



WOLSE: DRONE FOR EVERY SOLDIER



CYBER THREAT IS DANGEROUS



VERGOUW: CHAIN OF STRONG LINKS



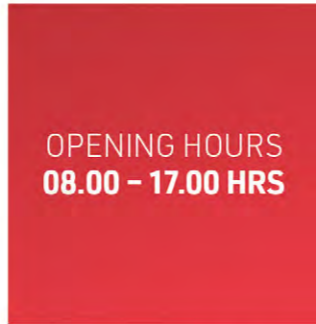
POWER OF SOCIETY

NEDS

NIDV EXHIBITION DEFENCE & SECURITY

35TH EDITION
THURSDAY NOVEMBER 21, 2024
AT ROTTERDAM AHOY

LEARN ALL ABOUT THE LATEST DEVELOPMENTS IN THE
FIELD OF DEFENCE AND SECURITY IN ONE DAY!

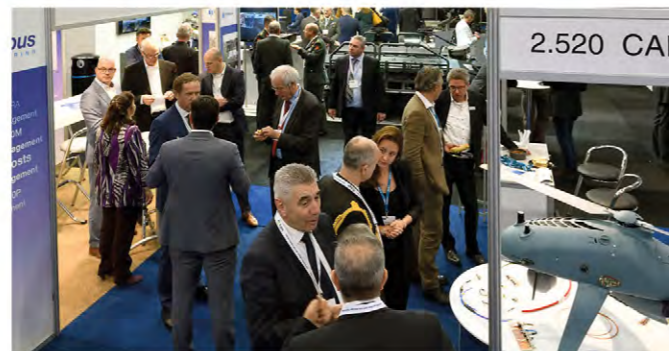


LARGEST DEFENCE AND SECURITY CONFERENCE & EXHIBITION IN THE BENELUX

NUMBER OF VISITORS
2500 DECISION MAKERS

Types of visitors
Government agencies,
companies, politics,
knowledge institutes,
international companies,
Ministries of Defence,
Economic Affairs and Climate,
Foreign Affairs, Justice,
Security Regions, Police
Corps, Coast Guard and
military attachés

More information:
www.nidvexhibition.eu



From our chairman

The Netherlands Industries for Defence and Security Foundation (NIDV) turns 40 this year. NEDS is also celebrating an anniversary this year with its 35th edition – and we are bigger than ever! The exhibition is sold out and the number of registered visitors is higher than previous years.

That is not surprising considering the current geopolitical situation. After all, many actions need to be taken after decades of budget cuts. The armed forces need to get back to full strength. Greater (inter)national collaboration is needed, we must take a more strategic posture at the availability of raw materials, the reliability of supply chains and most importantly: production capacity must rise rapidly. After all, as the US National Defense Industry Strategy rightfully states: production is deterrence.

The good news is that various countries are making the necessary budgets available to invest in our overall security. It is important to ensure the right preconditions and a level playing field with like-minded nations. That is essential for scaling-up and for true long-term collaboration.

The recently presented Dutch Defence White Paper includes a lot of these policy intentions and actions. One of them, a strategic partnership between the Ministry of Defence, the industry and knowledge institutions, is a precondition to scaling up, developing technology and strengthening the Dutch defence industry in the time ahead.

After all, tomorrow's challenges are much greater than those we faced in the times of the bipolar world. The threats come from all directions and have various dimensions and guises. The most dangerous threats are those that we perhaps do not see directly in our open society, but which could have potentially disruptive consequences.

Therefore, effectively investing in national security and defence is needed now more than ever. That is only possible if government and industry join forces and are supported both at a political level and in society.

All these parties come these days together at NEDS. I hope you have an interesting NEDS with many successful meetings. Let's get started!



Raymond Knops
Chairman of the board of NIDV

CONTENTS

- Drone for every soldier 4
- Cyber threat is dangerous 8
- KPN wants strong links 15
- Opening doors with PIB 20
- Power of society 26
- Civil defence Sweden 30
- Colophon 35

Cover: The use of drones and other unmanned weapons systems is on the increase in the Dutch armed forces. Companies are welcome to get involved. At battalion and brigade level, the mini-UAS Puma and the X-300 Integrator (pictured) have been in use for some time. However, these unmanned reconnaissance systems are specialised and scarce. Several systems will be on display at the Defence plaza during the upcoming NEDS, with the so-called 'Orange Puma' as the eye-catcher.

Photo: Mediacentrum Defensie

The Reaper, 'an aircraft with no human on board.'



The use of drones and other unmanned weapons systems is on the increase in the Dutch armed forces. Companies are welcome to get involved. 'We can stick a box like that in the Puma.'

'Flying binoculars' for every soldier

Text: Riekelt Pasterkamp
Photos: Mediacentrum Defensie

Soldiers of the future will carry a mini drone to collect information as part of their standard equipment. 'Sort of flying binoculars,' says Mr. Jos Wolse. And he should know as head of the Unmanned Aircraft Systems (UAS) management bureau at the Ministry of Defence's Material and IT Command (COMMIT).

Wolse's department is in Utrecht at the Kromhout Barracks, and he deals with all unmanned aerial vehicles within the armed forces, 'from 20 grammes to 20 metres.' Or: ranging from the tiny Black Hornet to the Reaper, 'an aircraft with no human on board.'



The so-called 'Orange Puma' is the eyecatcher at the Defence Plaza at the upcoming NEDS.

Several of the UASs used by the Ministry of Defence are listed in a catalogue, and users can take their pick. There is some variation in terms of cost and training. 'Furthermore, Defence uses the Wasp, the Raven and Puma as a "family". They can all be operated from the same ground station.'

Various systems will be presented at the Defence Plaza at the upcoming NEDS, with the so-called 'Orange Puma' as the eyecatcher. 'This drone has been given a green registration number, and we can carry out trial modifications above military grounds.' So, flying the unmanned systems above training grounds is not an issue. 'Outside those areas, however, we need to comply with all sorts of certifications,' Wolse says.

Crucial

In Wolse's opinion, there is no denying that drones will be crucial on the battlefield of the future. 'I've been working at Defence for the past 25 years and have sometimes felt like a voice crying out in the wilderness. But it's become topical since the general public has seen live how a Ukrainian drone strikes a target.'

Drones Action Plan

The Dutch company DeltaQuad is going to deliver advanced Intelligence, Surveillance & Reconnaissance (ISR) drones to Ukraine. In mid-October, the Ministry of Defence announced it is buying the drones for 42.6 million euros.

That purchase is the first concrete implementation of the Drone Action Plan that Minister Ruben Brekelmans announced during his visit to Ukraine.

The unarmed ISR drones can fly for a lengthy period and far. They are used to receive real-time information about the battlefield, gather intelligence and do surveillance.

At the same time, modern drones must be equipped with the latest technology to remain invisible, to resist jamming and operate autonomously if they temporarily lose contact with the home base.

Four hundred million euros has been earmarked for the Drones Action Plan, half of which is destined for the Dutch industry, claims the Ministry of Defence. According to the Ministry of Defence, the purchase is also an incentive for further specialisation and expanding the Dutch ecosystem of drones in the Dutch industry. Specialisation and scaling-up are required to drive the production of advanced drones as a whole.

Wolse's department deals with all unmanned aerial vehicles within the armed forces, 'from 20 grammes to 20 metres.' Or: ranging from the tiny Black Hornet (photo) to the Reaper.





Kamikaze drones, unmanned aircraft that survey the area or even fire-breathing drones: the war in Ukraine demonstrates how unmanned systems will play an increasingly greater role on the battlefield. The drones are used for various purposes.

Many are not technologically advanced systems but drones that can be bought ready-made in the shop and then adapted for the desired purpose, explains Major Daan van den Wollenberg in the online magazine *Landmacht*. He works at the Strategy and Plans Department of CLAS command. 'They work

relatively simply, are cheap and highly effective. If we need to protect our territory and that of our allies in a large-scale conflict, we must have the same capacities as our opponent. The army is therefore committed to the large-scale implementation of drones that are available on the market so that soldiers in the field can work easily with them.'

The Action Plan for Production Security for Unmanned Systems (APOS) has set their sights on large numbers. More than 1,000 off-the-shelf drone systems are planned at group level within the army. The small aircraft are foldable and easily fit in the top compartment of the backpacks. Furthermore, the devices weigh no more than a kilo and can fly two kilometres. Hundreds of drones are planned for use at platoon level. These are slightly larger (about three kilos), can cover a distance of five kilometres and are equipped with better cameras.

Taliban

The armed forces were introduced to drones when the Sperwer made its first flight in 1996. The responses were not entirely positive. Wolse:



The army is committed to the large-scale implementation of drones that are available on the market.



Mr. Jos Wolse, head of the Unmanned Aircraft Systems management bureau.

'It worked well in a laboratory but tended to falter somewhat in the field.' That was until the Sperwer was taken to Afghanistan in 2006. 'Eyes in the sky. The commanders loved that!' The Sperwer proved its usefulness even when the onboard camera didn't work. 'The device's humming noise scared off the Taliban. They stayed quiet when they knew they were being watched. They had no idea the camera was broken.'

Wolse predicts that autonomous flight will play a greater role in the future. 'If your opponent disrupts a data link, you do want the collected data to arrive at the ground station eventually. The drone must remember its target.' Wolse believes that we must not become completely dependent on the technology. 'We are spoilt with satnav in our phones and cars. But you must be able to navigate in a desert or above the sea, without clear landmarks. Soldiers must also be adept at traditional manual work by learning to navigate with a map and compass.'

Defence is working on an ecosystem for drones with knowledge institutes such as Delft University of Technology (TU Delft), TNO and NLR. 'Then we won't spend four years on a project, but three months,' Wolse comments. 'Developments move fast. Companies are warmly welcome to get involved. However, we have no need for yet another camera or sensor on board a drone. But there are certainly possibilities if someone devises a system to receive passive radio signals. We can stick a box like that in the Puma.' ●

Key role for drones

The Defence White Paper 2024 devoted a considerable amount of attention to the increasing role of technological innovation in the armed forces. Robots, drones and artificial intelligence (AI) play a key role in that. The white paper emphasises that unmanned systems and AI are essential to deploy defence more effectively and efficiently.

Funds are also being invested to build a Dutch ecosystem for unmanned systems and for short-cyclical innovations to rapidly respond to technological developments. At the same time, the Ministry of Defence is committed to measures to combat opponents' drones. That includes purchasing mobile anti-drone systems and High Energy Laser systems.

Besides drones, AI is playing an increasingly greater role in military operations. Defence sees artificial intelligence as a crucial factor for improving decision-making and making operations safer and faster. In recent years, Defence has gained experience with robotics and autonomous systems, particularly via the army's Robotics & Autonomous Systems unit. The Ministry of Defence will scale up these experiments in the future.

'Cyber threat is just as dangerous as physical threat'

Collaborations arise for various reasons: product development, joint bids for tenders or international ambitions. Even taking part in a trade fair such as NEDS (NIDV Exhibition Defence and Security) can lead to joining forces. For this edition of NEDS, five companies and the Ministry of Defence decided to work together to create an information security plaza on the trade fair floor: the Cyber & Security Plaza.

Text: Eveline Bos

'We will always be able to achieve more together than we can accomplish individually.' That is how Ron Verbossen, Defence & Safety Market Group Manager of Secura, summarises the thinking behind the initiative.

The idea of working together and acting collectively arose after Ron attended a meeting organised by the NIDV. During that meeting, it became clear that there was a lack of structural attention to cybersecurity within the Ministry of Defence. All the while, digital developments are moving rapidly. 'In fact, Defence's vehicles, vessels and aircraft are moving computers. In terms of harmonisation and multinational standardisation for example, there are few working groups or consultations. That contrasts with the civil market where we are already much further. The seed was planted to work together on this. I approached

other companies and there appeared to be a lot of support for collaboration.'

The first initiative is presenting ourselves collectively at NEDS. Besides the Ministry of Defence and Secura, the Cyber & Security Plaza includes the companies Bosch Energy and Building Solutions, Sectra, Signify and Compumatica. These companies' activities partially overlap but are also complementary. This serves the entire chain: ranging from physical security of buildings and corresponding infrastructure to crypto and consultancy services.

Relationship

Ron: 'All the companies already had a working relationship with the Ministry of Defence. We are also aware this is a complex domain. In terms of cybersecurity, you have the electronic side, the physical side and of course people who play a role in information security. No single party is an authority on all these facets. We complement each other, which enables us to tackle the client's challenge in its entirety. The sector has a natural tendency to want to solve issues by itself. We must move away from that and become a kind of trusted circle of partners. This group is open to that.'

That sounds like music to the ears of Ben Slaager, Chief Information Security Officer of COMMIT. 'The thinking behind the "plaza" is exactly what we need,' he confirms. 'Considering the rapid developments, it is no longer realistic for the Ministry of Defence to have every specialism in house. You will need to collaborate intensively with the industry. However, that demands a different relationship to the one we had. We have to shift from a client-supplier relationship to become more like partners.'

'Such a collective at an exhibition increases your visibility more than if you all have individual stands spread around. That is positive as there needs to be more attention to cyber and information security,' Ben emphasises. 'After all, the threat is just as dangerous as the physical threat, yet elusive. And there is constant competition in this area. There is no clear starting point, it's continuous. You therefore no longer have the luxury of choosing when to ensure your security is properly arranged. It is a necessity and from the very beginning.'

Design

With that beginning Ben means that information security must already be included in the design phase of a new weapons system – Security by



Photo: Mediacentrum Defensie



Ministerie van Defensie



Photo: Mediacentrum Defensie

design. That is COMMIT's role in fact, even when drafting the requirements for a new system consideration must be given to what the system – that will be operational several years later – must comply with. 'You need to include the industry and knowledge institutions in that, from the outset of such a process. And then later too for maintenance and upgrades. Information security therefore plays

a major role in a system's entire life cycle, and it must be properly arranged – always. You therefore also need the industry and knowledge institutions through the entire life cycle.'

'That is a responsibility of the industry,' Ron adds. 'We should not necessarily wait until Defence sets certain product requirements. We are also responsi-

Bosch Energy and Building Solutions

'I met Ron Verbossen from Secura at the 2023 NEDS. Seeing as our companies complement each other in terms of services, we saw possibilities to work together. They cover cybersecurity, and we deal with the physical security of buildings. And importantly when it comes to collaboration, it clicked on a personal level!' says Dick Blom from Bosch Energy and Building Solutions, where he is responsible for the DIS business line.

'The great thing about this plaza and the participating companies is that we are sharing and supplementing our expertise. This enables us to offer a broad range of activities and solutions that match customer demand. Collaboration is particularly important in the domain of information security. After all, you cannot create security alone. It is good to see Defence participating. There too, people realise that you need to connect with knowledge institutions and the industry to increase and guarantee security.' This type of initiative is nothing new for Dick. A few years ago, Bosch and seven other companies set up the Meldkamerplein (Control Room Plaza), where Dick, as a representative and

knowledge partner, responds to safety and security issues faced by control rooms and traffic control centres, etc. Besides sharing knowledge and innovation, the companies also join forces when participating at trade fairs.

'I see the joint participation at the NEDS as a first step for information security. It has potential. Together, we look at where the gaps are in the services. We then look for partners. I am sure more partners will join in. As a system integrator Bosch is well suited to this. We are brand independent and have gained vast expertise in the domain of security through the years.'

'We want to share our experience and knowledge to contribute to national security. That is also the case for the companies with us here at the Cyber & Security Plaza. Ultimately, the objective is to become a true partner of our clients, to work together with shared risks and shared win-wins. In short: with an understanding of each other's objectives. Initiatives like this one, acting as a collective force, is a start,' Dick states, 'and I am very enthusiastic about it.'

Signify

Secure, extremely high-speed communication via invisible light (LiFi). That is what Trulifi from Signify – previously Philips Lighting – offers. Light as a physically impenetrable layer for data transmission. Seeing as the data cannot leave the bundle, it is virtually impossible to intercept, hack or jam it. LiFi is a secure alternative to radio and a practical alternative to cables. 'This enables radio use to be postponed for as long as possible and drastically reduces the use of cables,' says Mark Gunther, Trulifi's Segment manager. 'LiFi has numerous applications in defence.'

Secure communication is only one aspect in terms of information security. The organisations at the Cyber & Security Plaza cover various aspects of information security. Because one party is not an authority on everything. When you join forces, you can offer the entire spectrum. The fact that the Ministry of Defence is also participating, and is thereby closely involved, has a positive effect on the development of solutions. 'It's all good and well to conceive something in a lab, but it all comes down to whether it works well in practice. That is why we have worked closely with a number of parties to develop something that is truly relevant to a specific environment. We are working on both static and dynamic (moving) solutions.'

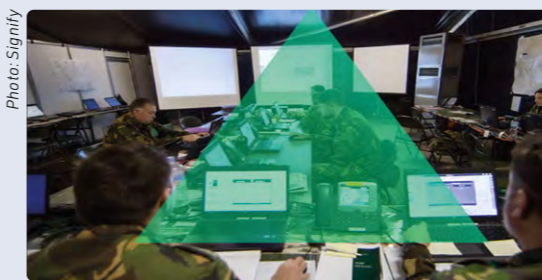


Photo: Signify

'I see this initiative as an ecosystem in the making. Together, we can offer solutions that you can't offer alone. You also learn from each other. We look at where our products or services intersect and how we can better align them. That requires mutual trust because you give each other a glimpse behind the scenes at your company. You make agreements with each other about that. But it starts with the feeling that parties can get along,' Mark emphasises. 'That's actually how it began. We are only just getting started, but I think this has the potential to genuinely contribute to The Netherlands and its international position.'

'The impact of a cyberwar would be massive. Without internet, a large part of our daily lives would come to a grinding halt. Information security is thus not only Defence's responsibility. It also concerns other security services, a secure government. In fact, information security plays a role wherever sensitive data is processed. That includes office environments, public buildings and ultimately at home. There are many positive sides to the high degree of digitisation, but it also creates vulnerability. There should be greater awareness of how vulnerable we are. Who knows, this collective may be able to contribute to that too!'

LiFi is the secure alternative to radio and a practical alternative to cables

ble to ensure a product is secure and stays that way. As Ben just mentioned, the industry could act more like a partner in that as opposed to a client-supplier relationship.

Collective

The first step has been taken. Supported by Defence, these parties are presenting themselves as a collective at NEDS to make this complex and relevant domain visible. What's next? 'We're considering sharing knowledge in organised sessions, but that still needs to be fleshed out. More companies can

join in too. Competition is no grounds to refrain from taking part. We look at the expertise and quality available. Indeed, Defence and the security sector need the very best!'

Ben frankly admits that the Ministry of Defence still needs some convincing when it comes to more intensive collaboration. 'Involving companies from the start is a novel approach for Defence. That trust needs to grow. Internally, however, this initiative to create a plaza together at NEDS was embraced right away. That in itself is a small success.' ●

SMART AND TO THE POINT.

Operationally Proven, Multi-Domain,
Multi-Layered Solutions



See us at
NEDS 2024
Booth C 4.0



RAFAEL

Their mission becomes ours ...



AAR Delivering SOLUTIONS

AIRCRAFT SERVICES

- Component Repair & Overhaul
- Depot Level Training
- Test Stands & Support Equipment
- F-16 Aircraft Maintenance (MRO)
- Repair Management
- Logistics Support Services
- Engineering Services
- Diminishing Resources
- Supply Chain Management
- Hydraulic Oil Purification Systems



F-16 Jet Fuel Starter (JFS)



F-16 Accessory Drive Gearbox (ADG)



DOING IT RIGHT

To better connect the world



Aircraft Component Services – New York
747 Zeckendorf Boulevard, Garden City, New York, USA
+1-516-222-9000

Aircraft Component Services – Amsterdam
Kruisweg 705, 2132 ND Hoofddorp, The Netherlands
+31-20-655-2222

For a full listing of our capabilities:

Visit us at: www.aarcorp.com
or email us at: F-16@aarcorp.com

C-390 MILLENNIUM

ONVERSLAANBARE COMBINATIE

MISSIE-GEREED VOOR DE HONGAARSE LUCHTMACHT

Hongarije is, na Portugal, het tweede NAVO-land geworden dat het C-390 Millennium verwelkomt. Het vliegtuig is het eerste ter wereld dat is uitgerust met een roll-on/roll-off intensive care-eenheid, waardoor het bij uitstek geschikt is voor humanitaire en medische evacuatiemissies. Andere mogelijkheden zijn onder meer zoek- en reddingsacties, vracht- en troepentransport, precisie-vrachtdroppings, parachutistenoperaties en lucht-lucht bijtanken. Een groeiend aantal landen in Europa kiezen voor de C-390 Millennium (waaronder Nederland, Oostenrijk en Tsjechië), aangetrokken door de onverslaanbare combinatie van technologie, snelheid, prestaties en multi-missie-eigenschappen. Deze laatste ingebruikname is een nieuwe mijlpaal voor een ongelooflijk vliegtuig dat al 14.000 vliegreuren heeft gemaakt bij de Braziliaanse en Portugese luchtmacht.

#C390UnbeatableCombination
embraerds.com



CHALLENGE.
CREATE.
OUTPERFORM.

Chantal Vergouw (KPN) wants to create a chain of strong links

'It's time for us to recognise that we are all part of the vital infrastructure'

'Our security is not just the responsibility of our government services. We all share that responsibility,' states Chantal Vergouw, executive board member at KPN. At the opening of the 35th edition of NIDV NEDS, she will explain why we shouldn't wait with intensifying public-private partnerships. We spoke to her before that event on 21 November.

Text and photos: KPN

Responsibility. That is a word we hear reiterated quite a lot during our interview with Vergouw. 'When I say that we all share responsibility for our security, I don't mean that responsibility lies somewhere in the middle, because then no one will take it on. We cannot afford that in these troubled times. Now is the time for us to acknowledge how our modern society works. Plus the fact that we all have a task in that, one that does not stand alone.'

And by that 'modern society', do you mean that everything is digitally connected?

'Digitisation gives us many fantastic benefits, convenience, contact, innovation and a way of life where we can achieve so much more than we could say 20 years ago. Moreover, we have a higher standard of living and that in turn creates new risks that affect society as a whole. People always talk about the vital infrastructure, the essential services that keep a country running. That invariably means the security services, the armed forces, police and things like the supply of energy, our drinking water and healthcare. Those institutions are crucial to our resilience and for society to function. My point is that we are so intrinsically connected in the Netherlands, both online and offline, that you can no longer speak of a demarcated vital infrastructure.'

Do you mean that we are that vital infrastructure together?

'We all form a connected system. If one of the suppliers of the Ministry of Defence is unable to deliver, we have a problem. If the logistics system in the Netherlands is crippled due to a hack, leaving



Chantal Vergouw has been a member of KPN's board of management since 1 June 2023. She spearheads innovation and secure IT solutions to increase cyber resilience. Before taking up her position at KPN, she worked in the banking and insurance sector for 23 years.

supermarket shelves empty during a crisis, then everyone will be in trouble. And vice-versa too of course: if our telecom and IT infrastructure fails, the Netherlands will come to a standstill. If we continue to appreciate one another in that light, we will become a stronger society together in the long run. That means not thinking in isolation and reasoning from a silo mentality, but rather from the realisation that we form a living network together.'

Are we sufficiently aware of our dependence on the digital world?

'I think "dependence" is an ill-chosen word, and rather outdated in fact. You used to be able to think in terms of being "connected" to the internet, but that is obsolete nowadays. You must realise that your digital infrastructure is an integral part of your business operations. I would even go as far as saying, your network is your business operations. That integrated mindset is crucial to your organisation's continuity, to the collaboration with your partners,



'It's our duty to help the country progress'

with your staff and of course for your innovation. And that's why it is important to think about how you deal with that network, with all the components and all your data. As an organisation, you are responsible for the data you have in your possession. Of course for your own continuity. If everything stops working, your organisation will suddenly cease to function. Imagine that happening to you. You would be paralysed. The costs would be massive, as well as the reputational damage. Not having your security adequately arranged not only puts your business continuity in jeopardy, but you also run a massive compliance risk. After all, you also have highly sensitive data about your clients, your chain partners, on your staff, financial data, medical data, etc. You have to keep that all together.'

Everyone wants to be in control, but how do you achieve that?

'It starts by constantly asking yourself where your data is. And what path your data and that of your client's takes. It no longer suffices to say: "Er, well, it's somewhere in the cloud." That's why we help companies and government agencies to think about how to separate various internet traffic flows. What are your crucial applications? Which partners do you trust and want to allow separately into your network, independent from all the other traffic? That means you must actively differentiate between internet traffic you trust and the rest of your internet traffic. That is something you can manage; you can implement separate security measures.'

Does that also change KPN's role?

'The way we fulfil our role is changing. Traditionally, we are the connecting force in the Netherlands. We supply connectivity and technological solutions, but of course we are not the only ones to do that. However, one thing that is changing is that we are acting as a system integrator for an increasing number of companies and government agencies. Organisations often have many different IT suppliers and a range of systems and platforms. Some of those systems are new and state-of-the-art, others are more legacy-type systems. All those elements and all external IT services must work together securely within the digital infrastructure. All those elements, such as data management, cyber resilience, protecting digital identities, etc., demand an integrated approach in the long run. For many organisations it is extremely complex to configure all that themselves, and even more so with the current shortage of IT and security professionals. So, we help with that. And I also consider it our explicit duty to help our country progress in that respect.'

'Your organisation must learn to anticipate uncertainties'

Where does that sense of duty come from?

That focus is historically ingrained; KPN has always been closely connected with the Netherlands. It is our second nature to take responsibility for securing our vital networks and those of the country. Of course, it's also due to the fact we've been active on the very crossroads of the physical and virtual network for many years. It is precisely that com-

'We have more to offer each other than we think'

ination that makes our people understand down to the last detail how each element in the network functions, what the risks are and how you respond to those risks. Based on that awareness, we take care of the crisis systems and the critical data and communication traffic in the Netherlands, ranging from government agencies and semi-government agencies to national defence systems. We are perfectly suited to building, monitoring and safeguarding those systems. And it goes without saying that not all our clients need the highest security level, but I do think that it is in everyone's interest to look at their security in a structured way.'

Aren't we lagging behind when it comes to our security?

'We certainly have some catching up to do in the Netherlands. Things are developing extremely fast. Attacks are becoming increasingly severe and more complex, and the attempts to extract your staff's credentials, for example, are becoming increasingly sophisticated. People must be taught risk awareness, but it doesn't end there. You can't prevent someone from clicking a malicious link. You really have to really consider management and access rights. Essentially, it comes down to the fact that your entire organisation must learn to anticipate uncertainties and security risks, from a zero-trust principle. That entails making your security part of all your business processes, and that you can also demonstrate you have implemented security measures. It's all about ownership.'

Do executives in the Netherlands have sufficient expertise to deal with this?

'I can't really give an unequivocal answer to that because it differs from one person to the next. But I

firmly believe that all executives in the Netherlands, from both public and private companies, must understand how this works. It's not something you simply leave to your CTO or CIO. Everyone involved must fully comprehend where digitisation is taking us and the incredible growth opportunities it offers. But you also have to understand how intrinsically intertwined that development is with multifaceted risks and an ever-increasing attack risk surface. And you shouldn't consider all that digital development as something that happens to you; you must want to be in control of things. Fortunately, there's plenty of expertise in the market to help you with that.'

In other words, you are advocating for a more intensive partnership between the public and private domains?

'I think there is still a lot to be gained in that respect. The collaboration could and, more importantly, should be intensified. And especially when you consider the challenges our country is facing: our sustainability, liveability, competitive position and particularly our security.'

In that respect, we have more to offer each other than we think. Companies and government agencies each have their own role in the chain. It's their responsibility to take on that role.'

What expectations do you have of NIDV NEDS 2024 on 21 November?

'I am really looking forward to good and constructive meetings. We can learn a lot from each other. And that's a necessity. This is not the time to sit back and wait. The world is too troubled for that. We must act right now and join forces. ●'



TRAINING COURSES FOR THE ELECTRONICS MANUFACTURING INDUSTRY					
PB DESIGN	PB FABRICATION	PB ASSEMBLY	PB REPAIR AND REWORK	CABLE AND WIRING TECHNIQUES	SPECIAL TRAINING PROGRAMS
<p>OFFERS TAILOR-MADE IPC / PIEK COURSES AND CERTIFICATIONS ACROSS THE WORLD TO ANYONE WORKING IN THE ELECTRONIC INTERCONNECT INDUSTRY</p>					<p>PIEKTRAINING.COM</p>
<p>QUALITY</p>					



Adverteer in dit magazine. Voor informatie en prijzen:

ER-communications T +31 (0) 627028877 E info@er-communicatie.nl | www.er-communicatie.com

Visit us at NEDS 2024
Ahoy Hall | Booth No. E 2.0
21st November | Rotterdam

750+

airborne missile protection systems already delivered. These are in use in various configurations on different types of platforms by customers worldwide.

>300

targets within 120°. SPEXER2000 boasts unparalleled effectiveness in target detection, ensuring critical battlefield security.

2.0

HENSOLDT MUSS for armoured vehicles is designed to counter threats posed by ATGMs and laser-guided ammunition. Over the past eight years, more than 350 MUSS have been delivered for the first batch of the PUMA IFV.

123

underwater optronic systems have been delivered by HENSOLDT since 2004.

Detect and Protect

As a system integrator, HENSOLDT offers platform-independent, networked solutions. Being a technology leader, the company is also driving forward the development of defence electronics and optronics and is continuously expanding its portfolio based on innovative approaches to data fusion, artificial intelligence and cyber security. We provide innovative sensor solutions to enable armed forces to detect and combat threats in both the analogue and virtual space. Following the acquisition of ESG GmbH, the company employs around 8,000 people. ESG develops, integrates, supports and operates highly complex, security-relevant electronics and IT systems in the fields of defence and security.

HENSOLDT – Innovations for a safer world



Opening doors with the PIB programme

For centuries, the Netherlands has had a well-deserved reputation as a trading country. People braved the dangers of the open sea on massive wooden ships hoping to trade successfully with faraway countries. Nowadays, the world is a lot smaller and trade and collaboration between countries covers many areas. Has international trade become easier? It has in many respects, but that doesn't mean there are no obstacles or new challenges.



Text: Sander Zijlstra
Photos: NIDV

Factors such as legislation, costs and cultural differences can greatly complicate international trade. Add to that, it can be extremely difficult to contact decision-makers and government representatives that most companies want to talk to. It takes a long-term sustained effort to build a relevant network. That in itself is often a barrier to international business for larger organisations. For SMEs, factors such as these make it almost impossible for them to break through in a foreign market.

"It's exactly these sorts of things," says Marcel Knoors, Partnerships programme manager at The Netherlands Enterprise Agency (RVO), that

make the Partners for International Business (PIB) programme so important and effective.

Programme

The Partners for International Business (PIB) is a programme that allows Dutch companies to enter public-private partnerships to realise their international ambitions. The Netherlands Enterprise Agency (RVO) implements this trade facilitation tool on behalf of the Ministry of Foreign Affairs.

Despite the Ministry of Defence's initial reservations about using this initiative for the defence and security sector, the NIDV received approval for the

first PIB with Malaysia and Singapore in 2019. Since then, the NIDV has worked with the RVO and the Dutch embassies in the target countries to organise PIBs with Greece and South Korea. COMMIT and the Commissariat for Military Production (CMP) are also closely involved with these initiatives.

The primary objective of these partnerships between the industry and the Dutch government is to support Dutch companies with their international ambitions. A PIB has an average term of three years and a maximum budget of €350,000 to fund activities for a cluster of businesses and knowledge institutions. These activities include trade missions, a local

PIB liaison and visits to international exhibitions to position the cluster in the chosen country's market. Cluster members support the PIB by investing both their time and a small financial contribution.

Benefit

According to Peter Huis in 't Veld (BDM International and PIB coordinator at NIDV), 'A major benefit of participating in the PIB is the strong position companies derive from the cluster. There is a substantial difference between a single company trying to position itself in a foreign market and a business doing the same as part of a delegation of companies with the support of the Dutch government. The

partnership with the government opens doors that would otherwise remain closed.'

Thanks to the support of the government and the local embassy, companies are more visible, and it is easier to get in contact with decision-makers and government representatives in the PIB country. This allows businesses to present their product and services at the right level and explore opportunities.

There must be a good plan in place before starting a PIB. Marcel Knoors emphasises the considerations made before a PIB can be approved: 'The importance of the defence industry in the PIB country is a significant point of course, but there are also other factors at play. For example, is the cluster mainly focused on the maritime, air or land-based sector or does it cross domains? Which activities must be included in the programme? Is there an existing network? It also has to fit in the budget of course. In other words: a good plan must be in place, with a suitable budget.'

Knoors: 'Based on these considerations, we can jointly identify and implement the right activities to really help the companies develop their business there.'

Results

There's no denying that taking part in exhibitions and discussions with decision-makers is positive and useful, but have there been concrete results? After all, each company has their own reasons for taking part in a PIB, even if it is initially just to explore opportunities. There are also concrete results!

'The only way to sell your product to a foreign navy is through a model like the PIB', says Niels Moerke, Managing director at Hull Vane. Through a regional PIB liaison they found a local agent, for example. 'Hull Vane may not yet have realised sales in Malaysia, but with the agent's help we are a step closer to achieving the growth potential we see there. We have several direct lines as a result of the collaboration with the agent. We expect to see the first sales this year. That would not be the case without the PIB.'

Ronald Koppelman, CEO of The IP Company, underlines the value of the contacts acquired by participating in the PIBs with Greece and Malaysia. The IP Company joined several Greek companies to integrate their software in a software package intended for Greek frigates. 'However,' Mr. Koppelman says, 'Malaysia is our most successful PIB.' During



Launch PIB Malaysia and Singapore



PIB South Korea

a PIB trade trip, we went to a naval base that had two training vessels with an acute problem. The IP Company is currently designing a solution with the aim of installing our software there on a small scale so that people can be trained to use it and that the benefits become so obvious it will be implemented in the entire fleet.'

Ernst Vonk, Director of Vonk BV, understands the importance of presenting products in the foreign market. 'It really doesn't have to be one-way traffic.' Most PIBs are set up with the idea of selling our products and solutions there, but you can also get things in return.' Vonk BV, for example, has found a Korean partner and they are currently working on bringing the products to the Netherlands. Besides this positive development in South Korea, Vonk BV also has good news about the results of the PIB with Malaysia. 'We have had so many interesting discussions that we are currently setting up a local entity there.'

Future

PIB participants are starting to see the results of the PIB efforts. So, what else does the future hold in this area?

After several extensions, the PIB with Malaysia will finish at the end of this year. However, because the activities and efforts are starting to bear fruit, a cluster will continue to exist. The members are discussing how they can carry on with their activities. 'It's not all over once the programme ends of course,' Marcel Knoors says. 'The contacts have been made and several projects are underway, so we hope the heart of the cluster can continue and enable the companies to achieve their international ambitions.'

The NIDV is not standing still either. PIB coordinator Peter Huis in 't Veld is already working on an application for a new PIB. This time focused on Finland and Sweden. 'It's not finalised yet, but there are great opportunities and companies are interested in taking part. I am very positive!' ●

Patria

PATRIA BOOTH C 1.1

Come visit us at NEDS, Rotterdam 21.11.2024



See you at NEDS 2024



Peli™ Single Lid cases
Available in 400+ sizes



vonkbv.com | info@vonkbv.com
+31 (0)88 0330 300 | Piershil



The strength of society

Rising global tensions and a war in Europe. Increased risk of natural disasters. New types of emergencies and disruptions to infrastructure fuelled by climate change, the energy transition and the data revolution. The government is not able to cope with all these threats on its own.

Text: NIPV

That is what the Netherlands Institute for Public Safety (NIPV) stated in an 'exploration into strengthening social resilience and adaptability in times of crisis', published in May of this year.

'If we want to be well prepared to respond to future disasters and crises, we need the full strength of

society. That requires a society that can be resilient and adaptable. The COVID-19 crisis and flows of refugees from Syria and Ukraine has demonstrated how great our self-organising capacity is.

At the same time, critical periods have taught us that we could improve the collaboration among govern-

You should not underestimate the role of the whole of society in times of crisis. At such times, a resilient and adaptable society remains intact despite it all – that is the resilience component. Photo: Mediacentrum Defensie



ment, the business community, social organisations and individual citizens on many points. Citizens and organisations would like to help, hand-in-hand with traditional emergency services. That has become apparent in recent years. Additionally, they don't sit back and wait for the government but take the initiative themselves.

Knowledge

Yet there is still a lack of attention to the structural deployment of these non-traditional partners in the security chain. Their deployment is still in its infancy. What is the cause of that? Standard emergency services often have insufficient knowledge of these new parties' capacity to act. Unknown is unloved.

Furthermore, there is a fear of stepping beyond the existing framework, in part because the responsibilities are not clearly defined. As a result, it remains a challenging search for traditional network partners to expand their network and enter constructive

partnerships with new parties. The cause is partly historical. In contrast to our neighbouring countries, the civil protection mechanism is fragmented in the Netherlands. The consequential lack of visibility means there is insufficient clarity and knowledge about what is expected from the network partner, what a party can provide in which scenarios and how deployment can be coordinated in a broader sense.

Network

You should not underestimate the role of the whole of society in times of crisis. At such times, a resilient and adaptable society remains intact despite it all – that is the resilience component. It is then able to bounce back to the old normal or a desired new situation – that is the capacity for adaptability.

Such a society comprises a network of relevant parties that tackle a crisis together: these range from government to the business community, utility providers, non-governmental organisations and citizens who can jump in as volunteers if the need arises. A well-functioning and competent social network shares knowledge, expertise and information, provides monitoring and image construction, increases public preparedness and awareness through risk communication, maintains strategic supplies and capacities and ensures a coordinated effort and effective recovery. All parties go through a cycle of education, training, practicing, testing, evaluating and learning. Such a network also maintains connections with comparable international networks.

The task is to eradicate the current lack of clarity and unfamiliarity to design such a contemporary form of civil protection in the Netherlands. Network partners can achieve that if they join forces to develop scenarios based on social needs and establish them in social network maps. That would enable the security chain to gain insight into the availability of everyone's capabilities, and we can better coordinate their deployment.

Additionally, we must work on a suitable legislative framework to clarify mutual responsibilities. Furthermore, the resilience and adaptability in society would benefit from targeted risk and crisis communication that is relevant to citizens' life experiences and encourages them to take action. That requires ministries, security regions, water authorities, municipalities and their new security partners to work together on a programme covering five lines: network creation, insight, effectiveness, awareness and frameworks. ●

(advertisement)

PHOTONIS: AN INNOVATIVE DEFENSE COMPANY SERVING THE DUTCH ARMED FORCES

Photonis is a global leader in advanced photo-sensor technology, best known for its cutting-edge Image Intensifier Tubes (IIT) integrated into night vision devices.

Today, Photonis' 4G technology remains the benchmark across European land forces programs, providing superior visibility in challenging conditions and maintaining a critical edge in night operations.

Although the company operates on an international scale, it has deep roots in the Netherlands, particularly through its factory in the North of the country, in Roden. With its two production sites in France and the Netherlands, Photonis offers the highest quality IIT for a wide range of night vision devices that meet specific environments and exacting requirements.

Photonis, pioneer in 16mm IIT for enhanced mobility

Thanks to its innovations, Photonis has increased the night-time mobility of soldiers by strengthen their tactical understanding, agility, targeting and driving skills, even on the darkest nights. While it is important to maintain the best performance of an IIT in all light conditions, it's nearly equally important to make this system as easy and comfortable to use in battlefield conditions allowing soldiers to operate safely.

Photonis night vision tubes, in service in the Dutch Armed Forces

Photonis intensifier tubes are the preferred choice of European Armed Forces and a trusted partner of NATO. Since 2021, Photonis has been supplying 4G 16mm IITs to the Dutch Armed Forces under a successful seven-year contract.

Decreasing the load on a soldier is a constant challenge to enhancing the efficiency and effectiveness of armed forces. Night vision devices based on the 16mm IIT maintain performance levels comparable to those utilizing 18mm IITs but with significantly reduced weight, improving military efficiency.

In fact, the COMMIT (Command Materiel and IT) signed in 2020 a contract with Elbit Systems to supply the XACT 32 NV Micro night vision monocular which features a high performance 16mm 4G image intensifier tube. COMMIT's choice of Photonis image intensifiers demonstrated a continued trust in the capabilities and technologies of Photonis.

Through its collaboration with the Dutch Armed Forces and its global market leadership, Photonis will continue to shape the future of opto-electronics for years to come.

PUSH LIMITS

At Aeronamic, we choose to dedicate ourselves to high-speed rotating components and precision parts. Developing, producing, assembling, testing and servicing them thoroughly, according to all standards.

Innovative as we are, we always invest in tomorrow's productivity. From new production technologies like additive manufacturing to our state-of-the-art F-35 PTMS knowledge and repair center in Woensdrecht. That same commitment to innovation is what inspired us to develop our own software to support our primary MRO process. By staying ahead of the curve Aeronamic is also able to attract the industry's best and brightest new talent. To help us tackle future challenges. So we can continue to push limits.

www.aeronamic.com

AERONAMIC



- PHOTONIS LEADER IN NIGHT VISION
- STATE-OF-THE-ART IMAGE INTENSIFIER TUBE
- PIONEER WITH THE 16MM FORMAT



Civil defence in Sweden: building resilience by involving society as a whole

Interview with Carl-Oskar Bohlin and Johan Berggren

Times are changing. After decades of peace in Europe war is now back on the continent, stimulating European states to reconsider the role of their armed forces. Investments in the armed forces are on the rise and focus is shifting from stability operations towards the original core task of the armed forces: the defence of (allied) territory. In the Dutch defence and security discourse, terms like 'whole of society' and 'resilience' are increasingly used, often accompanied by a reference to the Nordic countries. But what does a 'whole of society' approach mean and why do we need it? And how can we increase resilience in society? To find out, civil-military relations researchers visited Sweden and spoke with Minister of Civil Defence Carl-Oskar Bohlin and his State Secretary Johan Berggren.

Annelies van Vark and Huib Zijderveld*
Source: Militaire Spectator, 2023-11

Civil defence and resilience

The new Swedish government that came into office in the Fall of 2022 decided to strengthen the civilian components of total defence and to appoint a special minister of civil defence at the Ministry of Defence. What is civil defence and why and how is Sweden working to strengthen it? Hosting us at the Ministry of Defence, Carl-Oskar Bohlin is visibly passionate about his work and convinced of its necessity. He explains that 'the essence of civil defence is basically to get the whole of society to line up behind the effort of providing resistance against an antagonist or an aggressor', with the aim of 'securing the existence of the Swedish state'. The concept is in that sense basically the same as the one that was used during the Cold War: to make sure that in case of an armed assault resistance and resilience in all layers of society is high, and that the whole society is committed to hel-

ping the military defence to solve its tasks. Bohlin further explains that 'resilience is about the will and the ability to resist armed aggression'. He points at Ukraine, which since the first invasion in 2014 has started to build up its civil defence and has proven to be successful during the second invasion and the war that is still going on today.

As Bohlin points out, 'They have been able to keep their electricity going while it has been under attack, while it has been a clear Russian aim to break the backbone of Ukrainian society by attacking the civil part of society.' At the same time, 'resilience has kept up the will to resist among the public of Ukraine.'

Security of supply

Johan Berggren adds, explaining that sustainability is important in that context, as 'it's not enough to be able to deal with something complicated or challenging for a few days or weeks, it (the war) goes on for a long time'.

That goes for military defence as well, and an important part of the work being done at the ministry now is about how to achieve security of supply, for



The Swedish Home Guard exercises in Ystad

which cooperation with the private sector is essential. Bohlin explains: 'I would say there is not one task within the military or in civil defence that can be maintained without the help or the participation of private entities.' He is not only talking about building stockpiles, but also about the possibilities to redirect production, which is not only important in times of war, but also during crises other than war, such as disasters and complex emergencies. The COVID-19 pandemic is an example that immediately comes to mind. During that time production was redirected 'almost organically', to produce masks or sanitation equipment for example, but 'it needs to be more institutionalized, so that we have a preparedness for that in advance.'

Sense of urgency

An essential precondition to rebuild civil defence is a sense of urgency in society. Bohlin sees ample evidence in Swedish society for a growing sense of urgency, indicated for example by an increased will to defend Sweden in the general population and by a very large influx of volunteers into the voluntary defence organizations Sweden has. He explains that the government has been actively pushing this sense of urgency, 'since we find ourselves in a very dire security situation, in which we don't know what lies around the corner. We don't know where the endgame in this might take us.' He does not foresee a situation in which the current situation will go away and go back to prior 2014, or 2008. In addition Berggren explains that Sweden's geographical situation is very different from that of the Netherlands or countries further southwest: 'Sweden is where it is, and we have always lived under the shadow of the East.'

What can a country like the Netherlands, where the sense of urgency is at a much lower level, learn from Sweden in this respect? Bohlin is very clear on this issue: 'We need to prepare ourselves for a worse scenario than we are finding ourselves in right now. And that is a concern for every European country I would say.' Berggren continues by saying: 'Geographically, the Netherlands may be far away from the front lines, but in modern days geography matters less.' One can think about cyber sabotage, espionage, or other grey zone threats. Not to forget the port of Rotterdam: 'I believe Rotterdam is the biggest port in Europe and would be a key point of entry for reinforcements into Western Europe', which would make it a target for an aggressor.

Conscription and voluntary defence

As part of the effort to rebuild civil defence, Sweden has decided to reactivate conscription, starting with 4,000 conscripts per year in 2018, and expanding the total number of conscripts to 8,000 in 2025, including both men and women. The whole cohort receives a call-up letter when they are 18 and are obliged to fill out a digital form. Based on their qualifications and motivation, around 20,000 young people are invited for a medical check-up and two days of briefings, after which the final selection takes place.

As the numbers of draftees are (still) relatively low at around 10 per cent of the cohort, the Swedes are selective in their recruitment procedures, only allowing the most capable and motivated to serve, as Johan Berggren explains. After fulfilling their conscription, former conscripts are placed in a

* Annelies van Vark is Senior coordinating adviser at the Transition Team, Defence Staff and PhD candidate at Leiden University. Captain Huib Zijderveld is a PhD candidate at the Netherlands Defence Academy and Free University Amsterdam.



Minister of Civil Defence Carl-Oskar Bohlin (right) and his State Secretary Johan Berggren

reserve unit for 10 years and can be called up to serve in case of a state of high alert.¹

An important ambition for Carl-Oskar Bohlin is to establish civil conscription as a complement to military conscription, starting in the sector of the rescue services, which are a municipal responsibility. He explains: 'The experiences from Ukraine show the enormous amount of stress that the rescue services are under in terms of equipment requirements, personnel and new tasks.' What comes to mind is, for example, clearing unexploded ammunition and recovering people from collapsed buildings.

¹ If the Swedish government judges that Sweden is at war, or that war is imminent, it can declare a 'state of high alert'. During a 'state of high alert' the government's powers increase and there are a set of pre-prepared laws that ensure that Sweden can secure its needs for resources and personnel, amongst other things.

'Willingness to fight for your country (percentages)'

	Denmark	Finland	Netherlands	Norway	Sweden
Yes	74.6	74.8	46.7	87.6	80.5
No	23.3	18.3	40.9	10.4	15.6
Does not know	2.0	6.2	11.8	1.9	3.0
No answer	0.1	0.7	0.6	0.1	0.9

Survey 'Willingness to fight for your country', C. Haerpfer, R. Inglehart, A. Moreno, C. Welzel, K. Kizilova, J. Diez-Medrano, M. Lagos, P. Norris, E. Ponarin, and B. Puranen (Eds.), *World Values Survey: Round Seven - Country-Pooled Datafile*. Madrid, Spain & Vienna, Austria: JD Systems Institute & WWSA Secretariat (2020).

This makes the rescue services the logical starting point for the establishment of civil conscription. An enquiry is currently underway, looking at other sectors where civil conscription would be useful, 'similar to what we had during the Cold War, when we had civil conscription for people working with power lines, and in health care, functions that need extra support during an assault.'

By preparing for the worst (an armed attack on Sweden) the country is also better prepared for disasters and complex emergencies. In addition to government organizations, voluntary defence organizations play an important role. Bohlin explains that voluntary defence organizations get government funding to fulfil certain tasks during a peacetime crisis but also during high alert or an armed assault. Around 350,000 Swedes are members of such a voluntary defence organization and usually they are connected to different municipalities and have arrangements to assist during peacetime crises. As these voluntary defence organizations were never abolished or scaled down, 'they have the institutional memory of Swedish civil defence from before.'

Domestic role of the armed forces

The main purpose of civil defence is to funnel all of society's efforts into one direction: to protect the Swedish state from an armed aggressor. However, in peacetime the armed forces can support civilian authorities as well. An important principle in the Swedish governance model is the responsibility principle, 'which means that the agency or actor that has the responsibility for a task during peacetime, also has that responsibility during crisis or ultimately war, with some exceptions.' Bohlin illustrates this with an example from the rescue services, which are primarily responsible in case of an earthquake or a flood, for example, but can escalate up the chain, if necessary. 'Ultimately, the state can also ask for military assistance to provide resources to help out in a peacetime crisis.' The armed forces can in that sense be seen as the last resort in case of civil crises and can provide assistance when needed.

On the other hand, he explains, 'in the event of an armed assault or attack on Sweden, all of civil society is then committed to support the military defence to carry out its task.'

Lessons learned

What is the main lesson the Netherlands can learn from the Swedish system for civil defence? Referring to the low popular commitment to defend the Netherlands, Bohlin is very clear: 'Getting the

whole of society involved raises awareness about what is the ultimate task that needs to be carried out. Resilience and resistance start with your own personal preparedness and your own will to defend.' A holistic approach involving the whole of society may eventually lead to a higher will to defend as well 'because it comes closer to every citizen. It is not only the people in uniform who are carrying out the total defence effort, it is every individual within society that has to feel engaged when doing that.' ●

Total defence in Sweden

The Swedish model for total defence emerged during the Second World War, when an expert commission concluded that the boundaries between the military and the civil domain had been erased and war had become total. This called for total defence, including both a military and a civil component.¹ The model consisted of four elements, namely military defence, economic defence (including storage and supply of key provisions), psychological defence (including countering disinformation), and civil defence (including shelters, evacuation planning, et cetera). The whole population was in fact involved in preparing for the eventuality of a war. During the Cold War, Sweden had conscription for males and could mobilize up to 850,000 men.

Until the 1980s total defence had only been focussed on a possible external invasion. Starting in the mid-1980s experts began to point at possible threats from within the country itself. However, it was not until the early 2000s that the threat of an invasion was more or less written off, and was replaced by threats such as asymmetrical attacks, major accidents and natural disasters.² These security problems did not necessarily lie in the domain of the armed forces.³ This marked the beginning of a 'strategic timeout' for the traditional total defence model and a downsizing of the Swedish armed forces. The defence budget shrank from approximately 2 per cent of GDP in 1990 to approximately 1 per cent in 2010 and the conscript system was replaced by an all-volunteer force in the 2009 defence bill.⁴ In this period, a new term entered the security discourse: 'societal security'. In the 2010s a new shift took place. With the changing geopolitical situation and the rising Russian threat,

Sweden again began to increase its military capabilities. On 15 December 2020 the Total Defence Bill 2021-2025 was approved by the Riksdag. Total defence is designed to be able to counter an armed attack against Sweden. The starting point is that Sweden should be able to survive during a security crisis in Europe causing disruptions to society as well as during actual war for a period of time, at least three months. Important measures in the bill are the strengthening of both civil and military defence, including a substantial budget and personnel increase, increase of conscription volumes, and the strengthening of cyber defence. In 2022 a new Psychological Defence Agency (MPF) was created, mainly aimed at identifying, analysing, and countering foreign influence operations and disinformation taking place on social media, for example.

The new Swedish government, installed in the Fall of 2022, decided to move both MPF and the Swedish Civil Contingencies Agency (MSB) from the Ministry of the Interior to the Ministry of Defence, under the coordination of the new Minister of Civil Defence, in an effort to strengthen the civilian components of total defence, more specifically, civilian defence and crisis preparedness.⁵ As part of the reinstatement of total defence, the national defence courses that Sweden organized during the Cold War have been reinvigorated as well. These courses are organized at different levels (e.g. middle and senior management) and aim to bring people from different backgrounds (government, private sector, NGOs, et cetera) together to learn about national security. During the Cold War, the courses concerned total defence issues but recently they have been expanded to include crisis management.

¹ S. Larsson, 'Swedish total defence and the emergence of societal security', in S. Larsson and M. Rhinard (Eds.), *Nordic societal security; convergence and divergence* (Routledge, 2021).
² Larsson, 'Swedish total defence and the emergence of societal security'.
³ J. Stiglund, 'Threats, risks, and the (re)turn to territorial security policies in Sweden', in S. Larsson and M. Rhinard (Eds.), *Nordic societal security; convergence and divergence* (Routledge, 2021).
⁴ O. Kronvall and M. Petersson, 'Doctrine and Defence Transformation in Norway and Sweden', *Journal of Strategic Studies* 39 (2016) (2) 280-296.
⁵ U. Kristersson, *Statement of Government Policy*, (2022). See: <https://www.government.se/speeches/2022/10/statement-of-government-policy/>.

(advertisement)

NEDS
NIDV EXHIBITION DEFENCE & SECURITY

Stand H2.0
21 Nov

Secure communication wherever you are

At NEDS 2024, we will showcase our solutions for government and defense forces—products that enable the exchange of classified information across the world. Join us at stand H2.0 to discuss what we can achieve together.



Scan QR code to read more about our solutions

SECTRA

communications.sectra.com • communications@sectra.com

Mission

The Netherlands Industries for Defence and Security (NIDV) links companies, knowledge institutions, and the government within the Netherlands. Since being founded in 1984 by the ministries of Economic Affairs and Climate, Foreign Affairs, Defence, and industry partners, the NIDV ensures the sustainable positioning of the Dutch defence and security sector both at home and abroad. The NIDV acts as information provider, advocate and service provider for the Dutch Defence and security sector. ●

Exhibitions 2025

NIDV participates in a number of international exhibitions each year. The choice of exhibitions is made in close consultation with the Ministry of Defence and the Ministry of Economic Affairs.

During the exhibitions, the NIDV provides the Dutch pavilion for the participants and organises meetings with relevant companies and government officials. For 2025 this includes the following exhibitions:

SecD-Day	Helsinki	January 2025
DEFEA	Athens	May 2025
LIMA	Malaysia	May 2025
MADEX	South-Korea/Busan	June 2025
DALO	Copenhagen	August 2025
DSEI	London (only posters)	September 2025
ADEX	Seoul	October 2025

For more information, please contact Peter Huis in 't Veld. ●



COLOPHON



The Netherlands Industries for Defence & Security (NIDV)
Bezuidenhoutseweg 161
2594 AG Den Haag
(070) 364 48 07
info@nidv.eu
www.nidv.eu
The magazine is published several times a year in Dutch.
One English edition is published for NEDS
Final editing: Riekelt Pasterkamp

Subscriptions:

Employees of NIDV participants and government receive this magazine for free. Requests via: office@nidv.eu.

Advertising sales:

ER Communications 06-27028877
info@er-communication.nl

All rights reserved. Nothing from this publication is allowed to be reproduced, stored in an automated system database or made public in any form or in any way, electronic, mechanical, by photo copies, recordings, or any other way, without prior written permission from the publisher.

NIDV

Hans Huigen, *Director*
Hildegard Hof, *Business Development Manager Maritime*
Edwin Leidelmeijer, *Business Development Manager Land-based*
Donald Trouerbach, *Business Development Manager Air*
Peter Huis in 't Veld, *Business Development Manager International*
Frans Kleyheeg, *Advisor European affairs*
Seema Sahadew Lall, *Manager*
Nicole Rosbergen, *Management assistant*
Lotta de Ligt, *Management assistant*
Eveline Bos, *Communication manager*
Sander Zijlstra, *Communication advisor international*
Paul de Witte, *Advisor Sustainability*

Board NIDV

drs. R.W. Knops, *Chair*
R.F.M. Keulen MBA, *Damen Naval*
ir. G. van der Molen, *Thales Nederland*
ir. W. Riemersma, *CGI*
SBN b.d. M. G. L. H. Tossings, *TNO*
S. Hamminga, *Robin Radar*
ir. R.J. van Baaren, *ADSE Consulting & Engineering*
drs. I. Veerman, *Van Halteren Metaal BV*
ing. A. Hijwegen, *TriOpSys*
ir. A.J. de Jong, *Delft Dynamics B.V.*
E. Scheeren, *GKN Aerospace*
P. van Breugel, *Verebus*



HÉT SECURITY EVENT VAN NEDERLAND

21 januari 2025

📍 NBC Congrescentrum | Nieuwegein

NL
SECURE
[ID] LET'S TALK<<<
ABOUT IT
2025

Meld je nu aan via
kpn.com/nlsecure

