

Cyber Commanders Forum

Lieutenant Colonel Michael Backhaus

Communication Branch, German Cyber and Information Domain Service Headquarters

Cyber Commanders from more than 25 nations followed the call of Lieutenant General Ludwig Leinhos, Chief of the Cyber and Information Domain Service, to attend the Cyber Commanders Forum (CCF) meeting held on October 9, 2018 in Bonn, Germany.

The issue of resilience – i.e. the resilience of critical infrastructure to threats from the cyber and information domain – was in the focus of this year’s CCF and of the International Cyber Operations Symposium (ICOS), which took place the other day. Against the backdrop of discussions about the vulnerability of networks and systems to attacks and manipulations worldwide, this issue is highly topical. Risks from cyberspace have been identified by many states and companies as the most significant threat of the coming years and decades.

Close international cooperation at all levels is indispensable therefore, because the cyber and information domain does not recognise national borders. As Lieutenant General Leinhos emphasised in his opening speech, “We have set ourselves the target of using the CCF and 2018 ICOS events to ensure and promote dialogue and knowledge exchange among the participants. We also want to strengthen cyber cooperation between our partner nations as well as between business, research, politics and the military.” Subsequently, Finland, Spain and Estonia informed the other participating nations about the latest developments in the creation of cyber forces in their countries. The CCF attendees were unanimous in saying that only by working together and networking could improvement of resilience be promoted – a decisive prerequisite for the future of modern societies.



(Photo: PIZ CIR/Martina Pump)

In the ICOS keynote speeches, Lieutenant General Vincent R. Stewart, Deputy Commander US Cyber Command, stressed the importance of cyber security in an ever chaotic and unstable world and underpinned the importance of international cooperation in this field, “Never before has cyber security been as important as it is today and international cooperation is essential for our success in cyberspace.”

Bosco Novak, member of the board of Rohde & Schwarz, addressed the contribution industry can make in the field of resilience against cyber threats. His underlying postulate is that only the cooperation of state actors with equally transparent and reliable partners in industry will enable acting stakeholders to respond, commensurate with the challenges faced, to the question

of “We know that there will be incidents, but how quickly can we react and restore the security of our systems?”

The meaning of information as the most important asset of the 21st century was explained by a representative of science, Professor Dr. Dr. Michael Lauster, Director of the Fraunhofer Institute for Technological Trend Analysis. In a field of tension between “truth and alternative facts” the validity of information is of crucial importance for the quality of strategic decisions, according to Professor Lauster. He presented approaches that are suited to make strategic decisions more resistant to the influence of, for example, fake news.

For the Federal Ministry of the Interior, Building and Community, Andreas Könen, the head of the ministry’s Directorate-Ge-

neral Cyber and Information Security (CI), finally outlined the whole-of-government challenge of coping with information security risks in Germany. He also explained the part of the institutions involved, including the Bundeswehr. “The challenge for our country will be to develop from a purely defensive posture against cyber attacks to a proactive strategy of countermeasures in such a way that they fit into the legal framework of our country on the one hand, but also respond to the growing challenge of handling this increasing threat on the other,” Könen said.

In five breakout sessions, the participants focused on topics such as Legal Aspects of

Cyber Activities, Development of Weapon Systems, Analysis of the Information Environment, Artificial Intelligence for (Smart) Military Applications and, finally, Resilient IT Systems.

“This all has been very worthwhile and I especially appreciate the opportunity to look at the bigger picture of the subject,” as one of the participants summed up the session on the Legal Aspects of Cyber Activities. Another attendee summarised her impressions of the panel discussion of five experts as follows: “The dilemma resulting from the various international legal positions becomes apparent, but above all the need to define a common position as a ba-

sis for further action at the international level.”

“Germany will continue to chair the Cyber Commanders Forum until May 2019. I look forward to seeing all of you again in Tallinn, where this chairmanship will also be passed on to the next nation,” Lieutenant General Leinhos said at the end of the event. “To the United States of America,” he told the participants of the symposium, adding that he was particularly happy about it personally because of our close ties with the fellow soldiers of the United States. “This is also an expression of a firm transatlantic partnership in difficult times.”

Start of Trident Juncture 2018

(df) Today the biggest NATO exercise after the end of Cold Wald – Trident Juncture – started in Norway. This exercise will involve the participation of around 65 ships, 250 aircraft, 10,000 vehicles and 50,000 personnel. Every single NATO nation plus Finland and Sweden has sent troops.

The aim of this exercise is to make sure that 29 allies can work together in the air, sea, land and cyber domain. NATO pointed out the importance to test joint cooperation in a real environment and even in a challenging climate, therefore NATO has selected Norway for Trident Juncture.

“In recent years, Europe’s security environment has significantly deteriorated



(Photo: NATO)

and NATO has responded with the biggest adaptation of our collective defence since the end of the Cold War. Trident Juncture demonstrates that adaptation,” said NATO Secretary General Jens Stoltenberg prior to the exercise.

Stoltenberg continued: “The participants will split into ‘South forces’ and

‘North forces’. They will take turns playing the role of the fictitious aggressor and the NATO defending forces. The exercise will test our readiness to restore the sovereignty of an ally – in this case, Norway – after an act of armed aggression. It will exercise our ability to reinforce an allied country with troops and equipment from North America and from across Europe. It will test and certify the NATO Response Force for 2019. So Trident Juncture sends a clear message to our nations and to any potential adversary. NATO does not seek confrontation but we stand ready to defend all allies against any threat.”

www.nato.int

Stoltenberg on the INF Treaty

(df) Ahead of the Trident Juncture exercise NATO Secretary General Jens Stoltenberg also made a statement on the INF Treaty. “The INF Treaty is a landmark treaty but the problem is that no treaty can be effective, can work, if it is only respected by one part and therefore NATO allies have expressed concerns about the Russian behaviour, about the development of a new Russian missile and they have expressed, all of us have, that the most plausible explanation is that Russia is in violation of the Treaty

because they have now accepted that they are developing a new missile SSC8. We have had ongoing consultations on this for a long time. This was actually an issue that was raised by the Obama administration. It was an issue that we addressed also at our summit in July where heads of state and government expressed a very strong position on the INF issue and expressed their concerns about the Russian behaviour and at the Defence Ministerial Meeting in October this was one of the main issues discussed in the meeting but also publicly. At a

press conference I expressed my concerns and addressed the fact that Russia is developing a new missile but also Secretary Mattis declared and stated clearly that this cannot go on, this is untenable, that Russia is developing the new missile,” Stoltenberg said. “We don’t want a new Cold War, we don’t want a new arms race and therefore we strongly believe that it is important to address the concerns we have expressed for a long time regarding the new Russian missile.”

www.nato.int

Technology

Lynx Presented As Possible Successor To Bradley

(gwh) One of the U.S. Army's major armament programmes in the near future will be the replacement of the outdated Bradley infantry fighting vehicle, which was introduced in the 1980s with almost 7,000 units in a dozen variants. At AUSA's annual meeting, Rheinmetall, together with its partner Raytheon, presented the Lynx KF41 combat vehicle to the U.S. Army and the trade show visitors as a possible successor.

In the partnership, Rheinmetall is responsible for the vehicle's technical components, including hull, chassis, propulsion system, crew cabin and turret, while Raytheon contributes sensors, weapons, the Quick Kill active protection system and the Coyote unmanned aerial vehicle (UAS) system, which it integrates. Production will take place in the USA.

The fully developed Lynx is based on proven technology in a modular configuration that enables the cost-effective implementation of a wide range of military requirements. A free payload of 18 metric tons is available for this purpose. Rheinmetall has selected an 850 kW Liebherr die-

sel engine in conjunction with a Renk transmission for the propulsion system. The weapon carrier is the Lance 2.0 turret with the MK30-2 ABM machine gun, which carries mission pods on the outside from which rockets or smoke ammunition or UAS or electronic countermeasures can be deployed. The Lynx can transport up to nine fully equipped soldiers inside.

Raytheon's UAS Coyote is capable of swarming and can independently engage targets (e.g. UAV) with its own sensors and armament. Raytheon wants to use the TOW for anti-tank defence with a service life – after the latest upgrades – beyond 2050. For protection, the Lynx will be equipped with the Quick Kill 2.0 active protection system, which has been successfully demonstrated several times. Last but not least, the latest generation of thermal imaging devices is to be integrated.

The U.S. Army is running the programme under the name Next Generation Combat Vehicle-Optionally Manned Fighting Vehi-



(Photo: Rheinmetall)

cle (NGCV-OMFV). The Request for Proposal (RFP) is due to be issued this month, with a deadline for submission of the offer in May 2019. It is expected that two suppliers will be commissioned to build 14 prototypes in a development and production phase at the beginning of 2020. The first production order could be placed in 2023 with the aim of introducing the vehicle from 2026.

Rheinmetall is also offering the Lynx in Australia, where it might also be available from 2026 as a possible successor to the M113.

www.rheinmetall-defence.com

www.raytheon.com

Portable Drone Detector And Jammer

(df) MyDefence co-hosted the event Electric Storm to demonstrate the capability of the latest MyDefence Counter UAS products for dismounted soldiers. The event featured a live demonstration of the detection and jamming capabilities of the Wingman 103 drone detector and the Pitbull Counter UAS jammer.

This event follows last month's announcement of DeDrone, that they were able to detect drone swarms. Now MyDefence announced a drone swarm jamming capability, which was demonstrated at Electric Storm. During the event, five drone operators attempted to execute a coordinated drone attack. The coordinated attack was effectively neutralised using MyDefence Pitbull Counter UAS jammer, and all drone operators lost control of their drones.



The device is wearable and weighs only 775 grams. Used in conjunction with the Wingman drone detector, the Pitbull can

automatically jam drone signals when a drone is detected. This reduces the cognitive load of the operator, allowing the soldier to focus on the mission without worrying about enemy drones.

"Drone swarms are a concern in the military domain and it has been a priority for us to provide an effective solution to combat multiple drones for both dismounted soldiers and in fixed installations," says Christian Steinø, CEO of MyDefence. "With the Wingman and Pitbull setup, we have demonstrated just that, and the system will be able to defeat countless drones simultaneously."

www.mydefence.dk

Mission Master Wins ELROB's MULE Competition

(df) Rheinmetall's Mission Master vehicle has won the parcour in ELROB's MULE (Multifunction Utility Logistics and Equipment) category. MULEs are autonomous transport vehicles capable of carrying heavy loads and equipment. The contenders had to cover a 1,400 m-long track within 30 minutes. The Mission Master was not only the fastest vehicle, but also the most reliable, or unimpressed by disruption, during the tests.

The cargo version of the Mission Master was exhibited for the first time at Eurosatory 2018. Rheinmetall developed this variant to reduce the combat load carried by troops in the field, contributing to faster movement and greater operational efficiency.

According to the company Rheinmetall's new robotic vehicle can operate in hazardous, difficult-to-reach terrain, in turn contributing to the survivability and protection of troops deployed in harm's way. The Mission Master can also be networked with



(Photo: Rheinmetall)

advanced soldier systems such as Future Soldier – Expanded System, Gladius 2.0 or Argus.

www.rheinmetall-defence.com

155mm Guided Ammunition For U.S. Army

(gwh) NSPA is procuring the BONUS 155 mm guided ammunition manufactured by BAE Systems Bofors and Nexter for the U.S. Army. The ammunition is intended primarily for use against armoured targets, like tanks, and can be



used by all 155 mm artillery systems. The BONUS projectile carries two submunitions into the target area, up to a range of 35 km, which can independently find and engage targets in an area of 32,000 m²

using a multi-band infrared detector. Once a target has been located, the warhead is fired at the optimum height and forms an Ex-

plosively Formed Penetrator (EFP) with an initial speed of 2,000 m/s, which penetrates 100 mm to 140 mm armour-plated steel.

The ammunition is to be delivered by 2020. In addition to the USA, Finland, France, Norway and Sweden use BONUS.

www.nspa.nato.int

www.baesystems.se

www.nexter-group.fr

Mercedes-Benz LAPV For Montenegro

(gwh) The German Government has handed over six LAPV 6.1 (Light Armoured Patrol Vehicle) – called Enok in the Bundeswehr – worth €2.2 million to the Republic of Montenegro. The vehicles produced by Mercedes-Benz in cooperation with ACS with a gross vehicle weight of 6.1 tons will be powered by a 135 kW diesel engine. A free payload of at least one tonne is avail-



(Photo: Daimler)

able for mission equipment. With its outstanding bad-road characteristics, the LAPV is suitable for use under the most difficult

conditions. The light ballistic protection covers fire with infantry ammunition and against threats from anti-personnel mines or IEDs. A payload of one tonne might be added.

Montenegro became a member of NATO in June 2017 and is a candidate for accession to the European Union.

www.mod.gov.me

www.daimler.com

www.acs-armoured-cars.com

Light Protection Helmet F70 Presented At AUSA

(gwh) At the AUSA annual meeting, 3M presented the highly-protected F70 safety helmet in a version of particularly low weight, which resembles the helmets of special forces.

The helmet – optionally with low and medium height (high- and mid-cut) – with a weight of 1.0 or 1.1 kg ranges between the

Ultra-Light Weight Ballistic Bump Helmet and the heavier Combat II Ballistic Helmet, but offers a more favourable ratio of weight and protection.

The helmet has a dovetail splint to accommodate common accessories such as lower jaw protection, visors, ballistic ear protection and counterweights. 3 M



Peltor headphones and hearing protection solutions are compatible with the helmet.

According to 3M, the F70 helmet is suitable for wind-up line jumps and military free-fall jumps based on results of the Air Force parachute test programme.

www.3m.com

New Czech Jet Aircraft

(df) On October 12, 2018 the first L-39NG pre-series aircraft rolled out from the hangar at AERO Vodochody AEROSPACE, the leading Czech aerospace company. This significant milestone has been achieved in line with the L-39NG project schedule and Aero is now going to prepare the aircraft for its maiden flight planned before the end of this year, the company announced.

The L-39NG is a cost effective jet trainer and light attack aircraft. The L-39NG is a single-engine two-seater with staggered seating and an advanced cockpit design that includes full glass cockpit, a sophisticated on board virtual training system and a helmet mounted display. The L-39NG is a key component of AERO's training concept that includes state-of-the-art ground-based training devices, new learning methods and environment and extensive use of virtual reality and artificial intelligence



(Photo: AERO Vodochody AEROSPACE)

technologies. In anticipation of many decades of service the L-39NG has been designed as a maintenance-friendly aircraft, the company declared.

The development of the L-39NG has accelerated in the last two years in order to be able to deliver the first aircraft in 2020. In 2017, the initial pre-serial production and the industrialisation phase started including agreements with all key suppliers and partners of the project – both international and Czech companies (about 40 Czech suppliers). The certification of the new avionics and engine installation was already

completed at the end of 2017, while the certification of the L-39NG will be fully achieved before the end of 2019.

“Aeronautics has always been a strong tradition in the Czech Republic,” said Czech Prime Minister Andrej Babiš at the event. “The L-39NG project is demonstrating that industrial capabilities are still present in the Czech Republic. It is important that the Government supports this project, which will contribute to Czech export by high technological value. It strengthens the competitiveness of the Czech industry.”

www.aero.cz

Teaming Of Manned And Unmanned Aircraft

(gwh) The ability to control unmanned systems from a manned aircraft can significantly enhance the effectiveness of airborne operations.

In a demonstration over the Baltic Sea to military experts with five Airbus-built Do-DT25 target drones piloted by a mission group commander in a manned command aircraft (C2), the company demonstrated the performance of a manned unmanned team (MUT).



(Photo: Airbus)

During the flights, elements such as connectivity, human-machine interface and the concept of team building intelligence through mission group management were validated. For the aspect of teaming in-

telligence, several capabilities and basic technologies with sufficient maturity were used – from team/swarm algorithms and new sensors to mission management systems for command support by the crew of the manned aircraft.

MUT is expected to increase the mission efficiency of future air systems in many ways. The experience gained during the MUT test flight campaigns will feed Airbus into the development of the Future Combat Air System (FCAS).

www.airbus.com

Delivery To The Royal Thai Air Force

(df) Airbus Helicopters announced that the Royal Thai Air Force (RTAF) has taken delivery of its seventh and eighth H225M (previously known as EC725) multirole utility helicopters. Since 2012, the RTAF has placed orders for a total of 12 H225Ms under its fleet modernisation programme. Based on a contract signed in 2016, these



(Photo: Anthony Pecchi)

new additions will join the air force's existing fleet of six H225Ms for combat search and rescue, search and rescue flights and troop transport missions.

“The 11-ton-category twin-turbine H225M is relied upon as a force multiplier by many air forces worldwide thanks to its outstanding endurance and fast cruise speed,” Airbus Helicopters stated. “Close to 90 units are currently in service in six countries across the globe, surpassing the 100,000 flight hour milestone.”

www.airbushelicopters.com

Hypersonic Mode For Naval Radars

(df) Saab has introduced the Hypersonic Detection Mode, a capability for detecting



(Graphic: Saab)

and tracking targets travelling at hypersonic speeds, to its Giraffe radars. This radar has been especially designed to counter the evolving threat of low flying missiles travelling at greater speeds. With the emergence of threats in the high supersonic and even hypersonic speed ranges, this threat is getting even worse. Saab is therefore now offering a solution by introducing a Hypersonic Detection Mode (HDM).

“The hypersonic threat is credible and increasing,” says Anders Carp, head of Saab’s

business area Surveillance. “Navies around the world are asking for a capability to retain their dominant battlespace awareness and to give them crucial time to act. We are able to meet these requirements by using our existing technology, adapting it for the hypersonic challenge.”

The HDM is optimised for the Sea Giraffe 4A Fixed Face, which is a fixed array configuration that belongs to Saab’s multi-functional family of S-band AESA radar systems.

www.saab.com

MBDA Unveils Its New Maritime Missile

(df) At Euronaval MBDA unveiled its new naval missile that is based on the 5th generation MMP ground combat missile. This presentation followed the operational evaluation campaign carried out at the end of this summer by the French armed forces in Djibouti.

In that test the reliability and operational performance of the MMP system in a hot environment, both from the ground and also from a rigid hulled inflatable boat (RHIB) moving at high speed, was confirmed, the company stated. A total of nine MMP missiles were fired with all reaching their target. Two of these shots were fired

by the maritime force of marines and commandos from a ECUME RHIB. A first firing from sea to land and the second from sea to sea demonstrated the ease of use of the MMP.

“Today’s launch of a family of naval systems based on the MMP missile is aligned with the trajectory we initiated with the French Army at the launch of the MMP programme in 2011,” said Antoine Bouvier, CEO of MBDA. “By deciding at that time to introduce the most modern technologies of guidance and propulsion together with a multi-effect warhead, we laid the foundations of a family of weapons capable of meeting the most demanding constraints the armed forces may encounter in the



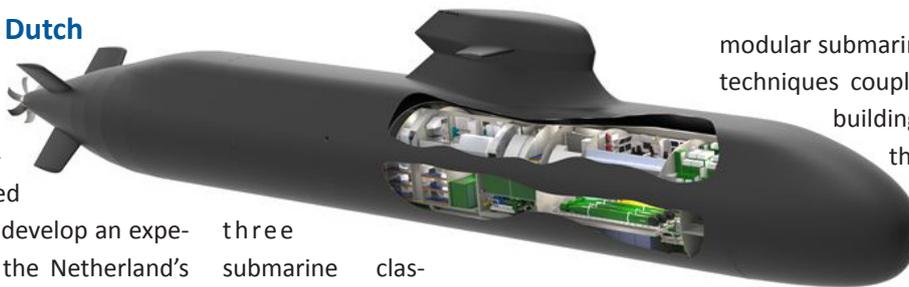
(Graphic: MBDA)

field, in terms of tactical effects, in terms of mobility, as well as in environmental terms. The MMP family sees today the advent of naval versions. I have no doubt that the MMP will give birth to other more powerful versions in the near future.”

www.mbda-systems.com

Cooperation For The Dutch Submarine

(df) Saab and Dutch shipbuilder Damen Shipyards Group announced their new partnership to develop an expeditionary submarine for the Netherlands’ WALRUS Replacement Programme (WRES) at Euronaval international naval exhibition. The Expeditionary Submarine will build on the capabilities of the Swedish A26 and the experience of the Swedish designed COLINS class submarine in service with the Australian Navy, the companies stated. “As a result the Expeditionary Submarine will be equipped with state-of-the-art technology whilst benefiting from de-risking on



three submarine classes,” Saab announced. “Saab and Damen are thereby creating one of the most modern Air Independent Propulsion (AIP) submarines in the world, which, if selected, will be done in consultation with the customer using a ‘design to cost’ approach.”

“Replacing the WALRUS class submarines requires a unique approach,” said Gunnar Wieslander, Senior Vice President, head of business area Saab Kockums. “Swedish

modular submarine design and production techniques coupled with the Dutch shipbuilding tradition bring together the capabilities needed to deliver an assured operational capability.”

Hein van Ameijden, managing director of Damen Schelde Naval Shipbuilding, added: “The result of the collaboration will be a customer-adapted submarine for expeditionary missions. This will ensure that the Royal Netherlands Navy continues to play an important role in European waters as well as globally.”

www.damen.com

www.saab.com

French Navy's Communication System

(df) Airbus announced that more than sixty vessels of the French Navy are now equipped with the 'Réseau Intranet de la Force Aéronavale étape 2' (RIFAN 2) system, ranging from aircraft carriers and front-line frigates to support ships, patrol craft based overseas, and submarines. Thanks to the system, all ships at sea can now establish secure broadband links with each other and with the onshore command centre. The RIFAN 2 programme contract, worth around €160 million, was awarded to an industrial group headed by Airbus as the prime contractor and comprising Naval Group and Rohde & Schwarz as co-contractors. The purpose of the programme is to equip the French Navy's surface ships and submarines with a truly secure intranet system. It is designed to transmit data with various classification levels, ranging from 'unprotected' to 'secret' and 'NATO secret'



(Photo: Airbus)

This network transmits data produced by the various applications, both to coordinate operations and for daily and logistical management of life on board, as well as to exchange data between information systems of theatre chiefs of staff on board a vessel for the duration of an operation. The system is capable of combining several communication streams in order to optimise the use of the transmission capacity available at sea, which is, by nature, limited. It therefore utilises satellite connections, such as Comcept or Syracuse, as well as radio communication resources. Existing radio systems have been refurbis-

hed, and a new UHF network has been deployed, which now allows all-IP (Internet Protocol) voice and data exchanges between ships, with a range of several tens of kilometres.

RIFAN 2 also provides overall network management and cybersecurity incident monitoring capability. This monitoring can take place both from an onshore management and control centre, or locally on board the ships, thus providing the crews with a degree of independence, so that they can make the best use of the network according to the operational situation.

The network will become increasingly dense with installation planned for the Barracuda submarines under construction, for medium-size frigates (FTI programme), which are to be the French Navy's future front-line vessels, as well as for the future replenishment tankers (FLOTLOG programme).

www.airbus.com

India Procures LRSAM Air & Missile Defense Systems

(df) Israel Aerospace Industries (IAI) announced it has been awarded an additional contract for supply of LRSAM Air & Missile Defense (AMD) Systems, the marine version of the Barak 8 AMD system, for seven ships of the Indian navy. The contract is worth \$777 million. It was made with the Indian state-owned company Bharat Electronics Limited (BEL) which serves as the main contractor in the project.

The LRSAM system, part of the Barak 8 Family, is an operational AMD system used by Israel's navy as well as by India's navy, air and land forces. It provides broad aerial and point defence against a wide range of threats to the marine arena from the air, sea or land. The system integrates several advanced state-of-the-art systems like digital radar, command and control, launchers, interceptors with modern RF seekers, data link and system-wide connectivity.

The Barak-8 AMD system was developed by IAI in collaboration with Israel's MoD,



(Photo: IAI)

India's DRDO (Defense Research and Development Organization), the navies of both countries, IAI's ELTA Group, RAFAEL and local industries in India and Israel.

www.iai.co.il

Naval Strike Missile For The U.S. Navy

(df) The Naval Strike Missile has been selected as the Over-the-Horizon Weapon System for the U.S. Navy's littoral combat ships and future frigates, Raytheon

announced. The missile demonstrated another mission capability this summer, land-based coastal defence. In the scope of a test the U.S. Army launched it from the back of a heavy wheeled vehicle during a live-fire, ship-sinking exercise at the Rim of the Pacific 2018 event in Hawaii.

The Naval Strike Missile is a long-range, precision strike weapon that can find and

destroy enemy ships at ranges up to 100 nautical miles away. The stealthy missile flies at sea-skimming altitude, has terrain-following capability and uses an advanced seeker for precise targeting in challenging conditions. Designed by Norway's defence company Kongsberg, NSM is now also being manufactured by Raytheon in the United States.

www.raytheon.com



Tests Of The New SM-2

(df) Five SM-2 surface-to-air missiles successfully completed five test flights in back-to-back summer exercises conducted at sea by the Republic of Korea Navy (ROKN), Raytheon announced. At these tests ROKN fired two Block IIIA missiles in an initial exercise to test the missiles' advanced semi-active radar seeker technology. During a second exercise, the navy destroyed three aerial threats using the Block IIIB variant. "These successful flight tests add to SM-2's impressive legacy of more than 2,700 suc-

cessful firings," said Mitch Stevison, Vice President Raytheon Air and Missile Defense Systems. "As we begin to produce a new generation of SM-2s, the missile will be in the inventories of navies worldwide for decades to come."

Raytheon restarted the SM-2 missile line in 2017 to meet global demands from international customers, which include eight international countries. The SM-2 missile gives navies the capability to defend against anti-ship missiles and aircraft out to 90 nautical miles. New deliveries are sche-



(Photo: Raytheon)

duled to begin in 2020 and will include 282 SM-2 Block IIIA and IIIB missiles.

www.raytheon.com

Optical Communication System

(df) The optical communication system developed by STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş. and Bahçeşehir University (BAU), which provides a link between submarines and divers, is intended to be integrated with the optical surveillance system of HENSOLDT, the companies announced at Euronaval. The joint project undertaken by STM with BAU for the development of optical communication systems aims to secure military



(Artwork: STM)

communication. STM-BAU has already developed a prototype optical communication systems that can provide communication between underwater units/platforms, underwater-air vehicles, naval surface-surface vehicles and stationary land platforms. Once serial production of

the prototypes begins and it is used in the field, it will complement RF (radio frequency) communication systems in terms of security and redundancy. The Optical Communication System will eliminate certain disadvantages of the RF system in areas such as interception, eavesdropping, and communication jamming, making communications more secure.

<https://bau.edu.tr>

www.hensoldt.net

www.stm.com.tr

Development Of An Electric Propulsion System

(df) BAE Systems has announced a £3.5 million commitment to develop greener and safer rechargeable electric propulsion systems. The investment will fund the development of a new test and integra-

tion laboratory, the company announced at Euronaval. "Our aim is to develop the next generation electric propulsion system which will be cleaner, greener, safer, more powerful, longer lasting, rechargeable and, in some cases, even able to operate underwater," said BAE Systems Project Mana-

ger Clare Gribby. "We've already invested around £1 million in concept and design work and will be moving towards the build and integration phase of a demonstrator in early 2019. The demonstrator is due to be up and running by September 2020."

www.bae-systems.com

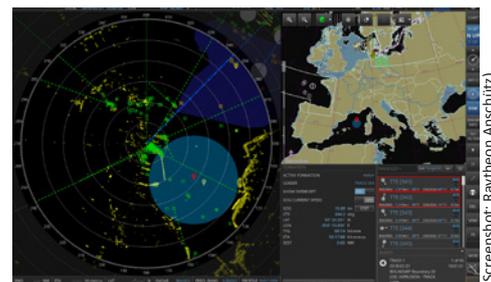
New Navigation Radar Software Synopsis Naval Radar NX

(gwh) At Euronaval Raytheon Anschütz presented the new Synopsis Naval Radar NX navigation radar software for the first time. The state-of-the-art software is based on an IMO radar display with optimized tracking characteristics and anti-clutter processing and is also equipped with tactical functions.

In addition, there is the video merging function, which integrates the video of se-

veral radar transceivers into a single, high-quality radar video. The modular software design offers a high degree of flexibility for future upgrades to adapt to the respective mission requirements.

To support specific naval requirements, Raytheon Anschütz has implemented tactical functions such as helicopter tracking, formation management, alarm and watch zones, and tactical target management in the radar software. This makes Naval Radar NX an effective and unique application



(Screenshot: Raytheon Anschütz)

for safe navigation and tactical tasks that can be performed within a single user interface.

www.raytheon-anschuetz.com

Modernisation Of Robust Laptops

(df) Dell has redesigned its notebooks for extreme conditions. The new robust models Latitude 7424 Rugged Extreme, Latitude 5424 Rugged and Latitude 5420 Rugged now offer even more performance and convenience, according to the company, including the use of the latest generation of quad-core Intel CPUs and graphics cards.

The dual battery configuration of the notebooks also enables zero downtime. The de-



(Photo: Dell)

vices are supplied with two rechargeable batteries that can be exchanged during

operation, increasing the notebook's battery life to over 14 hours.

In addition, all new notebooks are equipped with brighter and sharper FHD displays that cover an even wider colour spectrum. This ensures good display and legibility even in unfavourable lighting conditions. Users can therefore see everything clearly, whether they are in a dim hall or in an open field, and regardless of whether it is raining or they are in bright sunlight.

www.dell.com

Global 3D Elevation Model

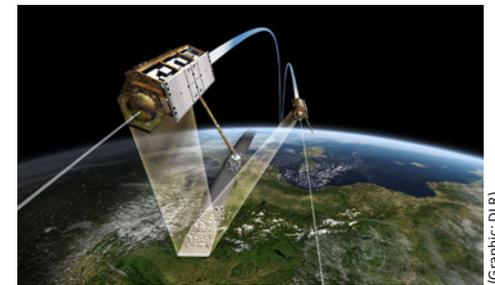
(gwh) The TanDEM-X elevation model with 90-metre scanning has been released for scientific use and is now available as a global data set. The German Aerospace Center (DLR) is thus aligning itself as part of the Copernicus Earth observation programme, which provides open and free access to satellite data.

The TanDEM-X-DEM covers all the earth's land surfaces with a total of more than 148 million square kilometres. The absolute height accuracy is one metre. This 3D image of the Earth was completed in Sep-

tember 2016 and is about 30 times more accurate than other global data sets. The elevation models created with TanDEM-X and TerraSAR-X also have the advantage that, for the first time, they capture the Earth with uniform accuracy and without gaps.

Currently, the two satellites are still recording the Earth in formation flight. After eleven and eight years in orbit, the satellites continue to function perfectly and have far exceeded their nominal life of 5.5 years.

DLR has also already designed a possible follow-on mission: The tandem L mission



(Graphic: DLR)

concept provides for two radar satellites in the L-band (23.6 centimetres wavelength) and is intended to record the dynamic processes on the Earth's surface with millimetre accuracy.

www.dlr.de

Encrypted Mobile Phone For NATO

(gwh) Swedish Sectra AB provides the NATO with Tiger/S 7401 mobile telephones with which strictly confidential information up to the NATO SECRET level can be exchanged in encrypted form. The phones

were developed in cooperation with the Netherlands National Communications Security Agency (NL-NCSA) and certified in February 2017. Sectra Tiger/S 7401 also enables secure communication between different security areas. This means that a

user can communicate securely with colleagues in NATO, the EU and their respective national networks via a single telephone. The phone is also approved for communication on mobile and fixed devices.

www.sectra.com

Secure WhatsApp

(df) One trend in IT security is building up functions, only in a secure and safe way. The German company Rohde & Schwarz Cybersecurity now presented a messenger that corresponds to WhatsApp in terms of appearance, functions and use. But instead of trusting in Facebook (that now owns WhatsApp) with data probably being read by several interested parties, the R&S Trusted Communicator – the official name of the messenger – offers secure encrypti-



(Photo: Dorothee Frank)

on that does not even allow the manufacturer to view the conversation. The app itself is already in a secure container, so that its security is guaranteed regardless of

the device and the software on it. End-to-end encryption to the other communicators takes place from this estimated area. The user can chat just like with WhatsApp, share photos, set up groups, add contacts, but in contrast to WhatsApp everything is secure. Secure voice, i.e. encrypted telephone calls, are also possible. The Messenger can be run on all modern Apple and Android devices, but with a cryptography that meets the NATO SCIP standard.

www.cybersecurity.rohde-schwarz.com

NIAS18

Dorothee Frank

Last week NATO's largest annual cyber security forum hosted by the NATO Communications and Information Agency (NCI Agency), NIAS18, took place in Mons, Belgium. The three-day event brought together an audience of over 1,700 international cyber security specialists. It was accompanied by a display with 87 exhibitors, who presented their newest or already battle-proven systems to the visitors.

What is particularly interesting about the concept is that the real NATO experts meet with the experts of the companies here in order to discuss the most burning issues of IT security for three days in a rather undisturbed and informal atmosphere. It is neither a sales event nor a marketplace, but a real meeting place for the exchange of ideas, which is unique in Europe so far. The structure of the lecture programme is in accordance with this format. In addition to speakers from the NCI or other NATO agencies concerned with IT security, speakers from industry showed how they have implemented appropriate solutions in their companies or what problems they are currently struggling with. Completely without product pricing, but as expert to expert, at eye level, in partnership.

Mark Ryland, CISO of Amazon Web Services, described an interesting (and apparently successful) approach to ensuring IT security. "Security is part of every single element of the process," Ryland said. "And we at Amazon always want to go from the source, especially the source code. Talking about security you don't want to take binary from outside." Accordingly, Amazon's security does not rely on the adoption of foreign code or the patching of functions, but on the knowledge of the code. And the implementation on the basis of this code known to the company. "The proper way to fix a problem is to go back to the source code," stressed Ryland. Nowadays,



(Photos: Dorothee Frank)

the entire infrastructure has to be thought of as code. "That means everything, from the harbour to the storage system, is code," said Ryland. "Security is the pipeline. If you do this job right, you have not much to worry."

According to Ryland, security stands and falls with this knowledge of one's own source code. A concept that Amazon had implemented directly and continuously from the start. However, despite the correctness of Ryland's statements, a real and life implementation may cause certain problems for the armed forces, since it seems almost impossible to actually know the code in view of the enormous varie-

ty of third-party software. Not to mention the hint, that for security reasons one should not actually integrate foreign binaries. Nevertheless, the approach gives reason to think whether too little attention has been paid to source code so far and, despite all the enthusiasm about the possibilities of artificial intelligence (AI), that AI might contradict the need for security at this point.

The slides of (almost) all presentations can be found on the NIAS18 website. It remains to be hoped that this exceptional event will take place again in the coming years in the usual length and depth.

www.nias2018.com

Indra Becomes Part Of Nato's Cyberdefence Network

(df) Indra announced it has been selected by the NATO Communications and Information Agency (NCIA) to join the network of companies that work with this agency exchanging intelligence on cybersecurity to reinforce its mutual situational awareness and detect, prevent and respond to any cyber attack. The corresponding industrial collaboration agreement was signed at NIAS18.

With this agreement Indra joins NATO's public-private collaboration model in cyber defence and will exchange cyber intelli-

gence to contribute to the anticipation and response against increasingly numerous and sophisticated cyber threats.

Kevin J. Scheid, General Director of the NCIA, said that, with this agreement, "we are strengthening international cybersecurity alliances and optimising NATO's collective defence missions. Only by working together will we be able to cope with the host of digital threats that we face."

"The pride that this milestone represents for Indra and the company's desire to support the agency with all its knowledge and experience is a highlight of our work we did with NATO so far," said Miguel An-



gel Acitores, Security Director of Indra. "At Indra, we are convinced that public-private cooperation in this area is essential. We need to optimise our cyber forces in the most efficient and consistent manner possible."

www.indracompany.com

Infodas Launches Novelty At NIAS18

(df) Infodas took the NIAS18 as an opportunity to present its new network interface controller to an international military audience for the first time. This is a piece of hardware that has not actually existed anywhere in the world before, as it is a network interface controller that cannot be manipulated. It will probably receive approval for GEHEIM (SECRET) from the German IT security testing authority BSI before the end of this year.



The need for such a secure network interface controller already arose after the evaluation of the Snowden documents, in which the BSI found out that the network

interface controllers represented a major weak point. In addition, there were more recent reports about the so-called espionage microchips from China. A corresponding hardware approved for SECRET was therefore necessary, which was now presented by Infodas. All future Infodas devices are to be equipped with this new component in future. In addition, the secure network interface controller has standard interfaces so that it can also be used by other manufacturers for their products.

www.infodas.de

Bittium's Secure Communication Solutions

(df) At NIAS18 Bittium showed their solutions for secure and reliable military communication, like the secure Bittium Tough Mobile LTE smartphone and related Bittium Secure Suite back-end system. Bittium Tough Mobile is a secure and strong Android-based LTE smartphone combining information security and commercial device technologies. The smartphone incorporates a hardware-based security platform, which enables strong device security as well as deep integration of both customers'

own and third party software security solutions.

Also the Bittium Secure Suite device management and encryption software that complements Bittium Tough Mobile smartphone with a scalable set of new software services for remote management, remote attestation and securing the network connections of the device, was another interesting exhibit. Bittium Tough Mobile smartphone and Bittium Secure Suite together form a quite reliable system for processing and transferring encrypted and classified material, and therefore securing



critical communications. Other elements, like Bittium SafeMove Analytics, evaluate the traffic to help organisations to monitor network connectivity and performance.

www.bittium.com

Invention For The Intelligence

(df) At NIAS18 BAE Systems presented their XTS Guard 5, that is equipped with the company's Geospatial eXploitation Products (GXP). The XTS Guard 5 has already successfully demonstrated its ability to provide U.S. and Coalition intelligence organisations with access to geospatial imagery and data from BAE Systems' GXP Platform, therefore ensuring secure sharing between networks of various security classifications and sections.

"Our expertise in developing technologies that quickly exploit massive amounts of data has allowed us to integrate products



that bring numerous advantages to U.S. military intelligence organisations to securely transfer data from multiple sources," said Kevin Malone, vice president of Analytics Systems at BAE Systems. "The EC-18 demo

proved XTS Guard 5's readiness to deliver operational success for a number of agencies."

As an intelligence organisation accesses geospatial imagery and data from BAE Systems' GXP Platform, the XTS Guard 5 provides cross-domain search functionality. This breaks down information stovepipes and secure boundaries that currently exist, providing a bridge between security domains to allow intelligence analysts to quickly and easily gather information that was previously cumbersome and time consuming to obtain.

www.baesystems.com

New Cloud-To-Cloud High-Speed Solution

(df) At NIAS18 Owl Cyber Defense Solutions (Owl) announced the release of the new Owl Cloud-to-Cloud (C2C) cross domain solution. C2C is a proprietary, data diode-based cybersecurity solution, designed for secure, extremely high-volume, high-bandwidth file transfers from one cloud repository to another.

Typical cloud-to-cloud transfers involve a long and labour-intensive process when cloud repositories are downloaded

to numerous hard drives and physically transferred to the new cloud repository, where they are uploaded. The C2C solution is designed to significantly reduce transfer times, by transferring data one-way directly from cloud to cloud, while also greatly increasing the security on the transfer process by eliminating potential attack vectors.

"We're extremely excited to unveil the Cloud-to-Cloud to the government, intelligence, and defence markets," said Mike Timan, Owl President & CEO. "This solution



represents the new industry standard for maximum security and throughput in cross domain solutions for the cloud, and could potentially save our clients hours or days of transfer time in a single job."

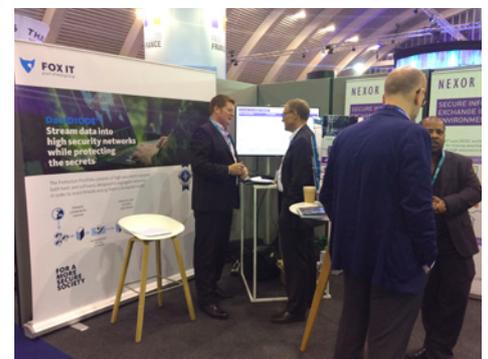
www.owlcyberdefense.com

Ruggedised DataDiodes

(df) At Nias18 Fox-IT and its partner Nexor showed their ruggedised 1G and 10G DataDiodes. Both have received the Common Criteria Certification at Evaluation Level (EAL) 7+ for Information Technology Security Evaluation. By meeting this security certification the Fox-IT DataDiode guarantees the unidirectional flow of data at a physical level by enforcing a one-way network connection. By using these devices information is derected into the agency, company or other entity, but really no data can be retrieved in the opposite direction.

The DataDiodes do not contain software or firmware, therefore they cannot be exploited or misconfigured. Due to the ruggedised design the diodes can also be used in demanding environments with extreme high or low temperature and humidity levels, dust, movement etc. and are therefore suited for military use.

The ruggedised DataDIODEs provide the following key features: Industry standard fibre optic lc connectors; Rugged coated steel and anodised aluminum casing; Extended temperature and humidity range; TEMPEST level-A compliant by default;



Suitable for transport; Shock and vibration resistant: truck, rail, air (non-operational) ASMT D 4728.

www.fox-it.com

Industry & Trade

Global Compact Network Finland

(df) A new network has been founded: The leading Finnish companies operating in international and domestic markets declared they have established Global Compact Finland Network to gather up all the Finnish companies and organisations committed to the UN Global Compact initiative. The new network will begin its operation in stages during this year. The target is to strengthen the Finnish companies' pioneering in corporate responsibility and sustainability. There are 78 companies in Finland that have committed to the Global Compact initiative so far that have been in close cooperation with the other Nordic companies in Global Compact Nordic Network. In accordance with the UN objective also

a national network has been established in each of the Nordic country. Together with Denmark and Sweden Finland is acting as a pioneer.

The ten principles of Global Compact Network, that the companies have to stick to, cover four areas.

Human Rights: Principle 1: Businesses should support and respect the protection of internationally proclaimed human rights; and Principle 2: make sure that they are not complicit in human rights abuses.

Labour Standards: Principle 3: Businesses should uphold the freedom of association and the effective recognition of the right to collective bargaining; Principle 4: the elimination of all forms of forced and compulsory labour; Principle 5: the effective abolition of child labour; and Principle 6: the

elimination of discrimination in respect of employment and occupation.

Environment:

Principle 7: Businesses should support a precautionary approach to environmental challenges; Principle 8: undertake initiatives to promote greater environmental responsibility; and Principle 9: encourage the development and diffusion of environmentally friendly technologies.

Anti-corruption: Principle 10: Businesses should work against all forms of corruption, including extortion and bribery.

<https://gcnordic.net>



Network Finland

MASTHEAD

ESD Spotlight

Email newsletter of the magazine "European Security & Defence" (ESD)

Editor-in-Chief: Dr. Peter Bossdorf

Managing Editor: Dorothee Frank (df)

Editors: Stephen Barnard (sb), Wilhelm Bocklet (wb), Gerhard Heiming (gwh)

Layout: Dorothee Frank



Published by

Mittler Report Verlag GmbH

A company of Tamm Media Group

Mittler Report Verlag GmbH
Baunscheidtstrasse 11
53113 Bonn, Germany
Phone: +49 228 350087-0
Telefax: +49 228 350087-1
Email: esd.spotlight@mittler-report.de
www.euro-sd.com

Managing Directors: Peter Tamm, Dr. Peter Bossdorf and Thomas Bantle
The company is located in Bonn
District Court of Bonn – HRB 18658
Identification number DE 811 223 089

To subscribe or unsubscribe please send an email to: esd.spotlight@mittler-report.de

New Armaments Group L3 Harris Technologies

(gwh) Communications and radar equipment manufacturer Harris Corp. and technology company L3 Technologies have agreed to merge their two companies. The new company is expected to be formed through an exchange of shares (1.3 Harris shares per L3 common share), subject to regulatory approval, by mid-2019. The combined company will be named L3 Harris Technologies and will be headquartered

in Melbourne, Florida. With sales of €13.6 billion, it will be the sixth largest defense company in the U.S. and the tenth largest in the world.

William M. Brown (previously Harris Corp.) will be the first Chairman of the Board and CEO, and Christopher E. Kubasik (previously L3 Technologies) will be the COO. After two years, both will swap functions.

www.l3t.com

www.harris.com

Cooperation For Safety And Security

(df) Rohde & Schwarz Cybersecurity and Panasonic Business announced their cooperation to jointly offer mobile IT solutions for the highest security requirements. As part of the cooperation, Rohde & Schwarz Cybersecurity is selling the latest Panasonic Android devices - 5" handheld FZ-T1 with barcode scanner and 7" tablet FZ-L1 - and equipping them with R&S Trusted Mobile, a secure (hardened) operating

system based on Android. With this cooperation, Panasonic and Rohde & Schwarz are addressing cybersecurity customers who require hardware security in the form of robust, long-lasting end devices with maximum operational availability, while at the same time placing particularly high demands on cyber security, like armed forces, police, disaster relief organisations or businesses with corresponding needs.

www.panasonic.com

www.cybersecurity.rohde-schwarz.com

TechNet Europe 2018

The two-day conference organised by AFCEA Europe in cooperation with the AFCEA Rome and Naples chapters, will be held under the patronage of the Italian Ministry of Defence. Representatives from some of the highest levels of the European and NATO institutional, academic and industrial world will discuss the current situation, challenges and the various prospects of maritime situational awareness.

November 6-7, Sorrento, Italy



International Fighter 2018

Join International Fighter 2018 to hear about Canada's Future Fighter project, the RAF's ongoing integration of the F-35, France's view of the multi-domain battlespace and the Spanish MoD's next generation weapons system. All that alongside an audience of 200+ air force commanders, senior operators, pilots, programme managers, policy leads and industry leaders, who will gather at the only fighter-specific air power conference – globally.

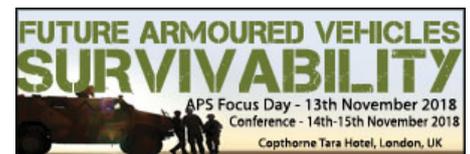
November 13-15, Berlin, Germany



FUTURE ARMoured VEHICLES SURVIVABILITY

As the only event purely dedicated to the area of vehicle protection, Future Armoured Vehicles Survivability 2018 will deliver a strong focus on the relationship between current requirements, emerging technologies and how these might be leveraged to enhance force protection.

November 13-15, London, UK



NIDV-Symposium – 30th edition

During the NIDV-Symposium and exhibition more than 130 companies show their potential. The top political level of the Ministries of Defence, Economic Affairs, Foreign Affairs and Security & Justice are invited. A special programme for the military attachés accredited in the Netherlands is offered. Sister organisations of the NIDV from abroad are also invited. And last but not least, representatives of the armed forces, the police, the fire brigade, the ambulance dispatch centre, the coast guard and other public security organisations are present.

November 15, Rotterdam, The Netherlands



I/ITSEC

The Interservice/Industry Training, Simulation and Education Conference (I/ITSEC) is the world's largest modeling, simulation and training conference. It consists of peer-reviewed paper presentations, tutorials, special events, professional workshops, a commercial exhibit hall, a serious games competition, and STEM events for teachers and secondary students. I/ITSEC is organised by the National Training and Simulation Association (NTSA).

November 26-30, Orlando, USA



International Security Expo

This year's International Security Expo showcases over 1,000 of the latest innovative security products to help improve the security. Featured over the two-day expo are 13 free-to-attend, CPD certified conferences and workshops covering every major sector of the security industry. Visitors will see ground-breaking, innovative features including the 300 SQM Protecting Urban Spaces Demonstrator designed to help every security professional understand how best to protect crowded spaces.

November 28-29, London, UK

