deployment, such as a multi-year Article 100 mandate.[13] It is indeed necessary to start building up the right access positions well in advance. Given that this concerns an intelligence operation, this is currently only possible under the Intelligence and Security Services Act 2017 (Wiv). For the rest of the armed forces covert operations are possible during a military operation, for example under Article 100 or through the Ministerial Core Group on Special Operations (MSKO) procedure.[14] However, in the current legal context, the structural and global deployment of the types of special powers that a cyber operation requires is still the remit of NLD DISS.[15]

It is therefore an operational reality that, in the current legal context, obtaining and maintaining the CNE access positions required to generate a military CNA effect is only possible for NLD DISS under the Wiv 2017.

6. Traditional levels of warfare are of limited relevance in cyber operations

21st century military doctrine has institutionalised the use of the Napoleonic military levels of warfare and has added the operational level.[16] As encompassed in the controversial but much used concept of the strategic corporal,[17] the categorisation of military activities according to level of warfare, under pressure from technology, has become increasingly complicated (strategic compression). It is therefore often problematic to distinguish between a defined, autonomous 'strategic' cyber

13 Article 100 of the Constitution of the Kingdom of the Netherlands, 24 August 1815; Article 51 of the United Nations Charter; Article 5 of the North Atlantic Treaty.

14 P.A.L. Ducheine and K. Arnold, 'Besluitvorming Bij Cyberoperaties', in: Militaire Spectator 184 (2015) (2).

15 The mandate of a military operation is in any case geographically limited.

16 Ministry of Defence, Netherlands Defence Doctrine (The Hague, Ministry of Defence, 2019) 27-33; Martin Dunn, 'Levels of War: Just a Set of Labels?'. See: www.clausewitz.com/readings/Dunn.htm; Larence M. Doane, 'It's just Tactics: Why the Operational Level of War is an Unhelpful Fiction and Impedes the Operational Art', Small Wars Journal, 24 September 2015. See: www.smallwarsjournal.com/jrnl/art/it%E2%80%99s-just-tactics-why-the-operational-level-of-war-is-an-unhelpfulfiction-and-impedes-the

17 Charles C. Krulak, 'The Strategic Corporal: Leadership in the Three Block War', in: *Marines Magazine* (1999); Franklin Annis, 'Krulak Revisited: The Three-Block War, Strategic Corporals, and the Future Battlefield', Modern War Institute, 3 February 2020. See: https://mwi.usma.edu/krulak-revisted-three-block-war-strategic-corporalsfuture-battlefield/; Walter Dorn and Michael Varey, 'Fatally Flawed: The Rise and Demise of the "Three-Block War" Concept in Canada', in: International Journal 63 (2008) (4) 967-978.

PHOTO MCD, JASPER VEROLME

Cyber operations can only be understood in terms of geography or chronology to a limited extent

operation on the one hand, and an 'operational' or 'tactical' cyber operation on the other, the responsibility for which can be delegated to a lower command and control level. In practice, the types of cyber operations that we deal with here are mostly operating on all three levels at the same time, being conducted remotely, in multiple jurisdictions, for long periods of time and against large or complex targets. The distinction between levels loses a lot of its meaning as a result.[18] As mentioned above, these types of cyber operations can also only be categorised in terms of geography or chronology to a limited extent. Consequently, military doctrinal constructs that define military activities in terms of time and space, and therefore also division into levels of warfare,[19] are often meaningless in the context of such cyber operations. In order to successfully integrate cyber capabilities in the armed forces, the idea of using levels of warfare as an organisation model must be abandoned where necessary.[20]

7. Cyber operations are not a silver bullet

Finally, the insights gained by NLD DISS constitute a warning against unrealistic expectations. Almost

18, This geographical delineation affects the the international law discussions around sovereignty, see for example: Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge, Cambridge University Press, 2017) 11-27.

19 Royal Netherlands Army Doctrine, Doctrine Publication 3.2: Land operations (Amersfoort, Land Warfare Centre, 2014) 6-21 to 6-27.

20 There is also the question of precisely how the cyber operations of the CEMA company of the army compare to the types of cyber operations conducted by NLD DISS.

every aspect of our society is digitalised, and therefore, according to Hypponen's law, everything is theoretically also vulnerable. 'Whenever an appliance is described as being smart, it's vulnerable'.[21] In practice, however, there is a direct relationship between the target's accessibility and quality of security on the one hand, and the time and effort required to penetrate it on the other. The most attractive targets for cyber operations,[22] such as weapons and C4ISR systems, but also vital infrastructure, are in practice often not directly accessible since they are very well secured and have a very obscure internal functioning, requiring significant time and effort to obtain the required access positions to be able to attack them. Cyber operations are not cost-efficient for some targets, since the capabilities and operational options required are simply not there.

Four advantages of integrated cooperation

In the DCS2018 a new cooperation model was chosen in which both NLD DISS and DCC would be better positioned to fulfil their roles. Conceivable military cyber operations after all demand a different set of characteristics from the organisational structure, since they are defined to a large extent by the underlying access positions, must mostly be conducted covertly, have different planning cycles and exceed traditional geographical and chronological mandate frameworks. In addition, the required implicit knowledge is not easily transferable from the intelligence component to the executing component.

The integration model of the CMT reflects these characteristics and therefore makes the timely delivery of the requested digital striking power significantly more realistic. By forming a CMT in which the operational capability of the DCC is brought together with the NLD DISS intelligence team, the CNE operation for obtaining an access position for a CNA operation can occur in an integrated manner. Figure 1 describes this process. This model also makes consistently sound legal safeguarding possible, since obtaining and maintaining the all-important access positions takes place under the Wiv 2017 and therefore under regulatory oversight. Below, we identify four advantages made possible by the CMT collaboration model.

1. Realistic preparation times
Through implementing the CMT collaboration model, the military CNA effects required by the armed forces, such as attacking C4ISR-systems and weapons systems, can be generated from access positions that are obtained well before a mission. This can happen only on the basis of joint CNE operations under the Wiv 2017. The 'offensive component' is limited to the phase in which the CNA effect is actually generated: the previously mentioned differentiation phase that covers 6 to 17 percent of a cyber operation. The integrated team must then fall back on the Intelligence and Security Services Act 2017 (Wiv) given that the battle damage assessment (BDA) of a CNA operation can probably only take place from access positions obtained by CNE operations under the Wiv.

2. Integration in military planning
In this collaboration model, desired military cyber effects can be translated into intelligence requirements by the Chief of Defence (CHOD) at the earliest possible stage and through the proper procedures, which can then be included in the multi-year operational planning of both NLD DISS and DCC. An integrated CMT from NLD DISS and DCC then work with a planning element, at an early a stage as possible together with the CHOD, so that the expected cyber effect can then actually be integrated into the military planning.

21 Mikko Hypponen, 'Hypponen's Law', Twitter, 12 December 2016. See: twitter.com/mikko/status/808291670072717312.

22 Dutch Ministry of Defence, 'NAVO-Top: Nederland Nog Altijd Achter Halen 2%-Norm', Dutch Ministry of Defence, 11 July 2018; Marno de Boer and Kristel van Teeffelen, 'Een Brug Kun Je Hacken in Plaats Van Bombarderen', Trouw, 25 March 2017; Dutch Ministry of Defence, 'Defensie Vergroot Slagkracht Tegen Cyberdreiging', Dutch Ministry of Defence, 12 November 2018

Far-reaching strategic cooperation between DCC and NLD DISS is the best way forward for offensive digital striking power.

3. Integral experience and knowledge building
Collaboration between NLD DISS and DCC in fully integrated CMTs under the mandate of the Wiv 2017 represents a solution to the physical, cultural and organisational hurdles and institutional distance between DCC and NLD DISS. Through fully integrated collaboration, the required intrinsic, implicit knowledge of an access position is built up at both NLD DISS and DCC. The personnel from DCC provide a meaningful contribution not only during but also before and after a military cyber operation.

4. Reinforcing digital striking power
Fourth, intensified cooperation between DCC and NLD DISS increases available cyber capabilities within both DCC and NLD DISS. The result of such integration is greater than the sum of its constituent parts. Above all, DCC can thus generate military cyber capabilities and digital striking power for the armed forces as a whole. It also better positions NLD DISS to carry out its investigation orders.

Conclusion

Given the insights gained from NLD DISS's above-mentioned experiences and their implications for other military cyber operations, the joint DCC-NLD DISS CMTs are a step in the right direction, offering significant advantages. CMTs are not the best solution in our opinion, but are the only option within the current administrative context of the DCS2018. The integration model of the CMT embraces the inherent characteristics of the cyber domain, rather than using traditional organisational structures. Far-reaching strategic cooperation between DCC and NLD DISS is the best way forward to generate the desired offensive digital striking power for the armed forces. For example, DCC can contribute to obtaining access positions through CNE operations which it will later require during deployment for SOF to generate effects in or via cyberspace. Furthermore, we see no inherent reason why this collaboration model should not also be possible for other parts of the armed forces, such as SOF or JISTARC units.

This is based on the assumption of our own strength and a solution that is tailored to the specific Dutch context. We have consciously chosen not to implement organisational or collaboration models used in other countries. This does not alter the fact, however, that the allies that the Netherlands mirrors follow a collaboration model in which cyber commands are almost fully integrated into the respective intelligence or security services. In other words, they collaborate on an even deeper level than the CMT collaboration model.

In the Netherlands, the institutional distance between the CNE and the CNA components of offensive digital striking power is greater than in any other country in the world, and that includes allies and adversaries. The Netherlands is currently one of the most progressive and advanced countries in the world in other cyber security areas, such as promoting private-public cooperation, contributing to the development and advancement of an international normative framework, and delivering cyber intelligence.[23] This is largely thanks to the Netherlands' characteristic pragmatism, realism and focus on operational effectiveness.

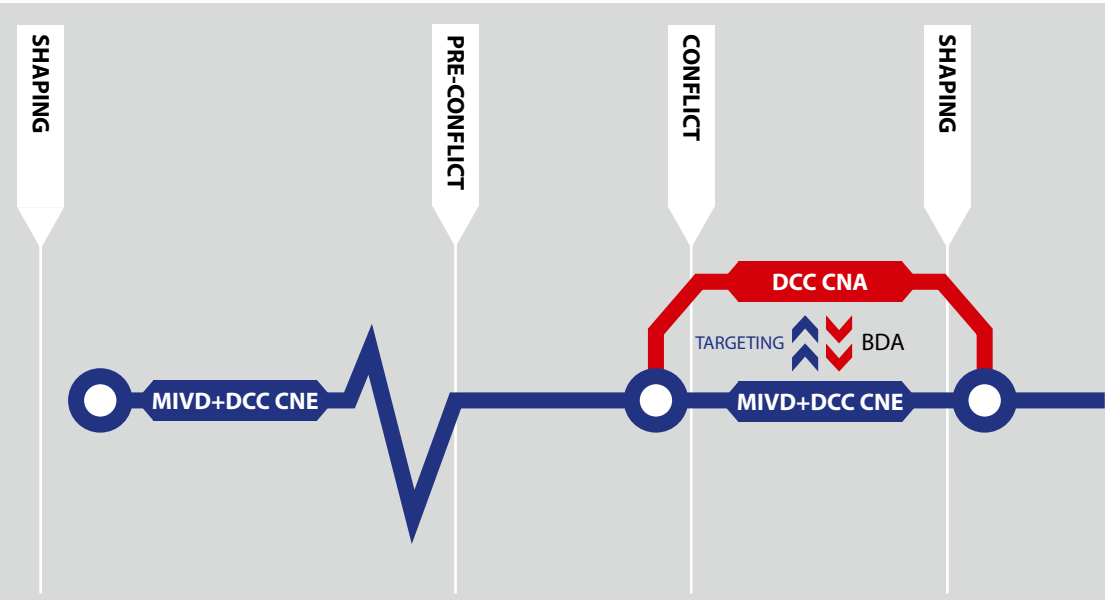


Figure 1. This is the suggested collaboration model in which NLD DISS and DCC jointly prepare CNE operations in a CMT before, during and after a conflict to support operations, including CNA operations carried out by DCC. In the framework of the CMT's ongoing CNE operations, options are developed for CNA operations to be executed by the DCC component in the integrated team during a possible conflict. If the CNA operation exceeds the Wiv mandate, the CNA operation is conducted under a Chief of Defence (CHOD) mandate. The implicit intrinsic knowledge for targeting purposes stems from the CMT's CNE operations and feeds the CNA operations. After all, these are conducted by the same personnel who set up the CNE operation together. The battle damage assessment (BDA) after the CNA operation is most probably carried out by the CMT in charge of CNE operations.

The CMT collaboration model from the DCS2018 aims to reach this level in relation to the generation of offensive digital striking power as well. Reducing the institutional distance between NLD DISS and DCC by developing and implementing integrated CMTs could occur more quickly and more intensively. We need the entire armed forces for this. Both DCC and NLD DISS are partially made up of personnel from the Operational Commands. In order to let go of traditional frameworks and to make a success of the CMTs, an understanding of the developments and insights on which the DCS2018 was based is required. This article aims to contribute to that understanding and to the further conceptual discussion within the armed forces so that DCC and NLD DISS can further focus on what must ultimately be the highest priority for the armed forces, the Netherlands and our allies: operational effectiveness and digital striking power in the cyber domain. ■

23 'The Hague Program for Cyber Norms', The Hague Program for Cyber Norms See: www.thehaguecybernorms.nl/about-us; Schmitt, Tallinn Manual 2.0, 2-6; 'Bevelhebber Krijgsmacht: Nederland in Champions League Cyberwereld' Security.nl, 9 December 2019. See: https://www.security.nl/posting/634606/ Bevelhebber+krijgsmacht%3A+Nederland+in+Champions+League+cyberwereld; Huib Modderkolk, *Het is Oorlog Maar Niemand Die Het Ziet (There's a war going on but no one can see it)* (Amsterdam, Podium, 2019)