Volume 191 issue 9 - 2022

MILITAIRESPECTATOR

FOG OF WAR 2.0

SPECIAL EDITION ABOUT NLD DISS

- Interview with CHOD and Director of NLD DISS: 'No security without intelligence'
- The future of NLD DISS
- The military intelligence service and its clients
- NLD DISS cyber operations: all about access
- History of the Netherlands military intelligence and security service(s) 1912-2022

PHOTO MCD, SJOERD HILCKMANN

The October 2022 edition of *Militaire Spectator* includes: 'Task Force Disaster Relief Bahamas. Zes inzichten voor toekomstige militaire noodhulpoperaties' [Six insights for future military emergency relief operations] by J.P. Kalkman.
After Hurricane Dorian had left a trail of destruction across the Bahamas in September 2019, the Netherlands sent help to the islands. The Task Force Disaster Relief Bahamas on board the HNLMS Snellius and HNLMS Johan de Witt consisted of an operational staff (NLMARFOR), a marine corps unit, an engineering unit, two Cougar helicopters, military personnel from the 1 CMI Commando and French and German units. During the emergency relief operation, relief supplies were delivered, fuel was transported, debris was cleared and a bridge and buildings were repaired. Over a period of ten days, approximately 650 military personnel were actively involved in the deployment.
A further study of the emergency relief operation shows that the Task Force was enormously adaptive. The structure and working method set up in advance proved to be incompatible with the local situation on a number of points, with plans quickly proving untenable, protocols too cumbersome and secure means of communication too slow. Within a short period of time, all sorts of organisational and operational changes were implemented to enable more rapid and effective operations. It is useful to learn from these experiences so that the unique requirements of emergency relief operations can be taken into account in advance for future deployments. ■

THE NETHERLANDS JOURNAL OF WAR STUDIES: CALL FOR PAPERS

This year the *Militaire Spectator* publishes a special edition (open access) focused on the future of war studies. The articles received will be submitted to a process of blind peer review. The deadline for submitting papers is 15 September 2023. For more information visit the *Militaire Spectator* website: www.militairespectator.nl.

Peering through the fog

Weapons are fired and targets are struck, causing smoke clouds, clamour and chaos and a resultant breakdown in communications and loss of oversight. Despite meticulous planning and preparation, it is the 'friction' inherent in the fog of war that dictates the course of every battle.[1] The same is true in our digitalised world, where uncertainty and ambiguity caused by digital noise, perceptions and deceptions have become increasingly crucial instruments of war. The possibilities offered by the internet, social media and ongoing technological developments have changed society and the battlefield of the 21st century.

Secrecy constitutes part of this friction. It is used to dissipate the fog and achieve victory, but also to wrong-foot adversaries. An organisation such as the Netherlands Defence Intelligence and Security Service (NLD DISS) is only too aware of this paradox, operating as it does in a democratic society where both privacy – or personal secrets – and transparency are of paramount importance. Secret services are tasked with protecting these crucial democratic triumphs. However, due to the nature of their activities they may be forced to violate this very privacy while sometimes failing to provide the required degree of openness.[2]

Since the outbreak of the war in Ukraine, the use, importance and necessity of intelligence to support national and international security have been at the forefront of everyone's thoughts, reinforced by the unprecedented disclosure of classified information in the months prior to the dropping of the first Russian bombs. But such disclosure cannot entirely dispel the secrecy in which intelligence is shrouded. Both military personnel on the physical and digital battlefields and civilians on the sidelines continue to peer through the fog. Correct and reliable information appears to be becoming increasingly scarce. More than ever, digital friction is becoming a part of the battlefield and contributing to the fog of war 2.0.[3]

In this special edition of *Militaire Spectator*, NLD DISS aims to dissipate some of the fog enshrouding its activities. Despite the limitations that it is faced with, it contributes to transparency by examining aspects of military intelligence and security. The authors discuss the historical development of the service and its predecessors, its future, cyber operations and intelligence, and the relationship between the producers and recipients of military intelligence. In a unique double interview, the CHOD and the Director of NLD DISS also discuss at length the current and future relationship between the service and the armed forces. ■

1 'Friktion ist das einzige Begriff (...) was den wirklichen Krieg von dem auf dem Papier unterscheidet', Carl von Clausewitz, *Vom Kriege* (Berlin, 1832).

2 Dennis Broeders, *Het geheim in de informatiesamenleving* (The Hague/Rotterdam, 2015); Paul Frissen, *Het geheim van de laatste staat*. Kritiek van de transparantie (Amsterdam, 2016).

3 Maarten Katsman, 'Fog of War 2.0. 20 jaar MIVD: Wat nieuwe ontwikkelingen vragen van inlichtingen- en veiligheidsdiensten', *See: www.militairespectator.nl, 30 June 2022*.

KVBK
KONINKLIJKE VERENIGING
TER BEOEFENING VAN
DE KRIJGSWETENSCHAP

PUBLISHER
Royal Netherlands Society for War Studies (KVBK)
www.kvbk.nl
E info@kvbk.nl
facebook.com/KVBKsecretaris
twitter.com/kvbk1

Secretary and membership records
Major R. Verheijen
E secretaris@kvbk.nl
Netherlands Defence Academy (NLDA)
Section MOW (Military Operational Sciences)
KVBK membership records
P.O. Box 90002, 4800 PA Breda
E ledenadministratie@kvbk.nl

Netherlands Institute for Military History (NIMH)
P.O. Box 90701
2509 LS The Hague
T 070 – 316 51 20
E redactie.militaire.spectator@mindef.nl
www.militairespectator.nl
facebook.com/militaire-spectator
twitter.com/milspectator

Militaire Spectator is a member of the European Military Press Association

SUBSCRIPTIONS
Netherlands €30.00
Students €22.50
Additional fee abroad €5.00

DESIGN
Coco Bookmedia

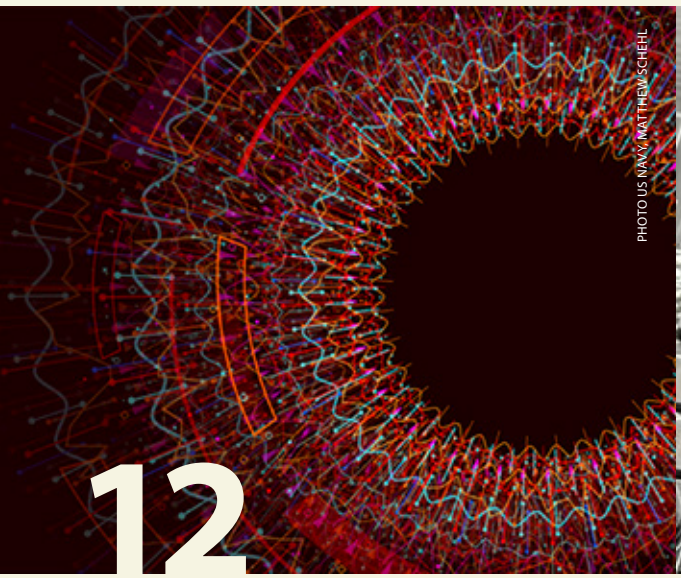
PRINTING
Wilco Meppel
ISSN 0026-3869

Cover photo: US marines training in a building
Photo: Shutterstock

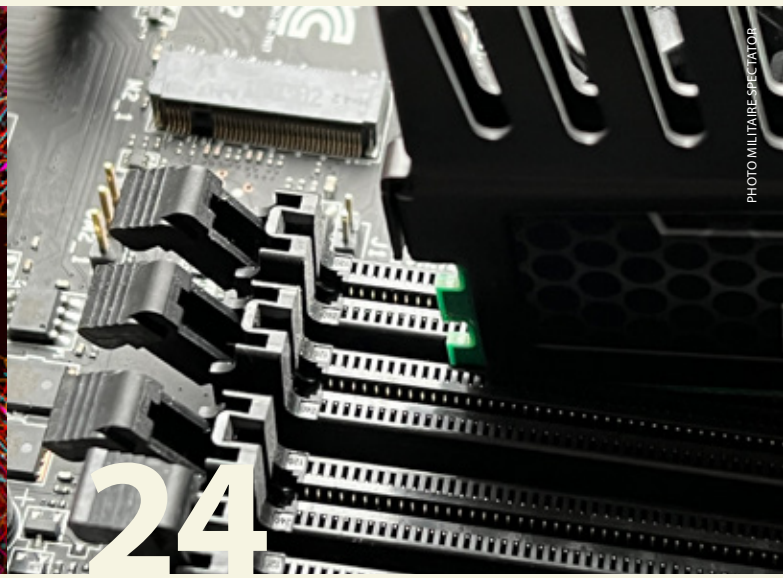

PHOTO HERMAN ZONDERLAND

MILITAIRESPECTATOR

VOLUME 191 ISSUE 9 – 2022



12



24

The future of NLD DISS

Bas Rietjens

In determining its policy for the future, NLD DISS should focus on adaptability, with complexity, open sources and data-driven working being the key elements.

All about access

Anonymous

Far-reaching strategic cooperation between the Netherlands Defence Cyber Command and NLD DISS is the best way forward to generate the desired offensive digital striking power for the Dutch armed forces.

46

Frustrated and fulfilled ambitions

Bob de Graaff

The maturation process for the Netherlands Defence Intelligence and Security Service and its predecessors has been a lengthy one, albeit not due to a lack of ambition.

AND MORE

‘No security without intelligence’

Interview with CHOD Onno Eichelsheim and Director of NLD DISS Jan Swillens

The Netherlands Defence Intelligence and Security Service (NLD DISS) has existed for 20 years in its current constellation. A recent seminar organised by NLD DISS highlighted the fact that the environment in which the service operates has not remained static.[1] Whereas in the past the work was carried out by ‘men in trilby hats hiding behind newspapers with eyeholes’, today the emergence of the internet and cyberspace has thoroughly transformed the way in which NLD DISS operates and expanded its options. In an interview with the Dutch military journal *Militaire Spectator,* Chief of Defence General Onno Eichelsheim (previously Director of NLD DISS) and the current Director of NLD DISS, Major General Jan Swillens, reflect on the field of intelligence, the threat landscape and a stronger J2 construction for the armed forces that would enable NLD DISS to respond more adequately to requirements at the operational-tactical level.

Alexander Claver, Peter Pijpers and Frans van Nijnatten

MS: The military confrontation in Ukraine appears to reflect the changing nature of warfare, with information and intelligence playing a highly prominent role, not only as a means of gaining insight into the enemy’s location and the situation on the battlefield but also as weapons, as evidenced by the narratives propagated by Russian media channels such as RT and Sputnik. How do we assess the changing nature of warfare, or is it simply a question of old wine in new bottles?

General Eichelsheim: It is true that 25 years ago the conflict in Ukraine would have been conducted differently, including the actions leading up to it. The Russian Federation may still be employing conventional assets, but it also

1 Maarten Katsman, ‘Fog of War 2.0 – 20 jaar MIVD: Wat nieuwe ontwikkelingen vragen van inlichtingen- en veiligheidsdiensten’. See www.militairespectator.nl, 30 June 2022.

General Onno Eichelsheim

General Onno Eichelsheim was appointed Chief of Defence (CHOD) on 15 April 2021 after serving as Deputy CHOD, and prior to that as Director of the Netherlands Defence Intelligence and Security Service (NLD DISS). As Deputy CHOD he was a member of the Cyber Security Council, the independent strategic advisory body that advises the Dutch government on cyber security in the Netherlands. Onno Eichelsheim has worked for the Netherlands Ministry of Defence since 1986.

Major General Jan Swillens

Major General Jan Swillens was appointed Director of NLD DISS in June 2019. NLD DISS gathers and analyses intelligence in order to ensure the safety of the Netherlands and its armed forces. Its tasks are laid down in the Intelligence and Security Services Act 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017* – Wiv 2017) and the Security Screening Act (*Wet veiligheidsonderzoeken* – Wvo). Jan Swillens has worked for the Netherlands Ministry of Defence since 1985, during which time he also served as Commander of the Commando Corps.

PHOTO HERMAN ZONDERLAND

CHOD Onno Eichelsheim (right) and Director of NLD DISS Jan Swillens

went through a process of using rhetoric to prime its own people for war. This process began more than a year ago, and for me it is a perfect example of the role that information and the information war played in the run-up to the conflict and how a hybrid war is ultimately waged.

Prior to the outbreak of the war, the West also employed intelligence capabilities to release information designed to negate the disinformation spread by the Russians and to reveal what the Russians were capable of and what their plans were. All the while the Russians were saying that they had very good reasons for engaging in the conflict and that they were only using lawful weapons. In a certain sense this is indeed old wine, since information-based manoeuvring has always existed. But the difference is that many more channels are available today.

In the current phase of the conflict, it is vital for Ukraine's President Zelensky that he can continue to spread his message within Ukraine and to the international community through social media and other communication channels. Communication and information play an extremely important role in gaining international support.

Cyber activities obviously also play a part in the context of hybrid warfare, although it is clear that the Russians' actions in the run-up to the war were not very successful.

The confrontation in Ukraine demonstrates how war can be waged in various domains, including the information domain. Our strength lies partly in the fact that we can release intelligence in the public domain in order to rebut an opponent's message to some degree. In any case, this conflict will teach the Russian Federation that it needs to greatly improve its integrated use of the various domains and to time the associated phases more effectively.

MS: Has it also taught the West anything? The Russian message appears to be catching on in Africa and Asia.

General Eichelsheim: There is so much more to be gained in this respect. The West takes the moral high ground and eschews manipulation. We must try to negate disinformation, but that is difficult if we do not follow the example of countries like the Russian Federation and China by combining these efforts with the use of other instruments of power such as economic or diplomatic support, which can for example be offered to an African country to ensure its backing in a subsequent quest. We are aware of this phenomenon, but are not yet addressing it sufficiently, and that could harm us in the long run. Western countries therefore need to employ all their capabilities to counter certain messages – of course doing so not as oppressors or 'colonists' and in a different manner than autocracies – otherwise we will eventually lose the battle.

MS: The 21st century information revolution (internet, social media, low-cost accessibility of bulk data) has yielded new types of capabilities. We are faced with threats from cyberspace. Have NLD DISS's work and modus operandi recently changed as a result?

Major General Swillens: NLD DISS has always been an all-source service. There are many ways of acquiring information and there is enormous strength to be had from incorporating all these processes under one roof. For example, we still conduct high-frequency interceptions, which is a crucial old-school capability. However, in recent years new elements have emerged as powerful drivers of NLD DISS's development, such as cyberspace, cable interception, open-source intelligence (OSINT) and international cooperation. With regard to the latter, digital threats are borderless, and no single country can combat them independently. We often speak of quid pro quo, but in my experience true international cooperation, for example in the area of digital threats, is based on trust.

It is important to focus on quality, since the emergence of the digital domain has brought new threats that target the vulnerabilities of the Dutch knowledge and digital infrastructures. Given the rapid rate of developments, quick action is more vital than ever.

In the grey zone between war and peace, attackers can operate below the threshold of physical armed conflict, but the effects of their actions could still harm another country. The digital domain underscores the importance of NLD DISS as an intelligence *and* security (I&S) service, since there can be no security without intelligence.

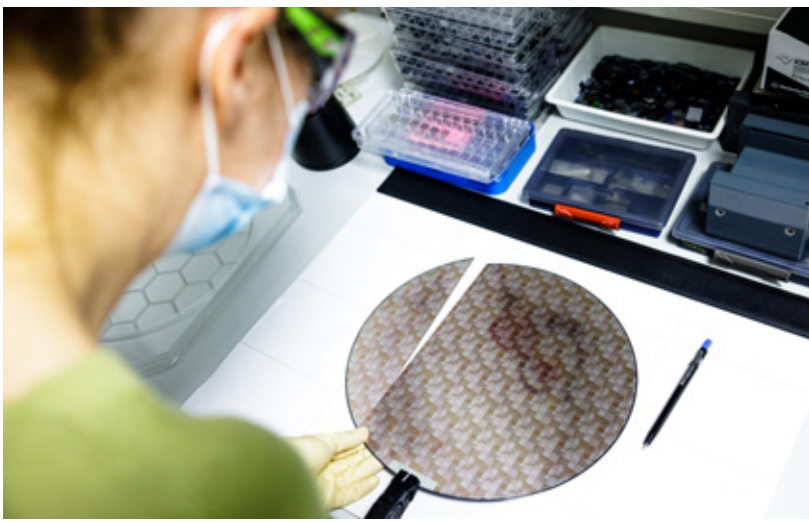
General Eichelsheim: Cooperation between the Defence Cyber Command (DCC) and NLD DISS could be better. Synergy could certainly be amped up, particularly to enable rapid and effective action in the cyber domain, where no distinction is made between the strategic, operational and tactical levels. Offensive operations in cyberspace must align with the focal areas identified by NLD DISS. But the CHOD will remain responsible for the employment of cyber capabilities.

Major General Swillens: The DCC and NLD DISS each have their own roles, tasks and responsibilities in the digital domain. These require a legal framework and a definition of what we are aiming to achieve. For example, the DCC has been commissioned by the CHOD to create military cyber effects and it also formulates the effects that we, on our part, wish to prevent. This is a different approach than viewing the cyber domain from an I&S perspective.

General Eichelsheim: Although a new phenomenon for the Netherlands, we find ourselves participating in a 24/7 strategic contest mainly taking place below the threshold of armed conflict. In the cyber domain, too, we need to decide what action to take in this contest and what effects we aspire to achieve. Intrinsically, we do not always want to achieve a military effect and must decide who is responsible for the application of these effects. A structure in which the DCC acts exclusively in the context of war and armed conflict is no longer appropriate. We are now exploring how we can better equip ourselves for the contest so that we can emerge as victors when appropriate.

MS: Economic security was not a focal point for the Defence organisation a few years ago, but it clearly is today. Is this an example of the shifting threats that have been mentioned, the key words being China and knowledge position?

PHOTO EUROPEAN UNION



In terms of chip technology, the Netherlands is having to deal with countries that launch offensive programmes in a bid to steal Dutch know-how in this field.

Major General Swillens: Certainly! Economic security is directly linked to national security. Consider, for example, the microchips used in weapons systems to render them faster and more efficient than those of our adversaries. Chip technology is the most obvious example, and the Netherlands ranks at the top in terms of companies and knowledge institutions in this field. We must protect this industry, since we are dealing with countries that have set up offensive programmes aimed at obtaining our know-how through hacking but also by 'buying off' people who possess such knowledge. The government may also request information from NLD DISS concerning export controls for other technologies. For example, it may wish to know the likelihood of Dutch technology ending up in the possession of another country's defence industry.

MS: The Netherlands has other entities that actively protect against influencing via the information environment. These entities include the Netherlands General Intelligence and Security Service (NLD GISS), the National

'Real-time answers are impossible to provide, but we need to generate answers increasingly quickly'

Coordinator for Security and Counter-Terrorism (NCTV), the National Cyber Security Centre (NCSC) and the DCC. How does NLD DISS collaborate with these entities, and has a role division of sorts been agreed?

Major General Swillens: Everything is based on the interest-threat-resilience triangle. The government begins by defining what we wish to protect. Next, NLD DISS and NLD GISS compile threat assessments and analyses. The NCTV is tasked with coordinating responses to these threat assessments and formulating resilience measures. We cooperate smoothly in this area, as evidenced for example by the report compiled jointly by the services and the NCTV entitled 'State actors – threat assessment' ('Dreigingsbeeld statelijke actoren').[2]

MS: Should the NCTV be granted the powers held by NLD GISS or NLD DISS?

Major General Swillens: The NCTV mainly acts as the central coordinator of courses of action by specific departments. I believe that this collaboration is currently organised clearly and effectively. It is vitally important that the right information and the right analyses arrive at the right place in a timely manner. This information sharing is efficiently organised in the Netherlands. Intelligence and security are no longer the sole territory of the Ministries of the Interior and Kingdom Relations; Justice and Security; Foreign Affairs; and Defence, and increasingly involve other parties including the Ministries of Economic Affairs and Climate Policy; Education, Culture and Science; and Infrastructure and Water Management, for example.

General Eichelsheim: The phenomenon analyses conducted by the NCTV[3] sometimes raise the question of whether the NCTV is not in fact an intelligence service. The purpose of phenomenon analyses is to identify societal trends that affect national security. The NCTV identifies these trends on the basis of analyses conducted by NLD GISS and NLD DISS. If the NCTV were to collect and process intelligence itself, it would indeed be the third service, a situation that would be undesirable under the current legal system.

MS: There is an increasing demand for real-time answers in the intelligence field. Are we capable of providing answers in real time? Are the recipients of intelligence aware of this?

General Eichelsheim: As former director of NLD DISS I know how much time it costs to compile a good analysis. It is important to process and analyse data rapidly. Real-time answers are impossible to provide, but we can and must generate our answers increasingly quickly.

Major General Swillens: An intelligence and security service should never speculate, nor should it make predictions. We assess whether a scenario is more or less probable, and this requires careful analyses that are regularly updated. At the same time there is a huge need for rapid assessments in the information society in which we live. When the attack on the shopping centre in Kremenchuk [Ukraine, 27 June – ed.] occurred, NLD DISS was expected to state within the hour whether it was a Russian attack, whether it had deliberately targeted civilians, etcetera. The risk involved in making hasty assessments is that any subsequent incorrect attribution will erode confidence in the service. If, for political or other reasons, a decision is taken to issue information very quickly after all, NLD DISS will always be extremely clear as to its information position and the degree of credibility it assigns to its assessment or conclusion. And because the service provides reliable situational pictures, these days it is also involved in consultations to discuss courses of action.

2 NLD GISS, NLD DISS, NCTV, 'Dreigingsbeeld Statelijke Actoren', 2021. See https://www.rijksoverheid.nl/documenten/rapporten/2021/02/03/ dreigingsbeeld-statelijke-actoren.

3 See for example, Phenomenon analysis 'The different faces of the corona protests'. See https://www.nctv.nl/documenten/publicaties/2021/04/14/ fenomeenanalyse-de-verschillende-gezichten-van-de-coronaprotesten.

General Eichelsheim: The scenarios compiled by the service show clearly which indicators we should or should not respond to. These assessments are useful when considering courses of action.

MS: Operational units have recently been partially and temporarily assigned to NLD DISS to meet the armed forces' need for operational and tactical intelligence more effectively. In order to serve the CHOD, the J2 cell will also be strengthened and expanded to provide additional direction to ensure that the various branches of the armed forces receive the operational and tactical intelligence that they require. How do you view this?

General Eichelsheim: In the current situation the armed forces cannot gather intelligence without an explicit mandate. However, when the armed forces are deployed or are preparing for a specific operation they have more powers, provided these are laid down clearly in a UN or NATO mandate supported by an Article 100 letter. In these cases it is advisable to make such preparations in accordance with the Wiv and in line with instructions issued by myself in consultation with the Director of NLD DISS. This ensures that all necessary activities are carried out within the relevant legal and regulatory frameworks and in line with the service's analysis regime.

This could appear to the armed forces as if they are being forced to follow NLD DISS's lead, but that is not the case. I know that in the past there has been a lot of internal strife, partly because many of the different branches' intelligence capabilities were combined under the auspices of NLD DISS, the idea being that NLD DISS would serve each branch strategically, operationally and tactically. That is not entirely fair, since the service has nowhere near sufficient capacity to meet everyone's needs, while at the same time the branches are often unsure to whom they should address their questions. We need a different construction in today's world, where tactical and operational developments occur so swiftly.

NLD DISS and the I&S capabilities of the armed forces must be able to operate within the law. The armed forces branches and the CHOD should be able to direct I&S capabilities, and it would be a shame not to employ these capabilities in a targeted manner. That is why we need a J2 organisation that is linked to the service. This is the path that the CHOD and NLD DISS should explore in order to prevent the creation of a third intelligence capability that would compile its own analyses.

MS: So, will the J2 cell, which will possibly be housed within a CHOD structure or a Permanent Joint Headquarters (PJHQ), fulfil this liaison role?

General Eichelsheim: Yes, because we have operational and tactical I&S capabilities throughout the line, and the question in this 24/7 strategic competitive environment is how they can be employed most wisely. Major General Swillens and I believe that a stronger J2 construction will allow NLD DISS to meet the armed forces' needs more effectively at the operational and tactical levels in all domains. Ensuring this happens will be the task of the J2 capability, whether it falls under the PJHQ, the Defence Staff or elsewhere. This will result in more effective coordination and a better structure, but nothing should be done entirely separately from NLD DISS. For example, it is good that NLD DISS is employing JISTARC's intelligence capabilities in relation to the Russian Federation. It would be strange if it did not do so, and we should actually be coordinating such activities far more frequently. Some people are still holding onto old resentments that they have to rely on a NLD DISS that only provides strategic intelligence, but of course it provides operational intelligence too. The entire I&S network must be opened up a lot more, and J2 will play a key role in this process.

Major General Swillens: Information is the key element of information-driven operations. Understanding situations on the basis of intelligence is crucial at every level. If that is organised properly, decisions can be made. This is the D of information-Driven operations (IDO), the act of driving, which is the core business of the CHOD. Next, the effects that the armed

forces wish to create should be considered. This, too, is a choice that the CHOD can make within the scope of our own capabilities. The conflict in Ukraine has demonstrated that data is an increasingly crucial element. IDO is all about the quality of information, how quickly it can be processed and how fast the armed forces can create the right effects, and so creating this type of J2 organisation is only logical.

General Eichelsheim: Building an information position could for example ensure that we know what the effects of deploying the HNLMS Evertsen [in the Black Sea – ed.] will be.[4] This supports the argument in favour of a PJHQ and a J2 cell that continually interact with NLD DISS across the entire spectrum of armed forces deployment, including readiness activities and deployment in all domains.

Major General Swillens: In the case of Ukraine, for example, we do not yet know whether or where the Netherlands will conduct mine-hunting operations, but we must consider these matters beforehand and compile an analysis in anticipation of a possible decision. NLD DISS aims to permanently exist at the head of the power curve, but military commanders always aspire to this. They want no surprises and always want to feel that they are one step ahead of the rest. This starts by having a sound intelligence position including underlying analyses, and by sharing information wisely with other key players.

MS: Are you satisfied with the current, recently amended Intelligence and Security Services Act 2017 (Wiv 2017) and the regulatory structure applicable to NLD DISS?

Major General Swillens: NLD DISS requires people, resources and a mandate in order to perform its duties. A legal framework is absolutely crucial. The evaluation committee and I myself were surprised at how hotly the interpretation of the letter and spirit of legal texts can be debated. The difficulty of such debates is that they are often based on the idea of a balance of sorts: more security means less privacy and vice versa. But in my experience this is irrelevant. That is why we must provide the public with as much information as possible about how NLD DISS and NLD GISS operate in the field of cyber security, for example, in order to create trust and understanding. For example, we will never 'trawl'[5] entire residential areas because there are other, far simpler ways of responding to requests for intelligence in the Netherlands. And cable interception must be explained even more carefully to the public. They need to know how it works and why it is so important. But if we want to keep the Netherlands safe, cable interception is crucial, since our adversaries flout all the rules and use and abuse cable communications. I think it is scandalous that this has not been sorted out yet.

The framings surrounding the invasion of privacy and the so-called 'Data Trawling Act' are extremely persistent, but I would have sleepless nights if something happened to the armed forces or the Netherlands and afterwards it transpired that we could have known what was going to occur if only we had connected all the dots. That is why I am happy that a temporary law is being drafted, which will enable us to do what is needed. Countries including the Russian Federation and China have launched offensive cyber programmes targeting the Netherlands. Under the current law we cannot identify our adversaries or act rapidly and flexibly on all fronts, and this poses a risk to our national security. If our safety is not guaranteed because the law forms an obstruction, then things have not been organised properly. Effective regulation helps boost confidence in the services, according to an investigation conducted by NLD GISS.

So, be my guest, monitor me at all times. I think that our regulators rate the services quite highly, but that is not always how they are perceived. NLD DISS needs to change this perception by becoming more publicly-oriented, without of course revealing our modus operandi or sources.

4 See also Captain Henk Warnar, 'Marinediplomatie: instrument in het Nederlandse evenwichtsbeleid', 9 July 2021. See https://www.militairespectator.nl/thema/essay/artikel/marinediplomatie-instrument-het-nederlandse-evenwichtsbeleid.

5 'Trawl' refers to the acquisition or tapping of data traffic through interception of an internet cable, for instance.

PHOTO TEUN VOETEN

A Ukrainian position near Mykolaiv: 'The conflict in Ukraine has demonstrated that data is an increasingly crucial element'

MS: At a recent NLD DISS seminar Bob de Graaff provided interesting insights into the service's history, transitions and predecessors and concluded that the latter had required a great deal of time to adjust their modus operandi.[6] Has NLD DISS's ability to change now been maximised? Or is the service in a constant state of flux, and if so can we keep pace with the changes?

Major General Swillens: Working in the context of continuous change is our core business. Developments are taking place in quick succession, and constant innovation and improvement are our reality. Stagnation equals decline, but you are never finished. The biggest challenges facing me as Director of NLD DISS are the shifting geopolitical developments, growing volumes of data, extremely rapid technological developments, shortages on the labour market and compliance issues, and the need to maximise our performance in the face of all these challenges. How can we handle our regular work while also freeing up sufficient time and energy to incorporate the necessary changes? I have ascertained that the coalition agreement allocated funds to us to enable us to achieve this.

We also learn from others. For example, we are carefully examining the lessons learned from the war in Ukraine regarding resilience in communication and cyber security, despite the country being under heavy attack day in day out. The Ukrainians have demonstrated that they have taken the lessons learned in 2014 to heart. And that is what we are now also attempting to do: learn the lessons without going through the same experiences.

MS: How do you both use the experience you gained in your previous jobs?

General Eichelsheim: Because I was previously director of NLD DISS I have a good understanding of the information position and the risks that exist in the world, so I definitely feel that my previous experience has enriched me. The director of NLD DISS becomes familiar with every domain, including the cyber and information domains, and learns how much time the service sometimes needs to interpret information correctly. As CHOD I therefore know how to use the service more effectively and that it is good to involve NLD DISS in planning and decision-making. The director of NLD DISS attends far more forums than in the past, since intelligence is also required for decision-making processes and for the development processes of the armed forces. A practical aspect for me as CHOD is that having been the NLD DISS director I was already familiar with the political environment and therefore knew the ins and outs of issuing recommendations.

Major General Swillens: I brought the creative mindset that I had cultivated in my former position as Commander of the Commando Corps to NLD DISS. You have to continually ask yourself whether you are seeing things clearly. The CHOD and I both have executive experience in the armed forces, so we know how crucial details can be and how important soldiers' comments and horizontal learning are. I recognise this from the SF environment where nothing is ever marked a 10; 9.5 is the top score you can get because there is always room for improvement. ■

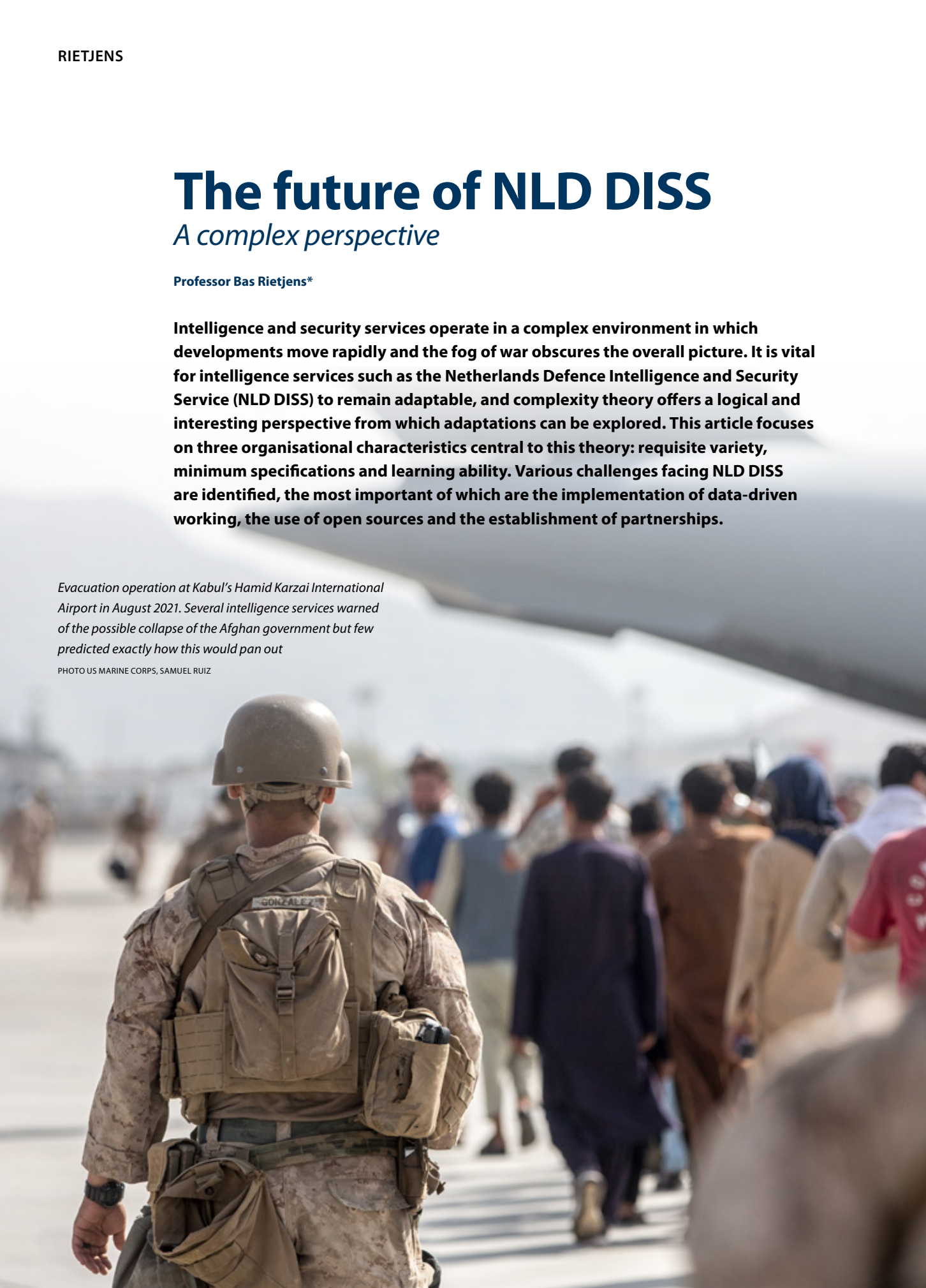
6 See also Bob de Graaff, *Ongekend en onderscheidend. De geheime geschiedenis van de MIVD* (Amsterdam, Uitgeverij Boom, 2022)

The future of NLD DISS

A complex perspective

Professor Bas Rietjens*

Intelligence and security services operate in a complex environment in which developments move rapidly and the fog of war obscures the overall picture. It is vital for intelligence services such as the Netherlands Defence Intelligence and Security Service (NLD DISS) to remain adaptable, and complexity theory offers a logical and interesting perspective from which adaptations can be explored. This article focuses on three organisational characteristics central to this theory: requisite variety, minimum specifications and learning ability. Various challenges facing NLD DISS are identified, the most important of which are the implementation of data-driven working, the use of open sources and the establishment of partnerships.



Evacuation operation at Kabul's Hamid Karzai International Airport in August 2021. Several intelligence services warned of the possible collapse of the Afghan government but few predicted exactly how this would pan out

PHOTO US MARINE CORPS, SAMUEL RUIZ

The tragic events in Afghanistan in the summer of 2021 and the recent Russian invasion of Ukraine demonstrate all the more that we live in an unpredictable and complex world. Although several intelligence services warned of the possible collapse of the Afghan government in the months prior to the fall, very few people predicted exactly how the situation would pan out. General Nick Carter, the highest-ranking British officer, summed up the situation by saying, 'It was the pace of it that surprised us and I don't think we realised quite what the Taliban were up to. They weren't really fighting for the cities they eventually captured, they were negotiating for them, and I think you'll find a lot of money changed hands as they managed to buy off those who might have fought for them'.[1] And while US and British intelligence services in particular predicted the Russian invasion of Ukraine with great accuracy, many were surprised by the resistance put up by Ukraine's armed forces. These examples demonstrate how challenging it is to generate intelligence that is accurate, specific and timely and that also offers perspective for action. This challenge is determined largely by the complexity of the operating environment of intelligence and security (I&S) services. This article begins by addressing this environment and outlining several major developments that contribute to its complexity. The following section discusses the literature on complexity and introduces three characteristics that are required by I&S services in general, and NLD DISS in particular, in order to operate effectively in a complex environment of this nature. The article ends with a conclusion.

Developments

I&S services such as NLD DISS face numerous developments, the most important of which are the changing nature of war and conflict, privatisation, globalisation, and the technology and information revolution, as outlined below.

The changing nature of war and conflict

I&S services face a wide range of threats. During the Cold War these threats were reasonably straightforward and transparent, but nowadays the situation is different. A wide range of terms are used to denote the current conflicts and threats, such as asymmetric warfare, hybrid warfare, grey-zone warfare and non-linear warfare.

And of course the current conflict in Ukraine resembles conventional warfare in many ways, although classifying it as such with no further qualification would be an oversimplification.

* Bas Rietjens is Professor of Intelligence and Security at the Netherlands Defence Academy.

1 Jessica Elgot, '"Everybody got it wrong" on Taliban strategy, says UK defence chief', *The Guardian*, 5 September 2021.

The common denominator of all these conflicts is the violence and threat of violence between various combinations of state and non-state actors. The boundaries between war and organised crime are highly diffuse, human rights are violated on a large scale, and all kinds of non-traditional weapons are deployed. In Mark Galeotti's most recent book this is described as the 'weaponization of everything'.[2] Concrete examples include the case of the refugees who were picked up in Syria by Belarusian president Lukashenko and then sent across his country's border with Poland, and the Swedish children who were made aware of the impending Russian threat through warnings issued between TikTok videos. Identifying these developments and protecting against the multitude of threats represent a huge challenge for I&S services.

Privatisation

A second development concerns the increasing role of private organisations in the I&S domain. First of all there are the civil contractors, who provide a wide range of goods and services varying from cloud services and security to personnel performing mission-critical tasks. Privatisation in the I&S domain has soared in countries such as Australia, France and the United Kingdom, but nowhere in the Western world is it as important as in the US, where around 80 percent of the total intelligence budget of $80 billion goes to private contractors. This inspired Simon Chesterman's maxim 'We can't spy… if we can't buy'.[3] Besides the procurement of goods and services by contractors, non-profit collectives have also proliferated in recent years. These collectives, consisting of networks of volunteers, utilise the abundant open sources that are available. While Bellingcat is the most prominent collective,[4] even an organisation such as Amnesty International has managed to gather evidence on war crimes in Sudan by mobilising 28,000 volunteers and utilising publicly accessible satellite images.

Globalisation

A third development is globalisation. In her pioneering study, Mary Kaldor describes globalisation as the intensification of global interconnectedness in the political, economic, military and cultural sphere.[5] Globalisation is increasingly blurring distinctions between the local, national, European and global strata, and this is having a considerable influence on the security situation. For example, globalisation has led to a substantial increase in transnational crime, including drug trafficking, people smuggling and technology theft. The boundary between internal and external security is also becoming more diffuse, and geographically defined national borders are becoming increasingly irrelevant to the categorisation of threats. Another consequence of globalisation is that government organisations no longer have sole ownership of intelligence. Individual citizens and private organisations are increasingly able to generate intelligence in competition with I&S services. In her recent book *Spies, Lies, and Algorithms*, Amy Zegart ascribes this to the accessibility of satellite data, the increased connectivity and availability of information, and the available processing power of computers.[6]

Technology and information revolution

Technology and technological developments such as biotechnology, quantum computing, radar technology and artificial intelligence are undeniably of crucial importance to intelligence and security organisations. However, while military organisations were previously pioneers in the development of new technology, this is no longer the case, as universities and tech companies have been the primary innovators for quite some time.

Many technological developments are taking place in the information domain. For example,

2 M. Galeotti, *The Weaponization of Everything. A Field Guide to the New Way of War* (New Haven, Yale University Press, 2022).

3 S. Chesterman, ''We Can't Spy… If We Can't Buy!'. The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions'', *European Journal of International Law*, Vol. 19, No. 5 (2008) 1055-1074.

4 See E. Higgins, *We are Bellingcat* (Amsterdam, Spectrum, 2021).

5 M. Kaldor, *New and Old Wars. Organized Violence in a Global Era* (Cambridge, Polity Press, 1999) 71.

6 A. Zegart, *Spies, Lies, and Algorithms. The History and Future of American Intelligence* (Princeton, Princeton University Press, 2022).

Contradictory reports on the conflict in Ukraine hamper interpretation of the large volume of data in circulation PHOTO TEUN VOETEN

in recent years developments in ICT have led to a massive rise in the volume of data that is generated and shared by companies, government institutions, scientific researchers, civilians and others. In the literature this data development is often referred to in terms of the so-called Vs,[7] which denote various aspects relating to data such as the large volumes, structured and unstructured forms, different formats such as text, video, images and sound recordings, major reliability discrepancies, and rapidity of access. The lack of reliability, for example, is clearly illustrated by the contradictory reports on the conflict in Ukraine. Data is often incomplete, ambiguous, contradictory or simply untrue, which makes it very difficult to interpret the information it contains.

The developments briefly outlined above are determining factors with regard to the complexity facing I&S services in general and NLD DISS in particular. This situation shows strong parallels with the so-called wicked problems,[8] which are ambiguous and fuzzy and which cannot be adequately resolved through the application of existing knowledge and standards. Even if something faintly resembling a solution is devised, it will not be possible to apply it across the board since different situations require different solutions. The literature on complexity defines various characteristics required by organisations in order to respond adequately to these wicked

7 Depending on the source, 3, 4 or even 7 Vs define the key aspects of data: Volume (large data sets consisting of terabytes, petabytes, zettabytes of data or more); Variety (multiple data formats with structured and unstructured text, images, audio files, videos, sound fragments or sensor data); Veracity (increasingly complex data structures, inconsistencies and incompleteness in data sets); Velocity (large volumes of incoming data with no homogeneous structure); Variability (data with constantly changing meaning); Visualisation (the presentation of data in a clear and comprehensible way); Value (the extraction of knowledge from large quantities of structured and unstructured data with no loss for the end users).

8 H. Rittel and M. Webber, 'Dilemmas in a General Theory of Planning', *Policy Sciences*, Vol. 4, No. 2 (1973) 155-169.

problems.[9] Three of these characteristics – requisite variety, minimum specifications and learning ability – and their relevance to NLD DISS are discussed in this article.[10]

Requisite variety

The first characteristic is based on Ashby's law of requisite variety,[11] which states that in order to be viable a system must have a level of internal variety equivalent to that of its environment. Only then will the system be capable of identifying and facing up to challenges.[12] In the case of NLD DISS, this means that the service must fulfil multiple, wide-ranging information requirements, varying from the identification of cyber threats from hacker groups affiliated with China or the Russian Federation to the detection of terrorist activities by groups such as Islamic State of Iraq and al-Sham (ISIS). This calls for highly diverse knowledge and expertise covering many different areas. An organisation that attempts to cover all these information requirements is in danger of becoming overly complex,[13] so in order to avoid this complexity it is essential to cooperate with various stakeholders. NLD DISS works with a wide diversity of stakeholders[14] within the Netherlands Ministry of Defence[15] and other ministries,[16] in addition to partner intelligence services in other countries, the business sector,[17] the scientific community and non-profit organisations. Managing all these partnerships is a huge challenge, particularly for an organisation that is intrinsically secret and quite closed. While the focus is often placed on formal cooperative structures, research by Pepijn Tuinier reveals that mutual trust and social relations are equally important, if not more so.[18] Ties between intelligence professionals are founded on reputation, acknowledged professionalism and shared characteristics. This helps them to bridge the divides created by nationality, organisation or even conflicting interests.

Besides cooperation, diversity is another important enabling factor in the quest for the requisite variety.[19] Cultural diversity is often viewed as the primary expression of diversity, based on race, skin colour, religion, gender, sexual orientation, background and age,[20] but cognitive diversity is also important since it offers different perspectives, experiences and ways of thinking. In his book *Rebel Ideas*, Matthew Syed suggests that complex problems must be viewed from different perspectives in order to release a group or organisation from the constraints of conventional frames of reference and thought patterns.[21] A classic example of the importance of diversity is the CIA's failure to pick up on the various signals that preceded the 9/11 terrorist attacks, a failure that can be attributed partly to the predominance of highly educated white males on its staff.

A distinctive feature of NLD DISS's workforce is the mix of military and civilian personnel. The civilians outnumber the military personnel and

9 See also S. Brown and K. Eisenhardt, 'The art of continuous change. Linking complexity theory and time-paced evolution in relentlessly shifting organizations', *Administrative Science Quarterly*, Vol. 42, No. 1 (1997) 1-34.

10 These analyses are based on available literature and documents as well as informal conversations with NLD DISS personnel. A draft version has been presented to three peer readers in order to reinforce validity and reliability.

11 W. Ashby, *An Introduction to Cybernetics* (London, Chapman & Hall, 1956).

12 See also G. Morgan, *Images of Organization. The Executive Edition* (Thousand Oaks, Sage, 2006).

13 K. Desouza, 'Information and Knowledge Management in Public Sector Networks. The Case of the US Intelligence Community', *International Journal of Public Administration*, Vol. 32, No. 14 (2009) 1219-1267.

14 See also H. de Bruijn, *Managing Performance in the Public Sector* (London, Routledge, 2007).

15 Including the Directorate-General of Policy (DGB), the operational commands, the Special Operations Command (SOCOM) and the Joint ISTAR Command (JISTARC).

16 Including the General Intelligence and Security Service (GISS), National Cyber Security Centre (NCIS), National Coordinator for Security and Counter-Terrorism (NCTV) and the various departments of the Netherlands Ministry of Foreign Affairs.

17 Including cyber security companies such as Fox-IT.

18 P. Tuinier, T. Brocades Zaalberg & S.J.H. Rietjens, 'The Social Ties that Bind: Unraveling the Role of Trust in International Intelligence Cooperation', *International Journal of Intelligence and CounterIntelligence* (2022) DOI: 10.1080/08850607.2022.2079161.

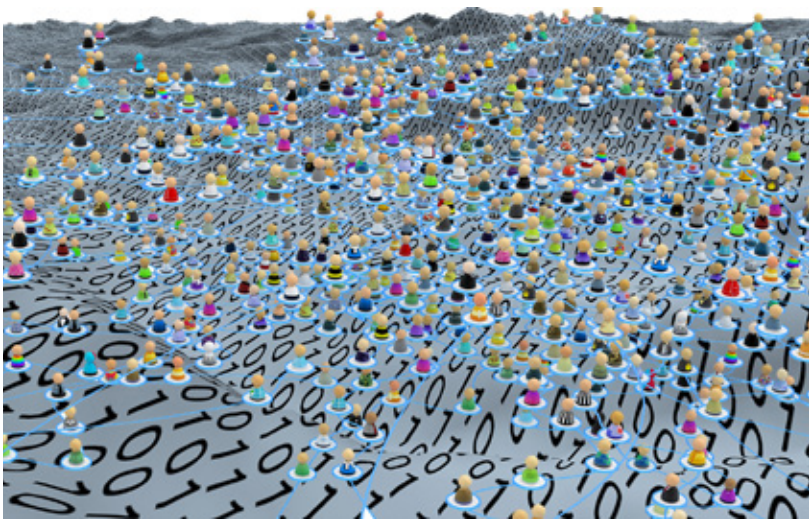
19 See also J. Gentry, 'Demographic Diversity in U.S. Intelligence Personnel: Is it Functionally Useful?', *International Journal of Intelligence and CounterIntelligence* (2021).

20 R. Callum, 'The Case for Cultural Diversity in the Intelligence Community', *International Journal of Intelligence and CounterIntelligence*, Vol. 14, No. 1 (2010) 25-48.

21 M. Syed, *Rebel Ideas. The Power of Diverse Thinking* (London, John Murray Publishers, 2020).

have diverse backgrounds, frames of reference and types of experience. For example, they may have knowledge relating to a specific country, mastery of a particular language, hacking expertise or experience with large data sets. However, it is the military expertise and knowledge that distinguish NLD DISS from other organisations and enable the service to fulfil its responsibilities,[22] and NLD DISS's increasing difficulty in attracting and retaining sufficient military personnel is therefore cause for concern. Another related factor is that NLD DISS employees have followed a wide range of different educational programmes. In terms of the traditional distinctions between the arts (history, languages), the sciences (physics, IT) and the social sciences (psychology, sociology, economics), personnel with a background in science are scarce. Given the significant developments in the information domain, it is vital for NLD DISS to recruit and hold on to people with expertise in science and technology. Facing competition with many other knowledge-intensive organisations in this employment market, NLD DISS attracts creative people with a science background through initiatives such as the annual summer school organised by the Joint Sigint Cyber Unit.[23] However, managing diversity involves more than just a varied workforce, which is why NLD DISS established the Devil's Advocate in 2008.[24] This office is charged with questioning the dominant train of thought within NLD DISS and proposing alternative perspectives with a view to reducing groupthink.[25] Other diversity management challenges facing the service include the creation of a collective identity, the combination of different leadership styles, optimum utilisation of the diverse backgrounds and areas of expertise, and the provision of a wide range of career and training opportunities.[26]

PHOTO DARPA



NLD DISS has a mixed workforce comprising military and civilian personnel who introduce different perspectives, experiences and ways of thinking based partly on their diverse educational backgrounds in the arts, sciences and social sciences

Minimum specifications

The second characteristic that enables organisations to cope adequately with complexity concerns minimum specifications. This entails specifying only the most essential aspects so that the individuals actually tasked with the activities have the freedom to experiment and question existing procedures, norms and performance criteria. Karl Weick refers to this as 'the charm of the skeleton',[27] emphasising the need to strike a balance between keeping a firm control over the organisation while simultaneously relaxing application of the regulations. In the intelligence domain these minimum specifications create a paradoxical situation. I&S services need room to manoeuvre when addressing complex intelligence issues, since intelligence teams are increasingly confronted with unknown threats, referred to in this field as 'unknown unknowns'. An important strategy for identifying such unknown threats is the concept of enactment, or, in the words of Dan Isenberg, 'fighting

22 See Article 10 of the Intelligence and Security Services Act 2017 (Wiv).
23 See https://jscu.summerschool.sh.
24 A. Claver and H. van de Meeberg, 'Devil's Advocacy within Dutch military intelligence (2008-2020). An effective instrument for quality assurance?', *Intelligence and National Security*, Vol. 36, No. 6 (2021) 849-862.
25 Claver and Van de Meeberg (2021).
26 NATO STO HFM-226 Task Group, *Civilian and Military Personnel Integration and Collaboration in Defence Organisations* (Brussel, NAVO, 2018); I. Goldenberg e.a., 'Integrated defence workforces. Challenges and enablers of military–civilian personnel collaboration', *Journal of Military Studies*, Vol. 8 (2019) 28-45.
27 K. Weick, 'Rethinking Organizational Design', in R. Boland and F. Collopy (Eds.), *Managing as Designing* (Stanford, Stanford University Press, 2004) 36-53.

Statement by an attendee at the announcement of the advisory referendum on the Wiv in 2018: the level of public support restricts the scope of NLD DISS's activities PHOTO ANP, REMKO DE WAAL

empirically'.[28] Enactment is based on the symbiotic relationship between an organisation and its environment, the assertion being that only organisations that take concrete action can comprehend and adapt to their environment. In this regard it is necessary to constantly reflect upon the situation rather than to regard the environment as a static entity. Offensive counter-intelligence operations such as breaking into the computer networks of a rival service are a good example of how I&S services interpret the concept of enactment. In principle the aim of these operations is not to put a stop to hostile intelligence operations but rather to acquire as much information as possible on the adversary, his operations and the development of his covert activities.[29]

A second strategy for identifying unknown threats is to detect correlations in large quantities of data such as bulk data sets. The aim of this strategy, often referred to as the data-driven approach, is to recognise general trends and deviations and thus diminish the influence of cognitive prejudices.

The minimum specifications characteristic does not imply that the activities of I&S services should be free of all restrictions. Various mechanisms exist to limit their scope. The Intelligence and Security Services Act 2017 (Wiv 2017) Evaluation Committee [30] and the Netherlands Court of Audit [31] have clearly identified where the tensions lie between the operational striking power of the I&S services and the implementation of the Wiv 2017, including the associated supervisory regime. The main tensions arise in relation to the collection and processing of bulk data, the automated data analysis, the cooperation with foreign services and the regulatory system. For example, Article 26 of the Wiv stipulates that when collecting bulk data sets the services must satisfy the requirements of necessity, proportionality and

28 D. Isenberg, 'Some Hows and Whats of Managerial Thinking', in J. Hunt and J. Blair (Eds.), *Leadership of the Future Battlefield* (New York, Pergamon, 1985).

29 B. de Jong and P. Keller, 'Contra-inlichtingen en contraspionage', in B. de Graaf, E. Muller and J. van Reijn (Eds.), *Inlichtingen- en Veiligheidsdiensten* (Alphen aan den Rijn, Kluwer, 2010) 280.

30 Wiv 2017 Evaluation Committee, *Evaluatie 2020: Wet op de Inlichtingen- en veiligheidsdiensten 2017* (2021).

31 *Slagkracht AIVD en MIVD. De wet dwingt, de tijd dringt, de praktijk wringt* (The Hague, Netherlands Court of Audit, 2021).

subsidiarity. Another important requirement is that data collection must be targeted. This means that the service must do everything that is reasonably within its power to minimise the by-catch of data that is not essential to the investigation and to explain how this is to be achieved when requesting permission to exercise investigatory powers.[32] The service must also demarcate its search as far as possible in terms of location, time, type of data, object or conduct. However, this demarcation conflicts with the need to identify unknown threats.

In addition to the legal regime, the activities of the services are limited by the Integrated Directive (*Geïntegreerde Aanwijzing* – GA). This document must be compiled on the basis of close consultation between the requisitioners and the services and must describe the target of the investigation, the intended goals and the priorities. The depth of the investigation must also be indicated per theme.[33] The GA is relatively effective in the case of known unknowns, when the investigators know there are things they do not know, and it is also a good instrument for allocating resources to a service and evaluating their results. However, in the case of unknown threats this directive is often felt to be too restrictive. The GA is valid for four years but can be adjusted annually, although an annual cycle seems too long to enable an adequate response to new and unforeseen threats to national security.[34] The legislator has attempted to overcome this problem by granting limited discretion to the Minister of the Interior and Kingdom Relations and the Minister of Defence to issue supplementary investigation orders. The Wiv 2017 also explicitly states that the services can continue to utilise their capabilities to identify unknown threats. However, I&S services will be inclined to prioritise the assignment of capabilities to those investigation themes for which they are accountable. Although this is understandable, it helps to create a situation in which unknown threats receive less attention than they deserve.

A final restriction governing I&S activities concerns public support and the associated balance between transparency and confidentiality. Many companies and government organisations collect and use personal details pertaining to civilians. It is often unclear why this data is collected, what it is used for and the extent to which this is in the citizens' interest. This lack of clarity is a major cause for concern within society, particularly in relation to privacy, since this data could be used for profiling, influencing or even manipulating citizens.[35] Special investigatory powers have been assigned to I&S services by society through the legislator, and consequently it is vital for these services to preserve public support and keep their activities as transparent as possible. Public perception of NLD DISS has been damaged not only by the sweeping revelations relating to the interception activities of the US National Security Agency (NSA), but also by recent reports on the activities of the Netherlands army's Land Information Manoeuvre Centre (LIMC)[36] and the NCTV's analysis division.[37]

In summary, the minimum specifications dilemma can be resolved by striking a fine balance between responsibilities, room to manoeuvre and restrictions. In order to perform its tasks effectively, NLD DISS needs room to manoeuvre, for example in relation to the above-mentioned enactment concept, but is restrained mainly by the legal regime, the GA and public perception.

Learning ability

The third characteristic relates to the learning ability of an organisation. The literature on organisations distinguishes between single loop learning (making relatively simple adjustments and implementing corrections), double loop

32 Parliamentary papers II 2018/2019, 35 242 No. 3, p. 5 (Explanatory Memorandum Wiv 2017 amendment).
33 P. Abels, *PER UNDAS ADVERSAS? Geheime diensten in de maalstroom van politiek en beleid* (Leiden, Leiden University, 2018).
34 Abels (2018).
35 Wiv 2017 Evaluation Committee (2021) 22.
36 E. Rosenberg and K. Berkhout, 'Militairen zouden dit zelf heel netjes moeten willen regelen', *NRC,* 16 November 2020.
37 A. Kouwenhoven, E. Rosenberg and R. van der Poel, 'Onmin en uitglijders bij de club die het land moet beschermen', *NRC*, 9 April, 2021.

The minimum specifications dilemma calls for a fine balance between responsibilities, room to manoeuvre and restrictions

learning (reframing and perceiving subjects in a new way), and triple loop learning (developing new processes or methods in order to enable reframing and new perspectives).[38]

There are clear examples of single loop learning within NLD DISS. Learning is continuous at both individual and team levels. For example, employees increasingly use open sources and data analysts experiment with the available software applications and models. However, few formal procedures exist at the organisational level to codify experiences and lessons learned, and while some employees register their experiences and lessons (often in self-designed formats), others pay little attention to this, resulting in fragmentation and preventing structural comparisons and analyses of the lessons learned. This problem is exacerbated by the limited term of office of military personnel in particular, who frequently move to a new position, leading to a loss of knowledge and the need to re-establish relationships. In addition, managers often have a preference for personnel who can be deployed operationally rather than personnel charged with registering and codifying acquired knowledge. Although this may be understandable from an operational perspective, it is detrimental to the organisation's learning ability. Finally psychological security plays an important role in learning ability. This concerns the capacity for critical self-reflection and criticism of the team and the organisation as a whole based on the expectation of constructive feedback from colleagues and managers when doing so. Only then will an organisation actually learn.

The double loop learning level represents a gradual change in the approach to intelligence issues. In the intelligence literature this is explored within the context of two schools of thought[39]. The first of these, derived from Jomini's theory of war, constitutes an attempt to systematically unravel the environment. The well-known spaghetti diagram created by General Stanley McChrystal and his staff to portray the situation in Afghanistan is a good example of this.[40] Critics of this approach point out that it is simply impossible to include all relevant elements in a single analysis,[41] and even if this were possible, the result would often be a stark simplification of reality with no satisfactory solution to the problem. The second school of thought acknowledges the problematic nature of this approach and instead places the emphasis on complexity and the associated uncertainty and confusion. This is often equated to the 'fog of war', a term introduced by the Prussian General Carl von Clausewitz, who stated that three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty.[42] According to this school of thought, a sensitive and discriminating judgement that approximates the truth or truths is the most that can be achieved.[43]

38 See also A. Romme and A. van Witteloostuijn, 'Circular organizing and triple loop learning', *Journal of Organizational Change Management*, Vol. 12, No. 5 (1999) 439-453.

39 See also W. Agrell and G. Treverton, *National Intelligence and Science. Beyond the Great Divide in Analysis and Policy* (Oxford, Oxford University Press, 2015).

40 See https://www.theguardian.com/news/datablog/2010/apr/29/mcchrystalafghanistan- powerpoint-slide.

41 K. Galster, *The Face of the Foe. Pitfalls and Perspectives of Military Intelligence* (Kingston, Legacy Books Press, 2015).

42 C. von Clausewitz, *Vom Kriege* (1832). Translated by M. Howard and P. Paret, *On War* (New Jersey, Princeton University Press, 1984).

43 Galster, *The Face of the Foe.*

The Dutch intelligence community still harbours many advocates of the Jomini approach, who often seek to unravel an environment systematically using tools such as the PMESII (Political, Military, Economic, Social, Information and Infrastructure) framework. Another frequently voiced expression is 'speaking truth to power', which implies that there is one single discernable truth, a notion that is clearly at odds with complexity theory. Even so, ideas are slowly but surely shifting towards the Clausewitz approach. Many of the parties concerned acknowledge that it is simply not possible to make the fog clear completely and they consequently recognise the need to manage complexity and uncertainty. This was underlined during a recent seminar on the occasion of the 20th anniversary of NLD DISS.[44] In this seminar, aptly entitled Fog of War 2.0, almost all speakers alluded to the confusing circumstances and the impossibility of acquiring full environmental awareness.

With awareness of this paradigm shift gradually dawning, it is important for NLD DISS to develop new processes or methods to enable an adequate response. This constitutes the third level of learning: triple loop learning. One of the greatest challenges at this level is the use of open sources. The conflict in Ukraine has reinforced the importance of open source intelligence (OSINT). There are many examples that illustrate this, ranging from the satellite data provided by Maxar Technologies to the Live Universal Awareness Map (Liveuamap), which tracks near real-time battlefield developments and depicts these on a map.[45] Open sources have several advantages. For example, OSINT enables already available intelligence to be placed in a broader context, it is less expensive than other intelligence capabilities, it can be used to compare intelligence products from different services, and it can easily be scaled up and disseminated.[46] John Gannon, former deputy director of the CIA, recognised this as early as 2001 when he stated, 'Open-source was the "frosting on the cake" of intelligence material dominated by signals, imagery, and human-source collection. Today, open source comprises a large part of the cake itself.'[47]

The huge potential of OSINT is apparently not yet being fully utilised, despite its clear advantages and the requirement of the subsidiarity principle that I&S services must deploy the lightest possible means to achieve the intended goal. This applies to I&S services in general, and therefore also to NLD DISS. This underutilisation is partly due to the culture within I&S services, in which special intelligence capabilities are often afforded a higher status than open sources. Another concern is that a more intensive use of OSINT could detract from the exclusive character of I&S services in relation to think tanks, research institutes and collectives such as Bellingcat.

Furthermore, since open sources are not protected and their collection is not covert, the distinction between information and intelligence is often vague and the concept of intelligence may consequently be devalued. Wilhelm Agrell summed up this dilemma two decades ago, stating, 'When everything is intelligence, nothing is intelligence.'[48] I&S services will therefore be compelled to rapidly reassess their perception of OSINT and its embedment within their organisation.

The second challenge in relation to the development of new processes and methods constitutes the implementation of a data-driven working approach. While many intelligence teams mainly use traditional and qualitative analyses, they now have to contend with major developments in the technology and information domain (Section 2). For example, the volume of data – including open source data – available to I&S services is growing exponentially, and the services also potentially have access to rapidly increasing computing

44 Seminar *The Fog of War 2.0* (The Hague, 23 June 2022). See https://www.youtube.com/watch?v=_C0jgTqQQjw.

45 See https://liveuamap.com.

46 See also S. Gibson, 'Open Source Intelligence', R. Dover, M. Goodman and C. Hillebrand (Eds.). *Routledge Companion to Intelligence Studies* (London, Routledge, 2014) 123-131.

47 John Gannon, 'The Strategic Use of Open-Source Information', *Studies in Intelligence*, Vol. 45, No. 3 (2001) 67.

48 See https://www.hsdl.org/?view&did=442465.

power and data analysis models. This necessitates the implementation of data-driven working. However, NLD DISS faces daunting challenges in this regard. One frequently mentioned challenge concerns the small number of employees with a background in science. Although this is certainly the case, this is just one of many challenges, such as the available infrastructure (including hardware, software and applications), the data illiteracy of many analysts and managers, the integration between quantitative and qualitative analyses, and last but not least information management.

Conclusion

'It is not the strongest of the species that survives, nor the most intelligent; it is the one most adaptable to change.' This quote is often attributed to Charles Darwin, the founder of the theory of evolution, although it cannot be traced back to him literally. Continual adaptation is also essential to the survival of I&S services in the face of major developments such as the changing nature of war and conflict, privatisation, globalisation and technology. Given the complexity of these developments, complexity theory is a logical and interesting perspective from with these adaptations can be explored. This perspective is defined by focusing on three organisational characteristics. The first of these is requisite variety, which emphasises the importance of both cognitive and cultural diversity and cooperation with a broad range of actors.

The second characteristic entails minimum specifications, for which a fine balance must be struck between responsibilities, restrictions imposed by rules and principles, and the room to manoeuvre and operational striking power required by an I&S service in order to be effective. The third and final characteristic is learning ability. In this regard a distinction can be made between making relatively simple adaptations (single loop learning), reframing and gaining new perspectives (double loop learning), and developing new processes or methods (triple loop learning). All of the above underlines the need to embrace complexity, make better use of open sources and adopt a data-driven approach. It was management guru Peter Drucker who stated, 'The only thing we know about the

PHOTO US MARINE CORPS, NICHOLAS GUEVARA

49 P. Drucker, *Management. Task, Responsibilities, Practices* (New York, Harper & Row, 1973).

The smoke machine takes on a metaphorical significance as the intelligence community gradually shifts towards the Clausewitz approach, which posits that the current circumstances are so complex that the fog of war will never lift completely

future is that it will be different,'[49] and faced with such uncertainty I&S services will need to be optimally prepared for an unknown future. ■

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.

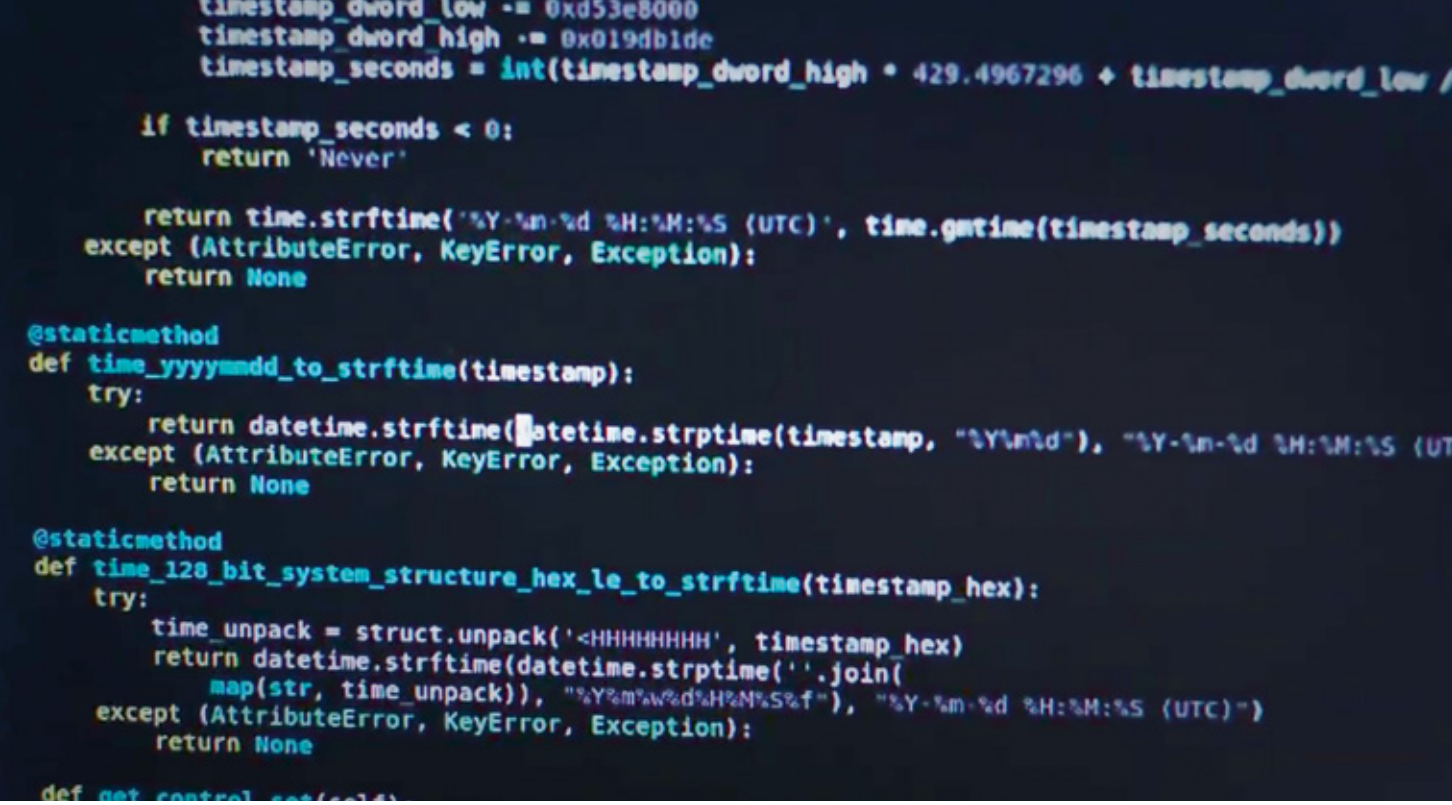
'Never get involved in a land war in Asia, never go against a Sicilian when death is on the line, and never hack the Dutch.'[1]

'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.

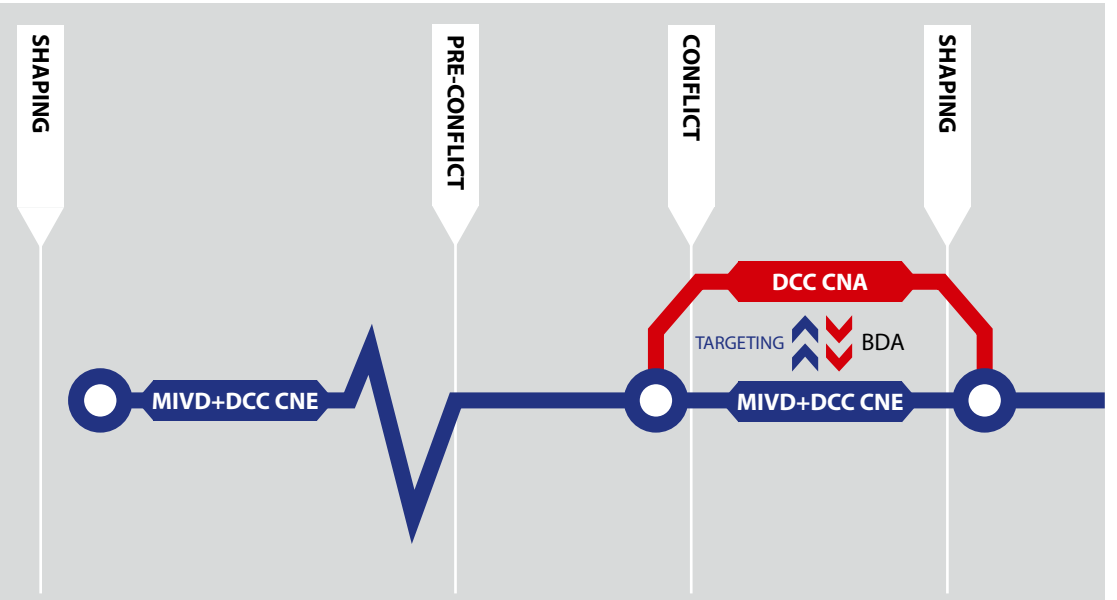


Figure 1. This is the suggested collaboration model in which NLD DISS and DCC jointly prepare CNE operations in a CMT before, during and after a conflict to support operations, including CNA operations carried out by DCC. In the framework of the CMT's ongoing CNE operations, options are developed for 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)

Saskia Pothoven is a PhD candidate at the Netherlands Defence Academy and also works for the Central Staff of the Ministry of Defence. This article, which approaches the topic from a specifically Dutch perspective, derives from a more extensive article by the author on the same subject for an international audience entitled: 'Producer-Client Paradigms for Defence Intelligence', which was published in the June issue of *Defence Studies: Journal of Military and Strategic Studies*.

Questioning the sacred cows

Military perspective on the relationship between intelligence producers and their clients

Saskia Pothoven MA*

The relationship between intelligence producers and their clients has been the subject of debate for decades, both in academic and professional circles. The military intelligence domain differs from the civilian domain in a number of important respects, and thus requires special attention. It is therefore relevant to assess the extent to which prevailing views about the intelligence producer-client relationship – the 'sacred cows' – which are usually based on the civilian intelligence domain, persist in the military intelligence domain. This article offers a military perspective on the intelligence producer-client relationship with reference to three distinctive characteristics and three sacred cows arising from literature study. The focus here is on the strategic level.

Institutional embedding could put pressure on a military intelligence producer to provide analyses that are not detrimental to their own organisation

PHOTO MCD, KEESNAN DOGGER

In order to be able to investigate how the prevailing conceptualisations based on the civilian intelligence domain persist within the military intelligence domain, the characteristics of military intelligence services must first be considered. These services are often the result of an amalgamation or centralisation of intelligence services from various branches of the armed forces and mainly serve the political and military strategic level.[1] For example, in the Netherlands, the Defence Intelligence and Security Service (NLD DISS) stems from the Military Intelligence Service (MID), which was created in 1988 from an amalgamation of the Naval Intelligence Service (MARID), the Army Intelligence Service (LAMID) and the Air Force Intelligence Service (LUID). With the introduction of the Intelligence and Security Services Act (Wiv) in 2002, the MID was renamed NLD DISS.[2]

Military intelligence services have a number of characteristics that distinguish them from civilian intelligence services. Firstly, we see a high degree of 'institutional embedding', which means that these types of intelligence services are part of the organisation that is also their main client: the Ministry of Defence. This also includes the relationship with the intelligence functionalities within the armed forces, which are responsible for intelligence gathering, analysis and dissemination during deployment of the armed forces. This institutional embedding creates a more intimate relationship with the main clients than is customary in the civilian intelligence domain. One possible consequence of this is that it could put more pressure on a military intelligence producer to modify analyses in such a way that they are not detrimental to the defence organisation,[3] for example by adjusting probability levels or threat levels to ensure wider parliamentary support for military deployment.

A second characteristic of military intelligence services is the mix of civilian and military personnel. Strategic military intelligence services such as NLD DISS have a unique double position because they straddle the middle of the dichotomy between civilian and military intelligence culture.[4] For example, the majority of the staff at NLD DISS are civilian.[5] As a result, there may be differences in leadership style and career and training opportunities, and complications can arise with regard to a shared identity.[6] In the context of the producer-client relationship within the military intelligence domain, this can lead in particular to challenges between military and civilian personnel on the different sides of the relationship.

Although in this type of organisation, the majority of the staff are civilian, these intelligence organisations are nevertheless rooted in military organisations and are thus influenced by cultural traits that are considered typically military. These include a high appreciation of hierarchy, rules and discipline, competencies and status, and clear lines of authority and accountability.[7] Characteristics that are generally highly valued within military organisations, such as decision-making and teamwork, can conflict with the requirements of intelligence work, such as qualifications, avoiding black-and-white thinking and continuous questioning and revision.[8]

Another characteristic is that military personnel often rotate frequently between different roles, often after just three years. This can result in knowledge and a good relationship with intelligence and/or producers and/or clients not being retained in the organisation. On the other hand, frequent rotation can also result in

1 Philip Davies, 'The Problem of Defence Intelligence', *Intelligence and National Security*, Vol. 31, No. 6 (2016) 799.
2 B. de Graaf, E. Muller and J. van Reijn, *Inlichtingen- en veiligheidsdiensten* (Deventer, Wolters Kluwer, 2010).
3 S. Rietjens, 'Intelligence in defence organisations: a tour de force', *Intelligence and National Security*, Vol. 35, No. 5 (2020) 719.
4 J. Thomson, 'Governance costs and defence intelligence provisions in the UK: a case study in macroeconomic theory', *Intelligence and National Security*, Vol. 31, No. 6 (2016) 854.
5 Netherlands Defence Intelligence and Security Service, *Annual report 2019* (The Hague, Ministry of Defence).
6 NATO STO HFM-226 TASK GROUP 2018; I. Goldenberg et al., 'Integrated defence workforces: Challenges and enablers of military-civilian collaboration', *Journal of Military Studies*, Vol. 8 (2019) 33.
7 J. Soeters, 'Organizational Cultures in the Military', in: G. Caforio and M. Nuciari (eds.), *Handbook of the Sociology of the Military* (New York, Springer, 2018) 254.
8 M. Herman, *Intelligence Power in Peace and War* (Cambridge, Cambridge University Press, 1996) 250.

producers of intelligence and clients having performed a role on the other side of the relationship (for example, first as an analyst at NLD DISS and then at the J2 of the Department of Operations, DOPS), which can lead to a better understanding of each other's duties and responsibilities.
A final aspect of military culture is its Janus-faced character, which means that military organisations work in two opposite situations, namely both in 'hot situations', such as combat situations that require immediate action, and 'cold situations', such as training, exercises and preparation for deployment. In line with this, there may be 'hot intelligence', aimed at matters such as mission support and 'cold intelligence', aimed at long-term objectives.

'We give you the weather forecast, but we won't tell you whether you should take an umbrella'

The sacred cows

The weather forecast and the umbrella
In the debate on the intelligence producer-client relationship, the issue of proximity is often questioned: how close or far should producers and consumers be from each other? In general, two schools can be distinguished in this respect. Traditionalists say that there must be a clear separation between intelligence analysis and policy because otherwise there is a risk of an intelligence product being influenced by policy preferences, which, in extreme cases, could lead to politicisation. The well-known saying at NLD DISS 'We give you the weather forecast, but we won't tell you whether you should take an umbrella' clearly resonates with this. The transfer of the J2 functionality from NLD DISS to the DOPS in response to the *Dessens Report* of 2006 can also be placed within this traditional framework.[9] On the other hand, the activist approach indicates that without interaction, there is also little relevance, and in fact advocates for a close relationship between intelligence producers and clients, whereby intelligence is related to and directed by policy objectives and intelligence analysts must have a deep and solid understanding of how policy is established.[10]

Politicisation means that intelligence is adapted to be more in line with policy preferences.[11] It is therefore also referred to as 'intelligence to please'.[12] This can take place both under clear coercion and by creating an environment in which analysts feel limited in drawing conclusions that do not match the preferences of the management or the client.[13]
In addition to the risk of politicisation or intelligence to please, military intelligence organisations may run an even greater risk of a phenomenon known as 'situating the estimate'. This means that a threat assessment is made based on the capabilities of the armed forces and that threats against which no action can be taken are ignored in the analysis.[14]

9 C. Dessens, *Inlichtingen en veiligheid Defensie. Kwaliteit, capaciteit en samenwerking (Intelligence and Security, Defence: Quality, Capacity and Cooperation* (Dessens Committee, 2006).
10 See J. Davis, 'The Kent-Kendall Debate of 1949', *Studies in Intelligence* Vol. 35, No. 2 (1992) 91-103.
11 See inter alia J. Rovner, 'Is Politicization Ever a Good Thing?', *Intelligence and National Security*, Vol. 28, No. 1 (2013) 55-67.
12 H. Ransom, 'The Politicization of Intelligence', in: S. Cimbala (ed.), *Intelligence and the Intelligence Policy in a Democratic Society* (Dobs Ferry, Transnational Publishers, 1987) 26.
13 G. Hastedt, 'The Politics of Intelligence and the Politicization of Intelligence: The American Experience', *Intelligence and National Security* Vol. 28, No. 1 (2013) 5-31; Rovner, 'Is Politicization Ever a Good Thing?', 56.
14 S. Badsey et al. (ed.), *The Falklands Conflict Twenty Years On. Lessons for the Future* (New York, Routledge, 2004) 97.

Afghanistan, 2007: in particular in deployment areas, military intelligence organisations have an intimate relationship with the armed forces' intelligence entities

PHOTO TEUN VOETEN

Military intelligence organisations have an intimate relationship, particularly in deployment areas, with the armed forces' intelligence entities, which is reinforced by the embedding in the same parent organisation. For example, intelligence services use these entities as on-site sensors. At the same time, in some cases these intelligence entities may also use analyses from a military intelligence service. Depending on the level and type of product, it is therefore possible to be at the same time both an intelligence producer and client. This could include, for instance, a J2 section that receives a strategic intelligence product from a military intelligence service and uses this product to produce an analysis intended for the tactical or operational level, although this is less common in the Dutch context because of the current setup of the DOPS J2, which does not have the analysis capacity. While in the Netherlands this is placed in the client domain, in countries like the US or UK a J2 section is more likely to be an intelligence producer because of its expansive analysis capacity. This shows that the producer-client relationship, which is often presented as a dichotomy, could perhaps be better conceptualised as a layered network of different intelligence entities.

In addition, different characteristics of military organisations, such as the frequent rotation of military personnel, a tighter-knit community life because of stationing and informal ties through training and deployment, can contribute to a closer relationship between military intelligence producers and clients. On the other hand, the mix of military and civilian personnel can increase the distance. Herman calls this 'the basic problem of civilian credibility', because civilians lack knowledge of military resources and culture.[15] While officers usually have operational knowledge and technical expertise, civilian staff more often

15 Herman, *Intelligence Power in Peace and War*, 249.

16 A. Wolfberg, 'When generals consume intelligence: the problems that arise and how they solve them', *Intelligence and National Security*, Vol. 36, No. 4 (2021) 472.

have experience at the strategic and policy level.[16] These types of knowledge and experience can complement each other, but may also lead to complications and mutual incomprehension, in particular when it comes to a military intelligence analyst and a civilian client and vice versa.

Analytic objectivity as holy grail

A second sacred cow in the intelligence producer-client relationship is the ideal of analytical objectivity. The idea behind this is that it is the most effective way to avoid influencing an intelligence product, and that politicisation can be avoided.[17]

Objectivity and the distance from decision-making as mentioned in relation to the first sacred cow are generally considered crucial in the ethos of an intelligence analyst.[18] They form the basis for the concept 'speaking truth to power', which is often mentioned as an important task of the analyst. Analytic objectivity, to be achieved for example by eliminating prejudices in an analytic product by means of analytic techniques, is used as a means of truth-finding. The pursuit of objectivity and a quest for the truth are embedded in the thinking of intelligence services. There is good reason why the motto of NLD DISS is *meritum in veritatum discernendo*: the merit lies in the recognition of the truth.[19]

The problem with the pursuit of analytic objectivity is that it requires the absence of bias, which has been acknowledged to be unachievable. What is more, cognitive biases are necessary to make an assessment from incomplete data.[20] In addition, ensuring that a consumer of intelligence faces inconvenient facts and unwanted interpretation requires a bias towards warning, which is often described in terms of (overly) positive policy makers versus (overly) pessimistic intelligence analysis.[21] Intelligence consumers also often ignore intelligence that does not suit them, which diminishes the value of analytic objectivity. A higher degree of objectivity therefore does not necessarily make intelligence more influential,[22] all the more because taking decisions often involves subjectivity and decision-makers are often presented with several versions of 'the truth'.[23]

Because complete analytic objectivity cannot be achieved in practice, all analysts in fact fall short if this is required as a standard. It could therefore be useful to shift the narrative from terms such as 'truth-finding' and speaking truth to power to more relative considerations such as integrity and the 'call it as you see it' approach.[24] In line with these considerations, Woodard argues, for example, for objective honesty (making assumptions and reasoning explicit) instead of policy neutrality.[25]

The idea of speaking truth to power may also apply more to tactical intelligence support than to strategic intelligence analysis.[26] This was applicable especially in the Cold War, when the analytic task was primarily based on tactical puzzles (such as the number of weapons held by the Soviet Union and their location). After the collapse of the Soviet Union, analytic issues became increasingly complex and strategic, moving more in the direction of mysteries which had no clear solution.[27] As a result, it has become even more difficult to pursue analytical objectivity.

17 S. Marrin, 'Analytic objectivity and science: evaluating the US Intelligence Community's approach to applied epistemology', *Intelligence and National Security*, Vol. 35, No. 3 (2020) 350.
18 Marrin, 'Analytic objectivity', 353.
19 Defence Intelligence and Security Service (NLD DISS) Public Annual Report 2019.
20 Marrin, 'Analytic objectivity', 354.
21 Marrin, 'Analytic objectivity', 354.
22 T. Fingar, 'Intelligence and Grand Strategy', Orbis, Vol. 56, No. 1 (2012) 128.
23 Marrin, 'Analytic objectivity', 355.
24 Marrin, 'Analytic objectivity', 360.
25 N. Woodard, 'Tasting the Forbidden Fruit. Unlocking the Potential of Positive Politicization', *Intelligence and National Security,* Vol. 28, No. 1 (2013) 91-108.
26 J. Kerbell and A. Olcott, 'Synthesizing with clients, not analyzing for customers', *Studies in Intelligence*, Vol. 54, No. 4 (2010) 13.
27 W. Agrell and G. Treverton, *National Intelligence and Science. Beyond the Great Divide in Analysis and Policy* (Oxford, Oxford University Press, 2014) 36; G. Treverton, 'Risks and Riddles. The Soviet Union was a puzzle. Al Qaeda is a mystery. Why we need to know the difference', Smithsonian Magazine, June 2007.

SOURCE: CIA PUBLICATION 'PRESIDENT NIXON AND THE ROLE OF INTELLIGENCE IN THE 1973 ARAB-ISRAELI WAR'

Soviet leader Leonid Brezhnev (left) meets with US President Richard Nixon in October 1973: after the collapse of the Soviet Union, analytic issues have become increasingly complex and strategic

This difference can also be illustrated by comparing Clausewitz's theory with that of the Swiss strategist Jomini. While Jomini's supporters see the intelligence domain primarily as an exact science that can be approached with mathematical logic, Clausewitz's adherents believe there will always be a certain degree of uncertainty in intelligence analysis.[28]
While intelligence organisations generally espouse the Clausewitzian approach, the pursuit of analytic objectivity is actually more in line with Jomini's thinking.[29] Because of military characteristics such as decisiveness, discipline and clear lines of authority, the military intelligence domain may be based even more on Jomini's thinking than the civilian intelligence domain. Military intelligence services usually also provide operational and tactical intelligence, such as threat assessments or mission support. This mix of strategic, operational and tactical intelligence support may ensure that strategic analysis is also conducted more according to Jomini's thinking, and is therefore treated more like a puzzle than a mystery. An example of this is NATO's Intelligence Warning System (NIWS), which uses a range of indicators in an attempt to identify new threats at an early stage.

Intelligence forms the basis for decision-making

According to traditional views, intelligence analysts provide information to decision-makers, who then use it to take decisions. In practice, however, especially at the strategic level, intelligence is by no means always used as the basis for decision-making.[30] While consumers of

28 S. Rietjens, 'Omgevingsbewustzijn voor militaire inzet: a mission (im)possible', *Militaire Spectator* 189 (2020) (4) 174-189; Agrell and Treverton, *National Intelligence and Science*, 36.

29 Agrell and Treverton, *National Intelligence and Science*, 36.

30 See, for example, L. Johnson, 'Bricks and mortar for a theory of intelligence', *Comparative Strategy*, Vol. 22, No. 1 (2003) 1-28; S. Marrin, 'Why strategic intelligence analysis has limited influence on American foreign policy', *Intelligence and National Security*, Vol. 32, No. 6 (2017) 725-742; Rovner, 'Is Politicization Ever a Good Thing?, 2011; P. Pillar, *Intelligence and US Foreign Policy. Iraq, 9/11, and Misguided Reforms* (New York City, Columbia University Press, 2011).

intelligence products find that these products are not always relevant enough for them, intelligence analysts are often frustrated if their products are not used or are not used correctly.[31] Although this need not always be a problem because decision-makers can include other considerations than just what is in an intelligence analysis, the developments in the US that led to the invasion in Iraq in 2003 are a clear example of what can go wrong if intelligence is disregarded or misused, with all the consequences this entails. Information was cherry picked, for instance, i.e. used selectively by clients, and there was 'stovepiping' or 'b-teaming' by the Office of Special Plans.[32] This means that raw intelligence is analysed without the involvement of an intelligence service. Related to this, intelligence from the British was sent directly to the prime minister in the Netherlands, without the Dutch intelligence services being able to give an opinion on this.[33] These kinds of cases can also occur when hierarchy and authority are too highly valued, with the run-up to Pearl Harbor serving as an historical example in this regard. Admiral Richmond Turner, the US Navy Director of War Plans, who himself had no intelligence experience, considered the judgments of his own division to be superior to those of the staff of the Office of Naval Intelligence (ONI), who, in his view, had too little seniority. As a result, Turner began to produce his own intelligence analyses separately from the ONI, which was ultimately a major cause for the failure to anticipate the Japanese attack on Pearl Harbor.[34]

At the foundation of this traditional view lies the intelligence cycle, which divides the intelligence process into the five sequential stages: planning and direction, collection, processing, analysis and dissemination.[35] This model has been criticised in intelligence literature for some time as an oversimplification of a very complex process.[36] Despite this, the intelligence cycle is still widespread in the thinking about the intelligence producer-client relationship and can be found in several military doctrines, including the *Dutch Joint Doctrine Publication 2, on intelligence*.[37] It could be argued that due to several characteristics of military organisations, the use of a simplified representation of reality by means of a model is preferred. Firstly, stereotypical military characteristics such as a top-down organisational structure and clear lines of authority do not always align with complex realities. Doctrinal thinking is especially predominant within military culture, accompanied by the use of models to reflect an intractable reality. In addition, the frequent rotation of military

In intelligence literature, the intelligence cycle has been criticised for some time as an oversimplification of a very complex process

31 R. Betts, *Enemies of Intelligence. Knowledge and Power in American National Security* (New York, Columbia University Press, 2007) 67.

32 G. Mitchell, 'Team B Intelligence Coups', *Quarterly Journal of Speech*, Vol. 92, No 2 (2006) 144-173.

33 *Report by the Committee investigating decision-making on Iraq* (Davids Committee) (The Hague, 2010) 318.

34 M. Handel (ed.), *Intelligence and Military Operations* (London, Routledge, 1990) 25.

35 M. Phythian (red.), *Understanding the Intelligence Cycle* (New York, Routledge, 2013) 21; S. Marrin, 'Intelligence Analysis and Decision-making', in: P. Gill et al. (ed.), *Intelligence Theory. Key Questions and Debates* (New York, Routledge, 2009) 133.

36 See, inter alia, G. Evans, 'Rethinking Military Intelligence Failure - Putting the Wheels Back on the Intelligence Cycle', *Defence Studies*, Vol. 9, No. 1 (2009) 22-46; A Hulnick, 'What's wrong with the Intelligence Cycle', *Intelligence and National Security*, Vol. 21, No. 6 (2006) 959-979; G. Eriksson, 'A theoretical reframing of the intelligence-policy relation', *Intelligence and National Security*, Vol. 33, No. 4 (2018) 553-561; Marrin, 'Why strategic analysis has limited influence'.

37 *Joint Doctrine Publicatie 2. Inlichtingen* (The Hague, Ministry of Defence, 2012) 48.

personnel means that specific knowledge and experience are difficult to retain within military intelligence organisations. In order to safeguard this knowledge and to adequately transfer it to new employees, models like the intelligence cycle are useful. Nevertheless, interpreting complex relationships such as those between intelligence producers and clients in terms of simplified models such as the intelligence cycle does not contribute to a deeper understanding of this relationship. Alternatives such as the 'web of intelligence' proposed by Gill and Phythian, which acknowledges the multiple complex interactions between various points such as targeting, collection and analysis, may be more appropriate for this.[38]

The Janus-faced nature of military organisations also influences the impact that intelligence analyses have on decision-making. In the spectrum from 'hot' to 'cold' intelligence, decision-makers are generally more receptive to 'hot' intelligence, such as operational-tactical intelligence that requires an immediate decision, or intelligence that directly contributes to decision-making regarding military deployment. 'Cold' intelligence, such as strategic intelligence analyses focusing on the long term, is generally more likely to be disregarded because it does not require immediate action. Officers often only gain experience with strategic intelligence on the 'client side' once they reach higher ranks.[39] This lack of experience with 'cold' intelligence could be a reason why military decision-makers are often more receptive to the 'hotter' end of the spectrum. This is also described by Handel, who points out that generals sometimes tend to apply their experience and methods for working with tactical-operational intelligence to the strategic intelligence domain, which requires a different way of working.[40] This is problematic because a lack of experience with the higher levels of operational and strategic intelligence can lead to intelligence failures if this intelligence is not used effectively.[41]

Conclusion

The purpose of this article was to investigate, on the basis of three sacred cows, the extent to which the usual way of thinking about the intelligence producer-client relationship also persists in the military intelligence domain. Firstly, it emerges that due to various characteristics of military organisations, the intelligence producer-client relationship is more complex and layered than is generally recognised in intelligence literature. As a result, the dichotomy between producers and clients that can be found in both the traditional and the activist approaches may be less applicable to the military intelligence domain. While the narrative often outlines this relationship in the context of separate roles and tasks, a representation of this relationship in more overlapping and layered roles could contribute to a deeper understanding of the networked and multifaceted nature of the intelligence producer-client relationship in the military domain.

Secondly, the high degree of institutional embedding could make military intelligence organisations more susceptible to direct or indirect pressure to modify intelligence analyses to conform to decision-making. However, a lack of empirical data makes it impossible for the time being to make unequivocal statements about this. The pursuit of analytic objectivity, which is seen as a way of remaining free from influence, may be more prevalent in military organisations because of the Jominian preferences of these organisations, which could result in an unattainable pursuit of absolute objectivity and 'absolute truth'. For a more effective use of intelligence products, it may be preferable to instead embrace values such as honesty and a 'call it as you see it' policy, which are in line with military values and would therefore fit in well with a military intelligence organisation.

Thirdly, consumers of military intelligence products are also not always receptive to the

38 Phythian, *Understanding the Intelligence Cycle*, 34.
39 Wolfberg, 'When generals consume intelligence', 460.
40 Handel, *Intelligence and Military Operations*, 26.
41 Handel, *Intelligence and Military Operations*; Wolfberg, 'When generals consume intelligence', 460.

Decision-makers are generally more receptive to 'hot' intelligence, such as operational-tactical intelligence, that requires an immediate decision

PHOTO MCD, EVA KLIJN

intelligence they receive, which can lead to frustration on both sides. A better understanding of the intelligence producer-client relationship, for example by means of the 'web of intelligence' or the Janus-face principle, could contribute to an improved understanding of how intelligence contributes to decision-making.

It can therefore be said that the military intelligence producer-client relationship requires different considerations and perspectives than the civilian intelligence process. Empirical research is needed to achieve a better and deeper understanding of these processes in a military context. ■

Frustrated and fulfilled ambitions

The Netherlands Defence Intelligence and Security Service, 1912-2022

Bob de Graaff*

Good wine requires aging. This also applies to the Netherlands Defence Intelligence and Security Service (NLD DISS), which is often said to have been born on 25 June 1914, the date on which the third division of the General Staff (GSIII) took shape. However, 1912 would appear to be a more accurate starting point, since this was when the Agency for the Investigation of Foreign Armies was established. However, anyone studying the 110-year history of NLD DISS and its predecessors would have to conclude that the maturation process for the Dutch service was a lengthy one, albeit not due to a lack of ambition. In this article I review the history of the service and its predecessors in a nutshell, based on the ambitions of the successive services and whether or not they were fulfilled.

Exercise involving a Raven, an unmanned reconnaissance system. This article discusses the history of the Netherlands Defence Intelligence and Security Service and its predecessors in a nutshell

PHOTO MCD, EVA KLIJN

* Bob de Graaff is Professor Emeritus of Intelligence and Security Studies. His book entitled *Ongekend en onderscheiden. De geheime geschiedenis van de MIVD* was commissioned by NLD DISS and the Netherlands Institute for Military History (NIMH) and will be published by Uitgeverij Boom in late 2022. He was granted access to the NLD DISS archives for research purposes, and unless explicitly stated otherwise, this article is based on his findings while conducting this research.

After the Second World War, the bar was raised even higher.

Ambitions and aspirations

Ambition was never lacking. After an inland security service had been placed under the auspices of GSIII in the neutral Netherlands in 1919, its leader, Major General J.W. van Oorschot, believed that the task of his service 'was far from a limited military one, and was of a much wider purport encompassing the entire population'.[1] When, towards the end of the Second World War and in the period shortly thereafter, plans were made to create one or more Dutch military intelligence and security services, the bar was raised even higher. Various parties believed that while the Netherlands might struggle to contribute militarily to the new allied partnerships, its intelligence work could more than compensate for this. The military intelligence organisation would enable the Netherlands to punch above its weight on the international stage.[2]

The fact that this plan had very little success was partly due to the fact that the Netherlands established three military intelligence services – the Army Intelligence Service (LAMID), the Air Force Intelligence Service (LUID) and the Naval Intelligence Service (MARID) – each operating entirely independently. When in 1987 the first Intelligence and Security Services Act stipulated that there would be just one Military Intelligence Service (MID), it took no less than thirteen years to create it and shed the remnants of the individual services. The new act that followed in 2002 stipulated that, in addition to the civilian service known as the Netherlands General Intelligence and Security Service (NLD GISS), the Netherlands Defence Intelligence and Security Service (NLD DISS) would also be established. Its director from 2006 to 2011, Pieter Cobelens, sought to have his service participate in what he referred to as the 'Champions League' of Western intelligence and security services.[3]

In addition to its international aspirations, from the Second World War onwards the Dutch military intelligence service strove to remain on an equal footing with its civilian counterpart, initially known as the National Security Service (BVD) and later as NLD GISS. The archives of NLD DISS and its predecessors reveal ongoing irritation with the arrogant attitude displayed by what it referred to as the 'ancillary service'. For a long time, the BVD's superior stance was due to the special powers it had been granted to conduct activities such as wire-tapping, installing microphones and covertly entering homes, all of which were denied the military services. For these reasons, the BVD believed that the military services had only a very limited counter-intelligence task that was not permitted to extend beyond the gates of military sites. Based on this difference in powers, the Chief of the General Staff G.J. le Fèvre de Montigny asserted in 1960 that the distinction between the BVD and the military services should not be based on the 'gates theory'. For him, the difference was simple: the BVD used improper

1 M. de Meijer, *De geheime dienst in Nederland*, 1912-1947 (unpublished) 177.

2 B. de Graaff and C. Wiebes, Villa Maarheeze. *De geschiedenis van de Inlichtingendienst Buitenland* (The Hague, Sdu, 1998) 33-34; F.A.C. Kluiters, *De Nederlandse inlichtingen- en veiligheidsdiensten* (The Hague, Sdu Uitgeverij Koninginnegracht, 1993) 43-44 and 240-241; F.A.C. Kluiters, *De Nederlandse inlichtingen- en veiligheidsdiensten. Supplement* (The Hague, Sdu Uitgeverij Koninginnegracht, 1995) 155-156.

3 'Het werk in Uruzgan is echt Champions League', BN De Stem, 7 June 2011; 'Directeur MIVD, Generaal-Majoor Pieter Cobelens verlaat binnenkort de dienst', in: *Ingelicht. Informatiemagazine voor de MIVD*, March 2011, 4 (4-5); E. van Outeren and S. Derix, 'Zondebok bij de politiek, succesnummer bij NAVO', *NRC Handelsblad*, 1 June 2011; O. den Hollander, 'Pieter Cobelens: "Nederland kan een digitale superpower worden"', Quote, January 2021.

PHOTO BEELDBANK NIMH

Chief of the General Staff G.J. le Fèvre de Montigny receives a British general. According to De Montigny, the difference between the BVD and the LAMID was simple: the former used improper methods while the latter used proper ones

methods and the LAMID used proper ones. Unsurprisingly, his proposal to lay down the distinction in formal regulations failed.

In the late 1990s, the chief of the MIS, Brigadier J.C.F. (Hans) Knapp, based his argument that the director of the service should be a two-star general entirely on the service's foreign and domestic aspirations. In his view, the second star was indispensable in dealing with the heads of foreign partner services and, moreover, was justified on the basis of the equality that now existed between the BVD and the MID. There were no longer any material differences between the two services in terms of staffing numbers and duties or, once the new law of 2002 came into force, in terms of powers. However, Knapp's argument was extinguished by the Director-General for Defence Personnel, who believed that the MID still lacked the same social relevance as the BVD.[4]

4 See also C. Wiebes, Intelligence en de oorlog in Bosnië, 1992-1995. *De rol van de inlichtingen- en veiligheidsdiensten* (Amsterdam, Boom, 2002) 120.

The argument used was that the BVD had developed a higher profile than the MID, which did not publish its first annual report until 1998 (after Knapp had issued his), while the BVD had been doing so for years. It also took another 10 years before a press conference was held to announce the publication of the MID / NLD DISS annual report. Following the terrorist attacks of 11 September 2001, political and public interest in NLD DISS grew, with the number of visits to the service by national authorities increasing sharply. The Parliamentary Standing Committee on the Intelligence and Security Services, which for many years had served only the BVD, began to treat the services as equal entities. The same was also true for the independent Review Committee on the Intelligence and Security Services, established in 2002. The directives that laid down the national intelligence requirements[5] for both services from 2003 onwards and the national security requirements[5] for the two services from 2015 onwards also contributed to their equality.

This equality became visible to a broader audience during debates in the run-up to the referendum on the third Intelligence and Security Services Act laid down in 2017, with the Director of NLD DISS, Onno Eichelsheim, and his NLD GISS counterpart, Rob Bertholee, regularly appearing side by side. The first major sign of the service's increased visibility was the press conference held in November 2018, during which Eichelsheim revealed how his service had thwarted a hacking operation by the Russian military intelligence service GRU at the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague.

Although there will always be some traditional rivalry between NLD DISS and NLD GISS, as Cobelens mentioned at his farewell in 2011,[6] the two services now work together on an equal footing in diverse fields. Moreover, their legitimacy in their own country is hardly debated, and both enjoy a sound international reputation.

Funding

Why did it take so long for the military services to achieve the prestige to which they always aspired? Above all, this was a matter of funding. The Agency for the Investigation of Foreign Armies founded in 1912, and initially also GSIII, were one-man businesses. Although GSIII grew into a workforce of two dozen employees during the First World War, this remained a small number for a neutral country that was to become one of the most important 'spy nests' for the warfaring countries.[7] This situation prompted the then head of GSIII, H.A.C. (Han) Fabius, to introduce a system that was in line with both the government's neutrality policy and its financial position. Individual employees in the service each maintained contact with the military attaché of a specific warfaring nation, who was stationed in the Netherlands. They agreed with these military attachés, and informally also with the leaders of the foreign espionage networks operating in the Netherlands, that while these intelligence services were permitted to operate on Dutch soil, they could only spy on other countries and not on the Netherlands itself, were forbidden to use violence or otherwise violate Dutch laws, and were required to share their information with the Dutch service.[8] By treating all parties

5 Referred to from that point as 'Integrated Directive'

6 'The Director of NLD DISS, Major General Pieter Cobelens, will soon be leaving the service'.

7 E. Ruis, Spionnennest 1914-1918. *Spionage vanuit Nederland in België, Duitsland en Engeland* (s.l., Just Publishers, 2012); W. Klinkert, '"Espionage Is Practised Here on a Vast Scale". The Neutral Netherlands, 1914-1940', in: F. Baudet, E. Braat, J. van Woensel and A. Wever (eds.), *Perspectives on Military Intelligence from the First World War to Mali. Between Learning and Law* (The Hague: Asser Press/Springer, 2017) 23-54.

8 See, for example, H.A.C. Fabius, 'De inlichtingendienst van den Generalen Staf. Het z.g. bureau G.S. III. Herinneringen uit de mobilisatiejaren 1914-1919', *Bijdragen voor Vaderlandsche Geschiedenis en Oudheidkunde*, series 7, part 8 (1937), 199-200 and 210-211 (196-212); A. Wolting, 'De eerste jaren van de Militaire Inlichtingendienst (GSIIIJ914-1917)', in: *Militaire Spectator* 134 (1965) (12) 566-51, 569; Ruis, Spionnennest, 78-79, 153, 192, 209, 227-228, 239; W. Klinkert, 'A spy's paradise? German espionage in the Netherlands, 1914-1918', in: *Journal of Intelligence History* 12 (2013) (1) 21-35, 21 and 24; idem, 'Fabius', 389; M. Smith, *Six. A History of Britain's Secret Intelligence Service* (London, Dialogue, 2010) 71-72; idem, 'Hendrik Anton Cornelis Fabius, 1878-1959. Stille strijder achter de schermen', in: W. Klinkert, S. Kruizinga and P. Moeyes, *Nederland neutraal. De Eerste Wereldoorlog* 1914-1918 (Amsterdam, Boom, 2014) 374-421; '*Neutraal Nederland was werkterrein van spionnen en contra-spionnen*. Men liet agenten rustig hun gang gaan en trok profijt uit gegevens van beide partijen', *Het Parool*, 2 July 1949.

Air Force intelligence personnel view photos. Various investigative committees emphasised the need for the military intelligence service to possess sufficient capacity of its own

PHOTO BEELDBANK NIMH

equally, at least officially, neutrality was maintained and GSIII had itself a good deal.

When a Central Intelligence Service was established in 1919, the government camouflaged this national security service division – referred to as GSIIIB – by accommodating it under the General Staff, with GSIIIA continuing to be tasked with gathering intelligence on foreign countries. It was precisely this camouflage that prevented the expansion of GSIIIB, since the government paid the service from the meagre funds for secret expenditure allocated by the Ministry of War. Since the government did not want to place GSIIIB in the public spotlight, its secret expenditure could not be drastically increased as this would have attract the attention of parliament.[9] Throughout much of its existence, GSIIIB consisted only of a director and an administrative clerk, assisted by the director's brother working in a pro bono capacity from 1930 onwards. When in the second half of the 1930s intelligence units were created in the navies in both the Netherlands and the Netherlands East Indies, their personnel could be counted on one hand.

The financial limitations that were imposed ultimately had a disastrous effect. The system that Fabius had introduced during the First World War became unbalanced in the 1930s because Germany was no longer cooperating. However, GSIII continued working as if nothing had changed. When, in November 1939, two British intelligence officers held talks near Venlo with individuals they believed to be representatives of the German military opposition to Hitler, they were accompanied by an officer of GSIIIA, Lieutenant Dirk Klop, who posed as a British national. After a German SS command had abducted the British and Klop on

9 See, for example, National Archives, The Hague, 2.04.26.01, Ministry of the Interior and Kingdom Relations, inv. No. 541, exh. 11 October 1919, No. 1095.

9 November and taken them across the border, the Germans found papers on the person of Klop (who had been killed in the incident), which revealed his Dutch nationality. This seriously discredited the Netherlands' neutrality policy, and Service Director Van Oorschot was forced to resign. When the Germans invaded the Netherlands in May 1940, they cited Klop's actions as one of the Dutch government's breaches of neutrality that legitimised their invasion.[10]

The Venlo incident brought home to the Dutch government that it would have to think carefully about what it was actually doing in the field of military intelligence and what it could confidently entrust to foreign partners. When it rolled out intelligence operations from within England, Australia and Ceylon (Sri Lanka) during the occupation of the Netherlands and the Netherlands East Indies, this necessity became even clearer. Because the governments of these two countries had left behind no organisations and the Resistance was struggling to find its way to unoccupied territory, the Netherlands and the Netherlands East Indies were the areas in Europe and Asia from which the least intelligence reached the Allies, at least initially.[11] This naturally caused irritation among the British and Americans, who therefore threatened to send out their own agents, which would of course have been an affront to Dutch sovereignty and a threat to national interests. The lack of transport and communication resources, among other things, also rendered the Dutch intelligence organisations dependent on their British and US partners.

Once the war was over, the Dutch had certainly learnt their lesson. However, the structure of the Dutch intelligence landscape was such that the military services had little material to exchange with foreign services. Operations by foreign agents were generally reserved for the civilian Foreign Intelligence Service (BID), renamed the Intelligence Service for Abroad (IDB) in 1972. The only material gathered by the Dutch services themselves which was of interest to partners related to signals intelligence and consisted of information received from the defence attachés in Belgrade and Warsaw (the only two Dutch posts behind the Iron Curtain) and material acquired during submarine patrols.[12]

This changed after the IDB was abolished in the early 1990s. From that point on, the MID and later NLD DISS began to conduct interesting intelligence operations involving human resources, which afforded the service prestigious allure in its contacts with foreign sister services. Also important was the conclusion reached consecutively by two separate committees, which stressed that NLD DISS required sufficient capacity of its own in order to continue independently collecting and analysing intelligence. The first was the Dessens Committee, which investigated the legitimacy and efficiency of the Defence organisation's intelligence and security capacity in 2005 and 2006, and the second was the Davids Committee, which in 2010 investigated the decision-making process in the run-up to the 2003 Iraq war.[13] This laid a solid foundation for a considerably expanded workforce, a foundation that was further reinforced by a system developed by NLD DISS itself in 2012 and which became known as Weighing and Prioritising. It was intended to confront recipients of the service's products with the costs involved in each request.

10 B. de Graaff, 'From seduction to abduction: how the Venlo Incident occurred', in: B. de Graaf, B. de Jong and W. Platje (eds.), *Battleground Western Europe. Intelligence Operations in Germany and the Netherlands in the Twentieth Century* (Amsterdam, Het Spinhuis, 2007) 49-70; B. de Graaff, 'Trefpunt Venlo: Amerikaans-Belgisch-Brits-Frans-Nederlandse spionagesamenwerking ten aanzien van nazi-Duitsland in 1939', in: *Mededelingen van de Sectie Militaire Geschiedenis van de Landmachtstaf*, part 15, The Hague 1993, 105-142.

11 L. de Jong, *Het Koninkrijk der Nederlanden in de Tweede Wereldoorlog*, IX (The Hague, Martinus Nijhoff, 1979) 890, 917, 927, 954 and 969; L. de Jong, XIV, 280-281; B. de Graaff, 'Hot intelligence in the tropics. Dutch intelligence operations in the Netherlands East Indies during the Second World War', in: *Journal of Contemporary History* 22 (1987) 568-569 (563-584); Ch. Cruickshank, SOE in the Far East (Oxford and New York, Oxford University Press, 1983) 137 and 150.

12 W. Platje, *Een zee van geheimen. Inlichtingenoperaties tijdens de Koude Oorlog* (Amsterdam, Boom, 2010) 22 and 197-198.

13 Research group on Intelligence and Security at the Defence department, *Inlichtingen en Veiligheid Defensie: Kwaliteit, Capaciteit en Samenwerking,* The Hague 2006; Report from the Committee investigating decision-making on Iraq (Amsterdam, Boom, 2010).

Government service or commanders' service?

For a long time it was also difficult to achieve a certain level of ambition because the military intelligence and security services were regularly at loggerheads as to their purpose. Until 1940, GSIII was partially a service for commanders. This was particularly true of GSIIIA, which was tasked with collecting information pertaining to orders of battle and the intentions of foreign armies. At the same time, GSIIIB was primarily a government service. It was set up by the government in 1919 in an effort to avoid a repetition of the incidents that had occurred in November 1918 during the Troelstra revolution. Around the time of the truce at the end of the First World War, when the thrones in Europe were teetering, the leader of the Social Democrats, P.J. Troelstra, believed that the Netherlands could use a revolution as well. Little came of his ideas, but some figures of authority had been so impressed that they were prepared to indulge him. The Central Intelligence Service/GSIIIB was therefore explicitly tasked with reducing any threats to their true proportions. As a result, the service had a tendency to minimise threats and, in particular, to focus on best-case scenarios.

After the Second World War, the LAMID, LUID and MARID believed that they existed primarily and almost exclusively to serve the commanders of the three branches of the armed forces. Conversely, the successive ministers – first the Ministers of War and the Navy and later the Ministers of Defence – had shown little interest in the military services for many decades. This only really changed in the first half of the 1980s, when the alleged involvement of the military attaché in Suriname, Hans Valk,[14] in the Bouterse coup and a number of counter-intelligence incidents relating to the Association of Conscripts (VVDM) and antimilitarists painfully exposed the lack of political control that existed at the time. This reinforced the demand issued by Parliament during the debate on the proposal that would culminate in the 1987 Act that the three services be merged into a single military intelligence service.

The structure of the Dutch intelligence landscape was such that the military services had little material to exchange with foreign services

However, more than a decade of conflict ensued between the successive heads of the MID and the central organisation on the one hand, and the commanders and their representatives at the central organisation on the other. The key issue came down to this: Whom exactly was the MID intended to serve? The ministry or the commanders? And should the service only collect strategic intelligence or also operational intelligence? In the late 1990s, this led to a major slump among MID personnel, who were constantly facing complaints that their intelligence products were not valued by their recipients in the armed forces.

Successive appointments of directors with extensive operational experience, including Joop van Reijn (1999-2002), Bert Dedden (2002-2006) and Pieter Cobelens (2006-2011), meant that MID / NLD DISS began viewing itself as a strategic service pursuing an operational objective. Once the service began providing on-site support to deployed units, it was occasionally even charged with providing tactical intelligence support. This was also a consequence of the fact that in crisis

14 E. de Vries, Hans Valk. *Over een Nederlandse kolonel en een coup in Suriname* (1980) (Zutphen, Walburg Pers, 2021).

management operations, the sharp distinction between the strategic, operational and tactical levels often disappeared. Nevertheless, there was still room for discussion on how and in what proportions intelligence support could be provided at the various levels. For example, NLD DISS performed the J2 task of the CHOD for several years under Dedden, but this was later reversed.

15 See also M.W. Jensen and G. Platje, *De MARID. De Marine Inlichtingendienst van binnenuit belicht* (The Hague, Sdu Uitgevers, 1997) 389-390; Wiebes, Intelligence en de oorlog in Bosnië, 145

The Directive and Integrated Directive also still had the potential to place NLD DISS in a situation in which it would be torn between meeting the wishes of the government and those of its military clients. In the 1990s, this became the fate of the Technical Information and Processing Centre, formerly MARID VI or Mathematics Centre (WKC), which carried out interception operations for both the government and the navy. The Admiralty Council had almost abolished the centre, since its usefulness to its own branch of the armed forces was unclear and the use of a frigate was therefore believed to be preferable.[15]

It was also problematic that the intelligence chain (NLD DISS's relationship with other Defence intelligence units) was not sufficiently tight. The Dessens Committee had already noted this in 2006,[16] and today this problem still appears not to have been fully addressed, since the old controversy between the central organisation and the commanders still seems to play a role behind the scenes. Apart from understandable conflicts of interest, one reason for this could be that the central organisation has constantly shied away from developing an overarching intelligence philosophy.[17] It always left this task initially to the Military Intelligence Service School and later to the Netherlands Defence Intelligence and Security Academy (DIVI).

New ambitions?

Perhaps formulating an intelligence philosophy is an ambition that NLD DISS should nurture. There appears to be a need for this, particularly since a number of traditional principles of military intelligence operations are shifting. Whereas a sharp distinction has always been made between intelligence and policy until recently, NLD DISS seems to be increasingly inclined towards defining perspectives for action. And while NLD DISS still mainly prefers to present objectifiable data behind the closed doors of government consultations, its British and US partners have begun to issue daily information concerning the course of the war in Ukraine and the intentions of the Russian regime.[18]

The past has proven that the successive military intelligence services were compelled to continually reinvent themselves in changing circumstances, since remaining static for too long involved risks. But over the past two decades, NLD DISS has demonstrated its ability to actively and promptly adjust its modus operandi, for example by conducting offensive operations that involve human sources or take place in the cyber domain. However, the fact that it has fulfilled many of its past ambitions is no reason for the service to rest on its laurels, particularly since changes in the task-related environment are occurring at an accelerated pace. Initially, changes were slow to occur, with nearly 30 years of neutrality policy followed by 40 years of allied cooperation during the Cold War. But the pace of change accelerated quickly from that point onwards, with activities ranging from providing support in crisis management operations between roughly 1990 and 2010 to combating terrorism from 2001 onwards and conducting cyber operations in the second decade of the 21st century. More recently, there has been a shift towards interstate and perhaps even large-scale conflict. Moreover, different threat aspects no longer displace each other but exist side by side. It is therefore time for an ambitious intelligence service to consider the future of its own modus operandi and facilitate the debate on this subject. ■

Over the past two decades NLD DISS has demonstrated its ability to actively and promptly adjust its modus operandi, for example by conducting offensive operations that involve human sources or take place in the cyber domain

PHOTO MCD, EVA KLIJN

16 Research group on Intelligence and Security at the Defence department, *Inlichtingen en Veiligheid Defensie: Kwaliteit, Capaciteit en Samenwerking*, The Hague 2006, 73, 90, 202 and 221-222.

17 See, for example, www.stichtingargus.nl, Report from the Executive Council of the NLD DISS, 5 November 2003.

18 B. de Jong, 'Amerikaanse inlichtingendiensten en de Russische invasie', in: *Clingendael Spectator*, 6 April 2022; W.P. Strobel, 'Intelligence Sharing Marks New U.S. Front In Information War', *The Wall Street Journal*, 5 April 2022; '"A real stroke of genius": US leads efforts to publicize Ukraine intelligence. Release of Russia's military woes is latest twist in novel spying strategy', *Financial Times*, 6 April 2022; K. Adam, 'How U.K. intelligence came to tweet the lowdown on the war in Ukraine', *The Washington Post*, 23 April 2022

The mysterious linguist in The Hague

Jaus Müller

There was recently an advertisement on the Dutch government's vacancy sites with a somewhat cryptic heading: 'Linguist in The Hague'. The text of the advertisement revealed that this was not just your average job grade 11 translation position: 'You will be working at the counter-espionage agency of the counter-intelligence and security department and helping protect Defence interests against internal and external threats in the short and long term'. The Netherlands Defence Intelligence and Security Service (NLD DISS), which placed this advertisement, was not just looking for an all-round languages whiz; a translation degree in translation or university degree in Mandarin Chinese was listed as an explicit job requirement.

The fact that NLD DISS is specifically looking for Mandarin-speaking counter-intelligence experts points to one of the intelligence service's focal areas at the moment: the Far East. Although the service's activities almost always remain secret, the main areas of focus can be deduced from the service's public annual report: the first chapter of the annual report published in April 2022 touches on the Russian Federation, China and Afghanistan (with Afghanistan receiving far less attention than in previous years).[1]

Intelligence capabilities are scarce. Someone who watches too much James Bond may think that intelligence officers spend the bulk of their time in international cocktail bars, eavesdropping on secrets in between vodka martinis. The reality is that the real intelligence work is much less exciting and is hidden behind complex supply and demand management. After all, intelligence services work with clients, also known as 'requisitioners'. At NLD DISS, these include the Central Staff and the four operational commands (army, navy, air force and Marechaussee), who are always at the ready to jump on intelligence from the service. All these interests sometimes conflict with each other. Since the invasion of Ukraine, for instance, demand for intelligence on the Russian Federation has dominated, while international security experts agree that the long-term focus may need to be more on China.

Paul Abels, Professor of Governance of Intelligence and Security Services at Leiden University, warned against this possible politically-guided short-term thinking in his farewell lecture last May. 'Requisitioners have a strong tendency to ask about yesterday's known threats, while the reality always goes beyond their imaginative capabilities,' Abels said. 'In theory, the services are given room for what is known as their "scanning task", to track down as-yet unknown threats, but the focus is mainly on keeping requisitioners happy and every effort in another new area will detract from this. Furthermore, the services are always overstretched, which is inevitably also at the expense of capabilities and focus in relation to recognising new threats.'

Intelligence work therefore means constantly making choices: let's imagine NLD DISS only has the budget for one linguist. Should they be looking for a Russian-speaker or a Chinese-speaker? Since the Russian invasion in Ukraine, it seems justified to focus all of the intelligence service's reserve capacity on the Russian Federation. But in early August, the Chinese People's

Liberation Army started a large-scale exercise in the waters around Taiwan. So should we be looking to the East (Russian Federation) or the Far East (China)? Quickly move some people from the Russian department to the China floor at NLD DISS, then? That's not how it works in the world of intelligence. Training staff takes time (you cannot just learn Mandarin in an afternoon) and networking, building knowledge and trust also take years.

You might ask yourself, why do we all need to be spending time and money on that? Why can't the Netherlands just rely on US information when it comes to Taiwan, for instance? In theory, that could be possible, but history teaches us that even the US sometimes has a nasty habit of not always telling the truth. Take the time when Colin Powell (who, incidentally, President Bush also shoved into the limelight to clean up the scandal) appeared at the UN Security Council in 2003 and told the world with a straight face that some tube or other of sandbox sand was actually Iraqi anthrax. This served as the basis for why the Netherlands also had to provide political and/or military support for an invasion of Iraq. NLD DISS (and to a lesser extent the Netherlands General Intelligence and Security Service - NLD GISS) systematically raised doubts about claims of possible Iraqi weapons of mass destruction. In a response to Powell's presentation, for example, NLD DISS wrote in an internal memo in 2003: 'The smoking gun has still not been found!'[2]

If the first Dutch cabinet headed by Jan-Peter Balkenende had listened more to the nuanced intelligence officers and less to Powell, the Netherlands would not have had to provide political support for the 2003 invasion which was illegal under international law. In hindsight, the critical analyses by NLD DISS hit the nail on the head: after all, the weapons of the then Iraqi leader Saddam Hussein were never found. At the time, the Dutch intelligence reports differed from the British and American reports on important points, with the Davids investigative committee writing in 2010: 'These other conclusions did not seem to be based so much on other independently-acquired intelligence sources, but instead on their own military technical analysis of the information provided.' This highlights the importance of well-informed, well-trained intelligence analysts, who studied information independently and made a series of sobering analyses on that basis. Unfortunately, the somewhat hawkish ministers in the Balkenende government ignored those recommendations.

Should that linguist speak Chinese, or perhaps Russian?

All in all, those properly skilled intelligence analysts can come in handy. Especially if some US officer or other were to start crying out about some threat from Chinese armed forces that may or may not be unavoidable. Then it would be nice to know that NLD DISS had in any event hired that Chinese linguist in The Hague on time so that it could assess the situation for itself. We can only hope that future ministers will indeed listen to NLD DISS, unlike their counterparts in 2003 in relation to Iraq. ■

1 See: Defence Intelligence and Security Service, *Public Annual Report 2021* (The Hague, 28 April 2022).
2 Quoted in the *Davids Committee Report 2010* (The Hague, 2010) 307.

‘Paid agents (lesser sort)‘, ‘play acting’ and the Dutch national character

‘The Intelligence Service is an indispensable reconnaissance body within the General Staff, not only to serve the Operations department, but also to assess the politico-military situation in peace time. No commander will neglect to first investigate what is known of the enemy before issuing orders.’[1] This is how, in 1921, then captain H.A.C. Fabius summarised in the *Militaire Spectator* the raison d’être of the military intelligence service, of which he was the de facto founder.

PHOTO BEELDBANK NIMH

Dutch Lieutenant Colonel Th.F.J. Muller Massis (front row left) accompanied by military attachés from other neutral countries visits the Gutehoffnungshütte industrial complex in Oberhausen during the First World War

It is the task of of intelligence work 'to collect data about the potential enemy, wherever and however is required'

Fabius himself actively contributed to charting out the politico-military situation in other countries and published situational overviews in the *Militaire Spectator* from 1914 onwards. Having taken over the Agency for the Investigation of Foreign Armies in 1913, he oversaw its transformation into GSIII a year later.

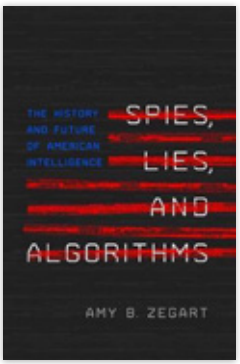
In his 1921 article, Fabius reflected on the influence of the First World War, or the Dutch neutrality policy, and the subsequent threat of revolution in Europe, on the intelligence domain. He noted that the Ministries of War, Navy, Colonies, Foreign Affairs and Justice had a vested interest in intelligence, but considered 'a strictly-implemented centralisation necessary' for the assessment of reports. In his article, Fabius also discussed the ways in which intelligence was gathered. For example, providers of intelligence also included the military attachés, who did 'nothing secretive', but who were solely involved in the 'study of the army configuration' in the country in which they were stationed. The attaché would not consort with agents, 'who could just as well be directly or indirectly spying on him under false pretences.'

In the event of a longer-term war, according to Fabius, vigilance was called for against false propaganda messages with political intentions. These messages could have come from both 'deliberate and inadvertent agents'. The first category included 'paid agents (lesser sort)'; the second group included people who, 'due to exaggerated feelings of sympathy', had become 'inadvertent instruments' of the enemy. During the First World War, there were agents active in the Netherlands who wanted to obtain information about their enemy 'via an impartial territory', or information about the neutral Netherlands itself. Fabius referred to the latter as 'spies within the meaning of the Penal Code' against whom real action needed to be taken.

Lieutenant Colonel A. Wolting made reference in the *Militaire Spectator* to an interview in which it was said that Dutch officers even felt that 'espionage was beneath them' in the run-up to the Second World War because the 'play acting' reportedly did not mesh with the Dutch national character. But it is ultimately the task of intelligence work 'to collect data about the potential enemy, wherever and however is required!' wrote Wolting.[2] ■

1 H.A.C. Fabius, 'De Inlichtingendienst bij den Generalen Staf', *Militaire Spectator* 90 (1921) 397-408.

2 A. Wolting, 'De eerste jaren van de Militaire Inlichtingendienst (GSIII, 1914-1917)', *Militaire Spectator* 134 (1965) 566-571.



Spies, Lies, and Algorithms

The History and Future of American Intelligence
By Amy B. Zegart
Princeton (Princeton University Press) 2022
424 pages
ISBN 9780691147130
€30

There is certainly no shortage of spytainment, the term used to refer to espionage-themed entertainment. It features in books, films and television series, including *Homeland, CSI, 24*, and characters such as Jason Bourne, Jack Ryan and, of course, James Bond. However, according to Amy Zegart, while spytainment is everywhere, spy facts are scarce. Public knowledge about the why and how of intelligence services is very limited, not just because these services themselves are by nature secret or secretive. There is also relatively little attention given to intelligence work in academia, especially in international relations and in the broader political sciences. In her second chapter, Zegart, affiliated with Stanford University, explains clearly why such a lack of public knowledge about intelligence is problematic. If the only source of information is spytainment, the public gets a distorted picture of the intelligence world. Her own surveys show that spytainment fans attribute more power and capabilities to intelligence services than they actually possess, are more in favour of torturing terrorist suspects and estimate that there is less supervision than there is in reality. This can feed conspiracy theories, complicate debate on surveillance and spread misconceptions about torture. After all, the latter is both unethical and ineffective. The lack of knowledge carries through to the political and administrative level, with Zegart claiming that there are more Congress members with knowledge of milk powder than knowledge of intelligence services. The dean of West Point, Brigadier General Patrick Finnegan, was once so concerned that the series *24* glorified the torture of terrorist suspects among cadets that he visited the film set to ask whether they could also make an episode where torture had the opposite effect to what was intended. When he appeared on set in uniform with this request, people thought he was an actor.

18 intelligence services

The misconceptions about intelligence are the prelude to Zegart's book *Spies, Lies, and Algorithms*, an ambitious work aimed at providing a thorough background on intelligence and espionage. As a political scientist, Zegart has been investigating US intelligence services for thirty years. She previously wrote the book *Spying Blind. The CIA, the FBI, and the Origins of 9/11*. As she herself states, she does not inhabit the intelligence world (she has never worked for a service), but is a visitor. As an outsider – who, in addition to literature research, has spoken with many intelligence service employees – she has a fresh view on this rather closed world. On the one hand, she understands the challenges facing services and the high expectations they have to meet. Intelligence services must, for instance, generate high-quality intelligence, anticipate international developments and events in good time (preferably predict these), and do all of this without infringing on the privacy of others. James Clapper, director at the time of the US intelligence community (DNI), once referred to this as the problem of 'immaculate collection'. On the other hand, Zegart does not shy away from speaking out when it comes to the failure of the services, in terms of analytical mistakes and organisational misconduct alike. Her book is deliberately broad in scope – the subtitle is 'the history and future of American intelligence'. This is a huge field of research. The US now counts 18 intelligence services (but an organisation only counts if it has a three-letter acronym), more than 100,000 employees, some 4 million 'clients' who have security clearance, and all for a price tag of $85 billion per year. In short, more than the GDP of a considerable number of countries.

Pitfalls in the thinking process

The core of the book is made up of four chapters: a historical background of American intelligence; the principles of intelligence work (knowns and unknowns), why analysis is so difficult, and covert action. All the chapters include tables and text blocks that elaborate on certain cases. The historical context is original because Zegart

goes back as far as the US War of Independence, in which George Washington managed, partly through espionage, ruses and deceit, to get the upper hand over the English, who are, after all, known as masters of the genre. Some examples from the Korean War are also well described. For example, General Douglas MacArthur was convinced that if China were to become involved in the war, its soldiers would have no chance whatsoever against the well-trained American soldiers. Things took a different turn, however. It brings to mind Russian President Putin's expectation at the beginning of 2022 that Ukraine would be under his control within a matter of days. Incidentally, this conflict is not described in the book; it was already at the printer at the time of the invasion. The chapter on analysis is also very worthwhile and describes various pitfalls in the thinking process (such as cognitive biases). Each chapter includes well-described case studies. From FBI mole Robert Hanssen, to Saddam Hussein's non-existent weapons of mass destruction and the hunt for Osama bin Laden; Zegart describes it all in beautiful detail.

Digital themes

A small point of criticism is the rather meagre discussion of the subject of cyber espionage. The word 'algorithm' in the title is seldom revisited in the book. This may be unavoidable given the broad focus of the work. The chapter on open-source intelligence focuses mainly on nuclear proliferation, but could just as well have devoted more attention to Bellingcat and algorithms, which have proved so effective in exposing Russian intelligence officers. The last chapter rushes headlong through the topics of online disinformation and offensive and defensive cyber operations. This deserved an extra chapter, with more conceptual distinction between the complicated digital themes. Regardless, Zegart's latest work certainly deserves a place on the bookshelf. For those who have had some introduction to intelligence studies, the work offers a fresh and broad perspective, with particularly the chapter on public knowledge and perception and the chapter on the US supervisory system adding new data and insights to the existing literature. The book is also a gold mine of source references. The text takes up some 275 pages, but Zegart also provides about one hundred pages in end notes and a short bibliography. Nonetheless the book will be most useful to people who are interested in intelligence but who do not yet have an overview of or grip on the field. In short, anyone who does not know the distinction between a case officer (or operator) and a source or an agent is advised to speedily acquire this book. *Spies, Lies, and Algorithms* will undoubtedly also appeal to fans of spytainment, because even though it has been written from an academic perspective, the interesting anecdotes, well-written stories and fluent writing style make the book especially entertaining.

Dr Sergei Boeke, Political Adviser at JSEC

Hackers

The internet's freedom fighters
By Gerard Janssen
Amsterdam (Thomas Rap) 2022
304 pages
ISBN 9789400408371
€22.99
Currently only available in Dutch

Hackers are often portrayed stereotypically: hoodies, a dark room, a screen with incomprehensible lines of computer code. Over the past several years author and journalist Gerard Janssen, has immersed himself in this mysterious world, with which he, like most readers probably, was previously unfamiliar. The book *Hackers* is the result of his quest. Breaking into a computer system is called hacking. Hacking is often done with malicious intent, but it can also be done to test a system for security. Janssen's book is about who these hackers actually are. It is not an analysis of how hacking works from a technical standpoint, what the impact of this is or how to take action against it. Janssen does write about that, but with the intention of explaining how a hacker thinks and operates. Janssen's quest starts from

journalistic necessity: he must have facts and sound sources. But, he admits himself, it is also a world that fascinates him: a Marvel Comics world with people with 'online superpowers'. He did not need to look far afield for some leads because the Netherlands proves to have both a capable hacking community and a great deal of IT knowledge and experience to protect against hacking. For example, it was a Dutch person who notified the White House of the poor security of then president Trump's Twitter account and we have all heard of Fox-IT, which shows up in the media to give an explanation every time another major hacking incident occurs.

Guardians and malefactors

Hacking started with good intentions by curious students in the 1950s who had their computers play games with each other and magically caused messages to appear on each other's screens. In order to do so, they had to understand the functioning of the system of digital pathways of the computer, the operating system and application software. And, decades later, how communications are routed via the internet. The idea was to help people and technology, for example by detecting vulnerabilities that pose a risk to safe use of the internet and everything that is connected to or dependent on it. These hackers, as they are now called, see themselves as the guardians of the free internet, which they consider to be the 'last great bastion of freedom of thought, ideas and expression'. They observed that governments and big business want to keep control and 'always (opt for) functionality over safety (of the user)'.

But soon a group of hackers arose who use their knowledge to steal and exploit information for their own gain. The culture of ethical hacking, denoting the difference between those with good intentions and those with malicious intentions, is entirely alien to them. They have taken the path of spreading malicious viruses, using phishing techniques, launching DDOS attacks et cetera. This is what the author describes as the criminal side of hacking, which is particularly rampant in the Russian Federation. It is therefore certainly appropriate that Janssen quotes the Netherlands Public Prosecution Service on the criminal nature of hacking. He also mentions the existence of hackers with political activist objectives.

Janssen gradually penetrates further into the world of hackers on his quest. There are descriptions of all kinds of special meetings, often in places where hackers feel the safest and most comfortable: their *hackerspaces*, or during major hacking gatherings at home and abroad. The world of hackers is really not only to be found 'underground'. When he succeeds in gaining their trust, the hackers provide Janssen with information, albeit sparsely, about what they are capable of: how they are able to break into the IT systems of governments, companies and organisations, what kind of information they find and what they could do with that. But also how nonchalant or even hostile the reaction is if this kind of security leak is reported. For the rest, Janssen is careful not to get involved in the criminal parts of this world himself. What he learns about this comes second-hand from hackers and security experts.

Personal traits and qualities

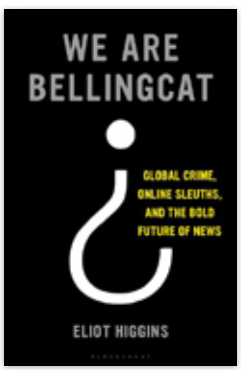
The conversations and meetings also provide Janssen with the information that allows him to tell more about the hackers themselves. Janssen devotes ample attention to the personal traits and qualities of the people he meets. It is a sobering story about what starts as an innocent challenge – which comes with being young and knowing a lot about computers – and often ends up leading to an isolated and distrustful existence. It is a closed world. The outside world does not trust them, they do not trust the outside world. Conspiracy thinking is not alien to hackers. Some are sometimes literally constantly on the run. The hacker environment remains mysterious, with its own rituals and etiquette. Nor does the 'nerdy' image, which hackers seem to be happy to confirm, go unmentioned. Janssen does his best to place this alongside positive qualities, such as mutual tolerance, idealism and willingness to help each other and – on a personal level – their perseverance and inventiveness; they are intelligent and critical, according to him. However, those positive traits and the fact that many hackers turn out to have ordinary and responsible jobs in everyday life, often precisely in the IT world, do not allow this book to overturn the generally negative image that exists of hackers.

Janssen leaned heavily on the willingness of hackers to share knowledge and information with him for the writing of this book. A paradoxical situation: the author who wants transparency and the conversation partners who prefer to remain hidden. This tension is noticeable when reading this book. Not everything is said and not everything was written down, Janssen admits.

Janssen has written an entertaining book that certainly holds the reader's interest. He seems to

capture the atmosphere of the hackers' world well, including by using colourful hacker jargon. In order to be able to place these exotic terms, the author has included, very helpfully, an extensive explanatory glossary. For the lay person who wants to know more about hackers than just the usual stereotypes and who wants to know how widely hacking is applied, this book is certainly worth a read.

Lieutenant Colonel Jan-Leendert Voetelink



We are Bellingcat

Global crime, online sleuths, and the bold future of news
By Eliot Higgins
Amsterdam (Spectrum) 2022
272 pages
ISBN 9781526615732
€23.99

In 1979, Italian historian Carlo Ginzburg wrote an article on a new form of scientific thinking at the end of the nineteenth century.[1] In it, he discusses a series of articles from 1874-1876 by Italian art historian Giovanni Morelli. In these articles Morelli attacked the practice at the time of attributing paintings. European museums were allegedly full of paintings attributed to the wrong artists. The so-called art experts, according to Morelli, went about it the wrong way. Specifically, they focused on the most eye-catching aspects of paintings, such as the smiles that Leonardo da Vinci often gave his portraits. Elements that were easy to fake, Morelli argued, not least because those very pieces of art were taught in certain schools. For that very reason, it was important to study the 'most negligible details': earlobes, nails and the shape of fingers and toes.[2] Not entirely coincidentally, Ginzburg argues, we see the same kind of attention to detail in Arthur Conan Doyle's books about Sherlock Holmes. Holmes also explicitly focuses on the smallest details that everyone else overlooks, thus going on to solve the most complex crimes. Ginzburg sees a new scientific paradigm in this: the 'paradigm of the trace', with an eye for what is in the background and not in the foreground. You will have to focus on the 'infinitesimal', Ginzburg says: only the marginal, the details – the fingernail or discarded match – allows the observant observer to penetrate to a deeper reality.[3]

1 Carlo Ginzburg,'Clues. Roots of a Scientific Paradigm', Theory and Society 7 (1979) (3) 273-288.
2 Ginzburg, 'Clues', 273-274.
3 Ginzburg, 'Clues', 280.

Bellingcat

Eliot Higgins, founder of the open-source platform Bellingcat, is a bit like Morelli. In his book *We are Bellingcat. Global crime, online sleuths, and the bold future of news,* Higgins outlines the history of this group of digital civilian detectives and journalists. Like Morelli – who tried his method and managed to attribute a number of high-profile paintings to other artists – Higgins is keen to show what painstaking online research can achieve. And not without reason: Bellingcat now has an impressive portfolio – and this book is also best read as a portfolio. It consists mainly of summaries of the course and results of Bellingcat's digital sleuthing during the Arab Spring, the Syrian Civil War, the MH17 investigation, far-right violence in the United States, Islamic State executions, violent crimes in Libya and the murder of Sergei Skripal. The common thread – and core idea of Bellingcat – in these investigations is that the truth is hiding in the details. Ginzburg could not have wished for a nicer counterpart to the paradigm of the trace, even though Bellingcat puts *digital* traces at the centre. During the Arab Spring in 2011, Higgins noted that many journalists were using footage of dubious origin, mostly from involved parties. Many photos and videos that served as evidence were misinterpreted as a result. He set out to date and geolocate photo and video footage that had been presented to the world via social media or otherwise. The MH17 investigation and the murder of Skripal are perhaps the most spectacular examples.

Is Bellingcat thereby acting as a 'secret service for ordinary people' (p. 20)? There is no doubt that Bellingcat conducts admirable as well as relevant investigation. Tracing and verifying online material for truth-telling purposes requires systematic, meticulous and time-consuming work from which there is much to learn. Especially regarding attribution issues – digital or otherwise – which is in the purview of intelligence and security services. But the objectives, activities and handling of data acquired by these services, from public sources or otherwise, are broader and different from Bellingcat's, such that the characterisation 'secret service' misses the mark. Intelligence and security services in a democracy serve the security of state and society. Independence, objectivity and speaking truth to power is the common adage. Yet their work is not outside the political realm. In the event of a political decision to undertake a military mission or combat jihadist terrorism, military and civilian services cannot avoid reporting on it regularly. Services can maintain professional distance but are not separate from politics. In contrast, Higgins claims to have nothing to do with 'political agendas' (p. 34). However, one could consider Bellingcat's choice of topics as a political act: why look at Rupert Murdoch's eavesdropping scandal? And the mere fact that Bellingcat cooperates with police forces means taking a stand against the Russian and Syrian states, for example. And the 'declaration of war' on the 'counterfactual community' is not apolitical either, of course.

A second important element of Bellingcat's identity concerns its distance from the subject. At several points in the book, Higgins stresses that the lack of language and cultural knowledge actually allows Bellingcat to look at the details. For intelligence and security services, the Bellingcat method of digital digging may be important, but without military experts, linguists, historians, or technical specialists, all that can be determined is where and when a photo or video was taken. The meaning of what can be seen, or what has been said or done requires active interpretation based on relevant – and thus context-related – knowledge and skills.

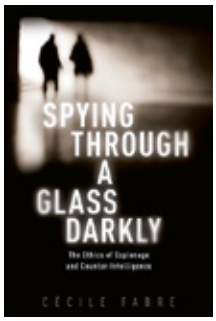
This brings us to a final difference. In addition to attribution activities for events that are in the past – either to identify perpetrators or draw lessons – secret services are there to give early and strategic warnings. They must warn about national security risks to enable other players to take action. This presupposes that they make statements about possible, future actions of states, groups and individuals. In doing so, it is not enough to be transparent, like Bellingcat; after all, the facts do not speak for themselves as they do for the digital forensic tracking in which Bellingcat engages. On the contrary, the context in which statements and actions are to be understood plays a major role in the interpretation of a threat.

Secret service or Sherlock Holmes?

Higgins, in his enthusiasm for Bellingcat's online research, can be blamed for what critics accused Morelli of a century and a half ago: positivism – understood for convenience as the unshakable belief in the irrefutable existence of (observational) facts. According to Ginzburg, this is fundamental to the paradigm of the trace, which calls for attention to the infinitesimal and marginal. Therein, after all, lie the facts that provide access to a deeper truth. Higgins believes the same thing. The facts are there for the taking in the public domain; just hidden in the details, like the metadata of a file, a minaret in the background, or a faint plume of smoke that is in view for just a second. That, however, does not make Bellingcat a secret service for ordinary people, rather a public Sherlock Holmes – a detective engaged in fact-finding in the context of investigating perpetrators. This does not diminish the importance of this open source research. An independent organisation which fact-checks and is thorough and innovative in doing so is an important ally for ordinary citizens, especially in a time of information overload and disinformation.

Dr C.W. Hijzen, research fellow at the Institute of Security and Global Affairs of Leiden University
Dr A. Claver, Ministry of Defence

NOTABLE BOOKS



Spying through a Glass Darkly

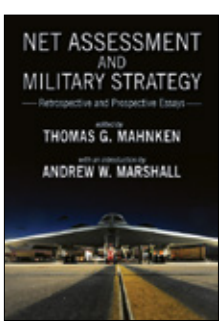
The Ethics of Espionage and Counterintelligence
By Cecile Fabre
Oxford (Oxford University Press) 2022
272 pages
ISBN 9780198833765
€36

In *Spying Through a Glass Darkly*, Cecile Fabre, professor of political science at the University of Oxford, addresses the ethical side of espionage and counter intelligence. Among the issues the author raises is whether it is morally permissible for employees of security services to cheat, bribe or extort people or manipulate them to obtain state secrets. And is it moral for states to monitor their own populations *en masse*? According to Fabre, in the context of war or foreign policy, such operations are ultimately justified only as a means – nothing more – of protecting one's own security and that of allies.

Ongekend en onderscheidend

The secret history of the Netherlands Defence Intelligence and Security Service
By Bob de Graaff
Amsterdam (Uitgeverij Boom) 2022
448 pages
ISBN 9789024444649
€34.90
Currently only available in Dutch

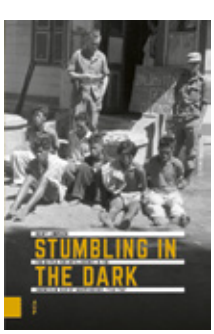
In *Ongekend en onderscheidend*, Bob de Graaff describes the history of NLD DISS and its predecessors and how they have operated internationally since 1912, including in the period of neutrality before the Second World War, the Cold War and the fight against terrorism in the 21st century. The intelligence services of army, air force and navy were forced to work together in one service in the late 1980s. After a rough start, the service rapidly professionalised and gained prestige, including among foreign partner services. De Graaff describes these developments using case studies such as countering Russian espionage in the Netherlands and intelligence support for Dutch troops in Afghanistan.



Net assessment and military strategy

Retrospective and prospective essays
By Thomas G. Mahnken and Andrew W. Marshall (eds.)
Amherst (Cambria Press) 2020
272 pages
ISBN 9781621965398
€40

In the volume *Net assessment and military strategy*, experts explain how net assessment uses a multidisciplinary approach to identify the military strengths and weaknesses of a competitor or adversary. During the Cold War, such analyses gave senior policymakers critical insights into the relative military clout of the US against the Soviet Union over a given period. However, the volume not only looks back, but also considers the future of net assessment, with the main topics being competition with China, the fight against radical Islam and – as a legacy of the Soviet Union – the Russian Federation.



Stumbling in the Dark

The Battle for Intelligence in the Indonesian War of Independence, 1945-1949
By Rémy Limpach
Amsterdam (Amsterdam University Press) 2023
272 pages
ISBN 9789463727181
€24.99

In their quest for military successes, the Netherlands and Indonesia engaged in a grim intelligence battle during the Indonesian war of independence from 1945-1949. In doing so, they used espionage, infiltration and other – often extremely violent – means, including when interrogating prisoners, concludes Rémy Limpach in *Stumbling in the Dark*. The author focuses on the actions of the Dutch troop intelligence services. Among other things, he describes how the Dutch and the Indonesians set up a widespread alarm system, which was supposed to give early warning of attacks to their own units. Limpach's publication is part of the series *Independence, Decolonization, Violence and War in Indonesia 1945-1950*.