NIDV DEFENCE& SECURITY
THE NETHERLANDS INDUSTRIES FOR DEFENCE & SECURITY

AUGUST 2017

NEWSLETTER

Netherlands selected for distribution and storage of spare parts F-35

The Netherlands will soon be responsible for the distribution and all storage of spare parts for 400 F-35 fighter jets stationed in Europe.

The Dutch industry benefits from contracts for the construction and maintenance of the F-35.

Logistics Center Woensdrecht, based at Air Force Base Woensdrecht, will be responsible for the storage, management and distribution of the spare parts for the coming decades.

This decision will lead to extra orders for approximately 70 Dutch companies. Ron Nulkes, director of the NIDV, gave an interview to *De Telegraaf* about the deal: "This is good for the Dutch defence industry. It also shows the trust that America has in the Netherlands by giving our country such a crucial role in maintaining a major weapons system as the F-35." The Dutch Minister of Defence, Jeanine Hennis-Plasschaert, emphasized that the deal is an illustration of the excellent cooperation between the government and the industry – a statement the Dutch industry strongly agrees with.

Besides the distribution and storage of spare parts, the Dutch industry has already been nominated for the maintenance of various F-35 capacities.

The Netherlands will buy 37 Joint Strike Figthers. Two have been delivered and eigth aircraft will be delivered as of 2019.

Contact person: Peter Huis in 't Veld at p.huisintveld@nidv.eu.

The police of tomorrow is a police which recognises and anticipates on patterns of criminals.

Police enforce, protect and innovate

Erik Akerboom, Chief Constable: "We attract around one hundred digital experts per year."

The police is currently introducing several innovation measures to enforce the digital connection to society and to make their own work safer, easier and more effective. Erik Akerboom claims that the measures result in a better service for the citizens, partners and colleagues.

With the help of 60,000 smartphones and 4,000 tablets, the police are now connected to every police office and its system. And being connected makes it possible to trace license plates or register declarations. The innovation strategy also entails more initiatives including police experiments with bodycams. Additionally, 'breeding sites' have been installed and this is where technology and data are combined, as sensor data and online data can deliver important information to stop improper behaviour and can also serve as proof of crimes. The breeding places come in the form of sensing, clouds, big data, digital-forensic investigations, artificial intelligence, cybercrime and real-time intelligence.

"Criminality occurs more and more on a digital basis. It is necessary that IT and the information supply is adapted to that fact," states Akerboom. Sensor data and online data are both important sources of information for the police. Experts expect an exponential increase in the number of sensors in devices; sensors in transport equipment, televisions, thermostats, as well as sports clothing and wearable items all produce data. A part of the data is suitable in terms of prevention or a proof of crimes.

Continued on next page

However it is still difficult to find a balance between the protection of privacy and the importance of incisive and effective investigation and crime fighting. "The police is not the enemy of privacy; we are rather the guardian of privacy. Of course we need to violate the privacy of a suspect, but only under provision and it must be verifiable. That's part of our work. Finding the balance is a political question. But I think we need to be capable of suggesting risks where needed. Consequently our professional view is a solid addition to the topic," according to Akerboom. He observes that there are several government organisations that interfere in the discussion around that topic: "The successful projects are the ones in which cooperation takes place. Information needs to be exchanged, we need to cooperate and act as one government."

This leads to Akerboom's ambition to expand the approach of cybercrime: "Our role in the digital world is different to that in the physical world. We cooperate with companies that are specialised in the fight against computer viruses or those that are capable of keeping our infrastructure safe. We attract around one hundred digital experts every year and we would like to duplicate that number."

"The police is enthusiastic about mobile work and we would like to proceed with those developments. But the developments bring new challenges and the police work is significantly affected by them." Akerboom tells that during his career the behaviour with security and data has changed. While police work mainly included research and reconstruction tasks, predictive profiling and predictive policing now play a more important role. "The police of tomorrow is a police which recognises and anticipates on patterns of criminals," says Akerboom: "The police is an information factory. Monitoring its own data is a necessity. Our IT vision is built on the combination of information and making data accessible, analysable and useable. In the end, it all comes down to continuous renewal with the aim to maintain the integrity and security in our country."

Contact person: Rob van Dort at r.vandort@nidv.eu.

European Defence Fund proposals now in stakeholder coordination phase

On 7 June 2017 the European Commission launched their proposals for the European Defence Fund (EDF), together with a draft Regulation for a European Defence Industry Development Programme for 2019-2020. Formal coordination with EU member states began in July and will continue in September with a view to reach an agreement by November 2017.

The EDF consists of three elements to be funded from the EC Multiannual Financial Framework (MFF) 2017-2021, namely a European Defence Research Programme (EDRP, 500 MEuro/year), a European Defence Industry Programme (EDIDP, 1 BEuro/year), and a governance structure.

The European defence industries coming together in the AeroSpace and Defence Industries Association of Europe (ASD), where the NIDV is an active member, are preparing their views on all elements of the EDF. For the Netherlands it is of particular importance that the EDF provides for a level playing field, where its small- and medium-sized innovative and competitive industries and knowledge institutions will be able to participate in the European field, so called cross-border participation. Another element

Continued on next page

already communicated by ASD to the European Commission is the notion that Defence Research normally receives 100% funding, due to the specificities of the defence market. There must be a clear deviation from the rules now in force under the Preparatory Action for Defence Research. Also, a clear definition is needed of eligible entities (companies, institutions). The preserve and autonomous use of intellectual property rights must be at the heart of the definition, rather than financial conditions. On the positive side, it has been noted that the EC does not claim any role in the export of products.

The substance of both the EDRP and EDIDP will of course be of paramount importance. Ultimately, European military forces should be equipped with the right capabilities. Therefore it is essential that EU member states agree on those EU level capabilities to be supported from the EDF. In mid-July France and Germany communicated their initial thoughts on priorities. They include MALE RPAS, Helicopters, Ground Combat Systems and Maritime Patrol Aircrafts. The idea that transpires from this list is that the EDF should focus on the support of a small number of major military capabilities, rather than its fragmentation over a large number of smaller capabilities. This approach may create opportunities for the Dutch defence industry.

The NIDV will continue to promote the interests of its members with all stakeholders, both nationally (government, parliament) and internationally (EC, European Parliament).

Contact person: John Jansen at j.jansen@nidv.eu.

Police fight cybercriminals

The police continue to concentrate their fight against cybercriminals. By paralysing malicious websites, blocking bank accounts, performing name registration and hacking malware, cybercrime operations are made even harder.

Preventing cybercrime goes hand in hand with tracking down the criminals. It is very easy to operate as a cybercriminal, and tracing the individuals is often very difficult and time-consuming.

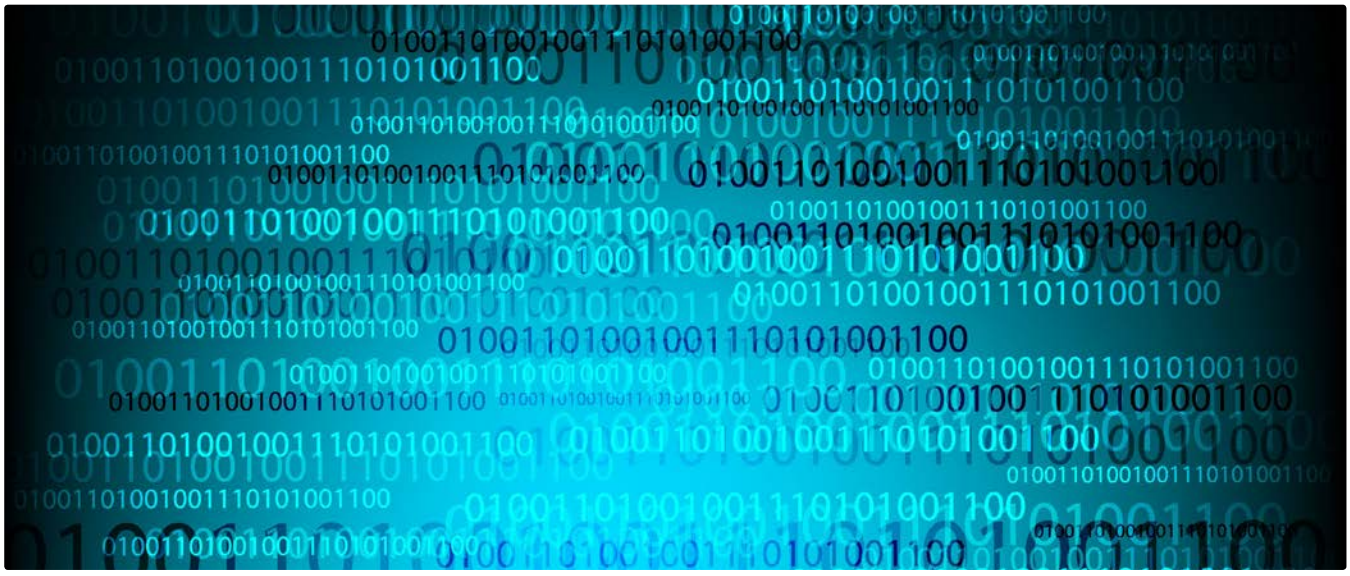
During the past few years, the police have been working hard to disrupt the activities of cybercriminals. Fighting this kind of crime has become a standard activity for the cybercrime teams and police experts, who now form part of every police unit. "Only looking for the criminal individual is not enough," states Theo van der Plas, Programme Director Digitalisation and Cybercrime at the Police. "Research is very time-consuming and there is a high chance that it is impossible to find the perpetrator, as they could operate from a call centre in India or Nigeria for example. In the meantime, the number of victims keeps rising."

Ransomware

This was exactly the case when ransomware was spread. Ransomware is software which blocks a computer until a certain amount of money is paid. The Dutch police cooperated with others including Europol and McAfee to ensure that key codes would be available to unlock a computer. Thanks to this, €8 million in ransom money was not paid out. Around 100 parties are currently cooperating in this project, which was initiated in the Netherlands. The key codes are used in dozens of countries.

It is also possible to block bank accounts which are known to be used by cybercriminals. Transferring money via for example iDEAL is made impossible. Banks and *Marktplaats* cooperate with the police on this project.

Continued on next page



During the past few years, the police have been working hard to disrupt the activities of cybercriminals.

Disrupting the activities however does not replace the search for the criminals. There were 360 investigations in 2016 concerning internet fraud, when goods are bought but never received. These investigations led to 500 suspects, including those whose principle income was earned by internet fraud. There are several differences between the suspects, and the investigation does not yet give a clear picture. Akerboom: "Sometimes we see that 16- to 17-year old are responsible, while there are also 'older' criminals who find new business on the internet. They know that there isn't a high chance of being caught and that's very beneficial to them."

It is very easy to get started with malware, for example, which makes it possible for criminals to steal bank accounts. Akerboom continues: "The software can just be downloaded. On the dark web, the part of the internet which is shielded for search engines, there is even a helpdesk which helps malicious people with their software problems. For a fee it is possible to anonymously receive online advice from the helpdesk 24/7. Some knowledge about computers is already enough to get started."

Contact person: Rob van Dort at r.vandort@nidv.eu.

Defence Attachés-Days 30 and 31 October

The NIDV participants will have the opportunity to meet with the Dutch Defence Attachés on 30 and 31 October.

The Defence Attachés are the Dutch representation of the Ministry of Defence abroad. In 2016, around 20 companies and 15 Defence Attachés took the opportunity to meet and share information about the developments and trends in various countries. Around 60 meetings were held under the coordination of the NIDV.

The invitations for the Defence Attachés Days will shortly be sent to all NIDV participants.

Contact person: Anne Brockherde at a.brockherde@nidv.eu.

Announcement: NIDV Masterclass Naval

The NIDV Masterclass Naval will take place on 14, 15 and 21 until 23 November 2017.

During the Masterclass, the participant will learn everything about Defence with a focus on the Royal Navy in particular. The aim is to get in touch with officers on an operational and tactical level but also with staff in workplaces at which maintenance and planning is being carried out. The participants can check the offered information against their own knowledge, experiences and work.

The challenging and interactive programme contains a diverse morning, afternoon and evening schedule. The participants will visit a major part of the naval locations in the Netherlands. A complete picture of the organisation and the tasks will be the result. Networking and discussions will be held with top officials from the Royal Netherlands Navy on the most ongoing and future material projects, major replacement programs and innovation within this military service.

The Masterclass Naval 2016 was very succesful and was graded highly by the participants with a score of 8 out of 10.

The Masterclass is coordinated by Chris Parthesius. You can register via the NIDV website or with the coordinator. The deadline for the registration is 18 October 2017.

Contact person: Maarten Lutje Schipholt at m.lutjeschipholt@nidv.eu or Chris Parthesius at chrisparthesius@hotmail.com.

New NIDV-participants

The NIDV has four new participants since July 2017. The new participants are Festo, Metasensing, LR Systems and SAS Institute.

Festo is a leading world-wide supplier of automation technology and the performance leader in industrial training and education programs. Their aim: maximised productivity and competitiveness for their customers. Festo stands for innovation and technology in 176 countries throughout the world **(https://www.festo.com/cms/nl_nl/index.htm)**.

Continued on next page

MetaSensing is an innovative Dutch remote sensing company which was founded in 2008 by Italian scientist and engineer Adriano Meta with the aim of commercializing the new compact, high resolution radar mapping technology. Today they are one of the unique companies in the world which offer cost effective airborne and ground-based radar sensors and services both for commercial and scientific applications. Combination of innovative technology and advanced processing techniques has made MetaSensing a fast growing, global company with projects in Europe and beyond **(https://www.metasensing-group.com)**.

The origin of LR System dates back to 2008, when the Stratagem Group team led a cluster of 30 companies and institutions to study and develop new technology for Anti Corrosion & Surface Treatment. The project was partly funded by the Dutch government and the Provinces of Noord Brabant en Zeeland. In December 2014, LR Systems came into existence to complete the development of the Laser Coating Removal robot and subsequently prepare for its global launch. In parallel to the LCR, in 2015 a robotic paint solution was also initiated and named the Automatic Paint Robot (APR), which is currently still under development. Both LCR & APR will be the largest production robots in the world today, able to handle aircraft such as the A380, B787 and C-17. The company looks to the future to leverage on its robotic heritage into various sectors and applications **(http://www.lcrsystem.com)**.

SAS once stood for "statistical analysis system," and began at North Carolina State University as a project to analyze agricultural research. SAS Institute is the leader in analytics. Through innovative analytics, business intelligence and data management software and services, SAS helps customers at more than 83,000 sites make better decisions faster. Since 1976, SAS has been giving customers around the world THE POWER TO KNOW® **(https://www.sas.com)**.

Agenda NIDV 2017

31 August	Expertgroup Export Licenses	Veenendaal
31 August	Johan de Witt Conference	Rotterdam
21 September	Defence Project Day	Amersfoort
30/31 Oktober	Defence Attachés-Days	The Hague
13-22 November	Purple Nectar 2017	Amersfoort
14, 15 and 21-23 November	Masterclass Royal Navy	Various
29 November	B2B-meeting	Rotterdam
30 November	NIDV Symposium	Rotterdam
November	Dutch Industry Day	Washington

Foundation Netherlands Industry for Defence and Security

Prinsessegracht 19
2514 AP The Hague

T: +31 (0)70 364 48 07
F: +31 (0)70 365 69 33

info@nidv.eu
www.nidv.eu/en