‘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.

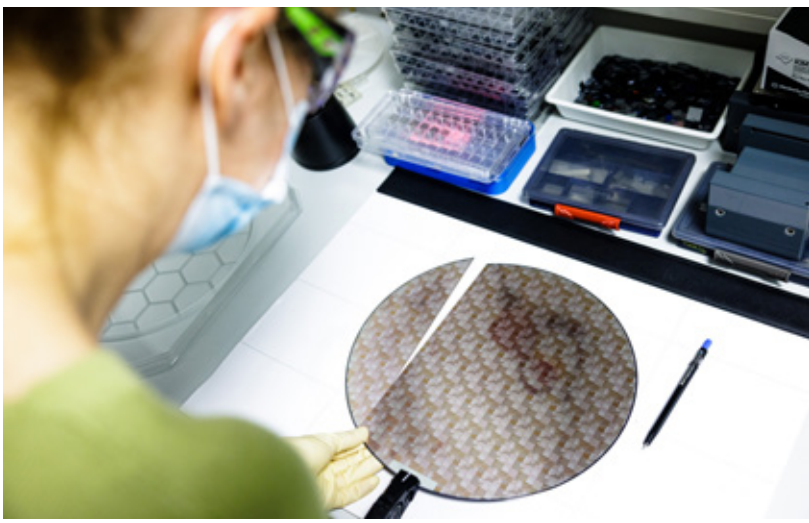
General Eichelsheim: Cooperation between the Defence Cyber Command (DCC) and NLD DISS could be better. Synergy could certainly be amped up, particularly to enable rapid and effective action in the cyber domain, where no distinction is made between the strategic, operational and tactical levels. Offensive 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)