Roadmap Security

Top Sector HTSM

May 2018

Content

1 Societal and economic relevance 3
1.1 Societal challenges addressed in this roadmap 3
1.2 The domestic and global market (2018-2025) 4
1.3 Competitiveness of the Dutch industry 4
1.4 Roadmap positioning 5
2 Cybersecurity 6
2.1 Context 6
2.2 Areas of application and technological challenges 7
2.3 Priorities and Programmes 9
3 Active and Passive Sensor Systems 10
3.1 Context 10
3.2 Areas of Application and Technological Challenges 10
3.2.1 Radar and Integrated Sensor Suites 11
3.2.2 Passive Sensor Technology 11
3.3 Priorities and Programmes 13
4 Mission Critical Systems 14
4.1 Context 14
4.2 Areas of application and technological challenges 14
4.2.1 Naval systems 14
4.2.2 Land-based vehicle platforms 16
4.2.3 Protection of IT infrastructure 16
4.3 Priorities and Programmes 17
5 Partners and process 18
6 Investments 19

HTSM Roadmap Security

1 Societal and economic relevance

1.1 Societal challenges addressed in this roadmap

The Netherlands has for long been a strong and safe nation, with deep-rooted beliefs in the value of openness, innovation and entrepreneurship. Close cooperation between government, citizens, research institutes, academia and industry has been a cornerstone of Dutch innovation and has made the Netherlands one of the strongest and most resilient economies in the world. The Netherlands is recognized around the world for its high-tech products, scientific knowledge and its leadership in innovation in all sectors of industry and all aspects of life.

Defence and Security are essential conditions for a flourishing society and a thriving economy. The Netherlands faces complex security challenges in the coming decades that demand innovations to protect national security interests, such as the continuity of the vital processes, protecting the integrity and exclusivity of information and monitoring the functioning of the democratic legal order. A role for the government is also conceivable in situations where there is no longer a level playing field in economic traffic and this is caused by the actions of state actors.

The impact is aimed at strengthening the global leadership and competitiveness of the Dutch industry, specifically through and in cooperation with our national defence and security industry, associated technology suppliers and universities. We aim to achieve this by strengthening the market position and knowledge position of the national (defence/security) industry, the related industries in the supply chain hereof and of the knowledge institutes respectively. One of the major goals is to accelerate the speed of innovation by consistency in joint roadmaps, creating unique products and an open exchange of knowledge and by increasing the scale.

The products and technologies in this domain distinguish themselves compared with others due to the nature of the defence/security domain. Therefore, cooperation is crucial in a ‘triple helix construction’ between knowledge institutions, industries and supplying technology companies and military/security stakeholders (both national and European level), whereby all together ensure at an early stage the development of an optimal knowledge base that is innovative, trend-setting and leading the way.

Dutch society has historically stressed the importance of defence and security. Defence and security are vital conditions for a prosperous society. The government is known for issuing strong policies to counter threats to society and investing significantly in Defence and National Security. This has led to highly-effective defence and law enforcement agencies, robust infrastructures and a society that has demonstrated its ability to cope with the many recent challenges to national security, business continuity and democratic order.

However, the world will face rapid and fundamental changes due to technological advances, geopolitical shifts and environmental changes. Further adoption of digital technologies will change the very fabric of society, and will forever change the way we communicate, collaborate, do business and live our lives. Through networks, everything and everyone will be connected, across distances, frontiers and time. The barriers between the physical and digital world will dissolve further and will transform the way our vital infrastructures are built and our society functions.

These developments will challenge national security in unprecedented ways and necessitate new capabilities to safeguard digital, physical and operational security. Threat actors will exploit vulnerabilities in this evolving landscape for the purpose of subversion, terrorism or organised crime and challenge traditional countermeasures. Additionally, the hyper connectedness of societal systems will demand new forms of control and governance, and test the human ability to oversee and manage.

Digital security has quickly evolved from a networking issue into an IT and system (of systems) challenge, including its surrounding processes and human factors. It is focussed on creating a safe and secure digital environment in which the economy can thrive, and criminals have little chance to interfere. As for operational security, civilian and military agencies in operational duties need to be equipped with tools and platforms that allow them to observe, communicate and act in time, using accurate information. This will require new sensor- and data-integrating platforms that are safe, secure and effective to cope with tomorrow's operational challenges. New threats to physical objects, vital infrastructure and persons will require new levels of physical security, such as novel protective materials, smarter surveillance systems and the use of robots for protection of assets. The development of these innovations requires effective concept, development and experimentation strategies, and will need to embrace all to the intricacies of the human factor to result in effective assets for the Netherlands.

To counter these challenges, the Dutch Industry must work with the security sector and capitalise on its strong research, development and innovation capacities. The security sector needs to overcome fragmentation of effort, and make better advantage of available resources and expertise. To this end, it is important to establish smart supply and demand coordination between government, vital sectors, companies and research institutes (academic and applied) and build joint research and development efforts. These efforts need to result in an effective innovation chain that swiftly brings exploratory research into applied research and implementation at customer level.

The *HTSM 2018 R&D Roadmap Security* sets out the major challenges and opportunities in three priority areas of national security: **Cybersecurity, Active and Passive Sensor Systems** and **Mission Critical Systems** .

1.2 The domestic and global market (2018-2025)

Because of the continuing threat of terrorism and global geopolitical tensions, the security and defence technology market sees significant growth. There is a wide interest in high-tech developments and a strong demand for rapid innovation and product development.

With a turnover of €97.3 billion in 2014, the EU defence industry provides a wealth of highly skilled jobs with 500,000 people directly employed in the sector and an additional 1,200,000 indirect jobs. Similarly, the EU security industry has a fast-growing market value of around €35 billion, and employs 180,000 people. Europe is currently the second largest security market in the world.

The size of the European market for the security industry, excluding the defence industry, is estimated at approximately €40 billion. The national market has an approximate market size of €1 billion per year, with a related R&D effort of more than €100 million annually.

1.3 Competitiveness of the Dutch industry

This roadmap is grounded in the ambition of the Netherlands government (in particular by the Ministry of Economic Affairs, Ministry of Defence and the Ministry of Justice and Security) to create a strong security-related innovation chain and to connect this chain to the challenges of the Dutch

industry as a whole. Launching customership has been the guiding principle for these ministries for quite a while and, in addition to the deployment by their own departments, these ministries also contribute to the export potential (in an economic and international political sense) of the Dutch industry in a non-level global playing field.

In the area of Mission Critical Systems, the Dutch as well as the European research & development (R&D) infrastructures are very well set-up to obtain a solid industry position in this emerging market. The strategic cooperation between DMO, TNO, Thales and RHMarine exploits these opportunities through a "triple helix construction" which supports the innovation of industrial products with national and European long-term research programmes. For the national and export markets there are significant opportunities for combat management systems and platform management systems. TNO as a research institute, combines artificial intelligence technology with systems engineering and software architecting to automate situational awareness and decision making in complex systems of industry for e.g. combat management and platform management. Regarding combat management systems, the TACTICOS CMS of Thales is sold worldwide to over 20 navies across Europe, Asia, Latin America, the Middle East and North Africa. For the Dutch navy, Thales performs research on CMS functionalities in close cooperation with DMO/JIVC. With regard to platform management, RHMarine is an expert in automating and integrating systems for propulsion, power generation, navigation and electrical installations. Besides serving the Dutch navy, RHMarine exports its products to countries such as the United Kingdom, Singapore, Poland, Morocco, and Oman.

Given the strong and persistent growth in both the domestic and global market for cybersecurity solutions in combination with the Dutch knowledge and industry base, the economic potential for cybersecurity solutions is substantial. Recent initiatives by the Ministry of Justice and Security and the Ministry of Defence to strengthen this knowledgebase and the national resilience against digital infringements confirm this. Under the present circumstances the dependency on foreign cybersecurity technology is still very high in the Netherlands.

The Netherlands has an excellent and confirmed market position in the global Radar System market. Market analyses show significant further potential. In the area of active sensors, the Netherlands holds a top position in the world market, both in terms of knowledge and industry and facilitated by a launching customer of highest international standing, i.e. the Royal Netherlands Navy and is a powerful innovative player in this area. In the accessible markets the Netherlands is world leader in the area of radar and command and control systems in use by first and second tier Navy organisations.

The involvement of end-users and other stakeholders during research, development and innovation processes contributes in a very direct manner to solving public security issues. In addition, it provides a significant spin-off effect to the competitive ability of the Dutch defence and security sector. The private security sector has shown distinct growth the last years, due to privatisation of areas of government responsibility (outside the monopoly on the use of force) and the focus on and transfer towards the personal responsibility of citizens and businesses. Against this background, there is a good prospect for companies in the HTSM sector in the security domain to strengthen their economic activities.

1.4 Roadmap positioning

The HTSM Security roadmap is closely linked to many other HTSM roadmaps, contributes to the development of several key enabling technologies (*'Sleuteltechnologieën')* and thus provides for many of the societal challenges.

The primary societal challenges to which HTSM Security contributes is **'Safe and Secure Society** '. HTSM Security offers key technological innovations that contribute to the main challenges in this area, especially in the area of cybersecurity, observation capabilities and operational control. In concertation with the results from other roadmaps. Such capacities help the Dutch society to respond to better respond to new digital, natural and operational threats, and form essential building blocks for new societal capacities.

The innovations from HTSM Security are also relevant for other MU's, especially those where ICT and security play a significant role, such as '**Mobility and Transport'**, '**Healthcare and welfare'** and '**Inclusive and Innovative Society**'. Each of these MU's demand secure and capable infrastructures, high levels of data protection, effective observation capabilities and strong operational control platforms. Even for seemingly less relevant MU's, such as **'Agriculture and Food'** and '**Climate and Water management**' the HTSM Security can provide valuable contributions because of the increasing use of smart sensor technology and internet-based systems in these areas.

Furthermore, HTSM Security is a key contributor to **Key enabling technology 'ICT**' (network security, information security) and '**Quantum and Nanotechnology**' (encryption) through its cybersecurity innovations. Furthermore, HTSM Security developments in Active and Passive sensor systems are directly linked to the key enabling technologies '**Photonics'**, '**Micro and Nano-Electronics'** and '**Measuring and Detection Technology'**. Development in these areas support HTSM Security, and vice versa. For other key enabling technologies, possible contributions from and to HTSM Security are less pronounced, but not inconceivable.

Through these contributions, HTSM Security can contribute to various other HTSM roadmaps, such as '**Healthcare'**, **'Smart Industry'**, '**Automotive'** and '**Aeronautics'** where secure information infrastructures and sensor technologies are prime assets.

2 Cybersecurity

2.1 Context

The world is rapidly transforming through digitization. Digital networks and cyber-physical systems are entering every aspect of society, and cause tremendous changes in the way people work, communicate, travel and live. Information & Communication Technology (ICT) has become one of the main pillars upon which communities and businesses are built.

The impact of digitization is usually perceived through the benefits it brings. Digitization brings great new opportunities to businesses, individuals and governments, and enables the creation of inspiring new means to connect, share, communicate and experience. However, with the wide embrace of digital systems, we also need to accept new security challenges. Cyberspace yields new opportunities for malicious actors to destabilize society and take advantages of vulnerabilities for criminal gain. As our hyperconnected society will become wholly dependent on digital systems and services, our traditional views on security will need to be updated, alongside an updated arsenal of instruments and practices. We will need to develop a new understanding of digital security and build appropriate capacities to safeguard the wellbeing of business and individuals.

R&D in cybersecurity has two main drivers in the Netherlands: the protection of National Security, and the preservation of business continuity and earning capacity.

For National Security, the main governmental stakeholders in cybersecurity R&D are the Ministry of Justice and Security and the Ministry of Defence. Research, Development and Innovation in National Security is driven by various joint and sectoral roadmaps, and focusses on the strengthening of civil and defence ICT systems, enhancement of cyber intelligence capabilities, the fights against cybercrime, and the prevention of disruption due to cyber-attacks on critical infrastructures. Also, for the Ministry of Defence, the build-up of offensive cyber capabilities is an important focal point.

For the preservation of business continuity and earning capacity, the main governmental stakeholder is the Ministry of Economic Affairs and Climate Policy. Its 'Topsectorenbeleid' is focussed on creating the conditions in which businesses can thrive and grow. All nine 'top-sectors' are susceptible to cybersecurity challenges (e.g. protection of intellectual property, personal data, and business continuity) and require digital security to fulfil their role as foundation of the Dutch economy. Moreover, as many innovations in these top-sectors are highly dependent on ICT as key enabling technology (e.g. smart industry), the dependency on ICT and the need for strong cybersecurity will only increase. For that reason, this roadmap is closely connected to the **HTSM Roadmap ICT**, in which cybersecurity is mentioned as an essential capacity for businesses, government agencies and other organisations to thrive. In addition, the cybersecurity challenges create new business opportunities for novel cybersecurity products and services.

This requires well-coordinated research, development and coordinated innovation across sectors and (inter)national governmental institutes.

2.2 Areas of application and technological challenges

Cybersecurity stems from several key capacities: the ability to design secure systems, the capacity to withstand attacks, the ability to safeguard privacy and identity, the capacity to govern effectively and the ability to provide society with cyber defence capabilities. These capacities provide businesses and government agencies such as the National Cyber Security Centre, intelligence services, National Police and the Ministry of Defence with the tools and knowledge to enhance their cyber resilience and contribute to the cybersecurity of the Netherlands.

Each of these capacities requires smart technological innovation and active participation in public-private partnerships to collaboratively work towards implementation.

Challenges are not only technical. With the increasing digitization the number of non-technical challenges of legal, economic, social and human nature are rapidly increasing. Ongoing research is needed in the multi-disciplinary field of cybersecurity. A guiding document for multi TRL research in the Netherlands in this area is the (soon to be published) National Cyber Security Research Agenda version 3 (NCSRA III), written by a broad team of authors with input from several field consultations. A preliminary version can be found on www.dcypher.nl.

Based on the preliminary NCSRA III and other relevant national and international policy documents and agendas, a non-exhaustive list of general research subjects has been produced, addressing areas of application and technological challenges in cybersecurity. These subjects are meant to give context to the diverse nature of cybersecurity research and to provide inspiration to policy makers, researchers and other interested stakeholders to develop answers for the security challenges mentioned above.

In more detail:

- **Horizon scanning and predictive analysis of innovations.** The cybersecurity landscape is turbulent and rapidly evolving. Horizon scanning is a method to gain insight into nearing

technological and societal development. The ability to perform effective horizon scanning is crucial asset in attaining cybersecurity.

- **Cyber capacity building and cyber workforce development.** Attaining cybersecurity requires the build-up of a wide class of capacities, ranging from technological development to strategic planning. The build-up of required capacities demands a suitable workforce, and necessitates the development of educational courses and practical training.
- **Secure behaviour (beyond awareness).** Cybersecurity warrants proper secure practices and digital hygiene. Effective training programs and support instruments can help to incentivise citizens and organisations to behave more securely and ultimately result in inherent cybersecure behaviour of individuals.
- **Cybercrime & fraud.** With businesses and social networks going online, cybercrime, data theft and fraud have become commonplace in the digital domain. Businesses and governments need tools and practices to counter.
- **Impact of the advent of quantum computing (incl. (post) quantum crypto).** As current crypto is impacted by quantum computing, there is a growing urgency in developing quantum safe algorithms.
- **Testing and certification.** A more thorough understanding of the performance of cybersecurity technology is needed, given the high complexity of the hard- and software and a high dependency on foreign and less trusted solutions. Certification standards and policies for testing of systems- and software security are needed to provide sufficient assurance for users. Especially end 2 end cybersecurity, for instance in IoT applications, still needs development
- **Governance, data privacy and ethics.** The digital society poses significant challenges to current approaches to governance, privacy and ethics. These aspects need to co-develop with technological innovations and be an integral part of RD&I in the cybersecurity sector.
- **Cybersecurity and Resilience Concepts**. Our hyperconnected society has become very dependent on critical (information) infrastructures but needs to stay resilient at the same time. Understanding this complexity requires a variety of solutions and innovative concepts, involving collaboration and information sharing in networks or during cyber incidents, risk management, governance and other solutions on a technical and human factor level.
- **Secure design**. Cybersecurity in systems design is seen as an afterthought for producers, for instance in IoT devices. To address cybersecurity in systems during their whole lifecycle, a secure design and development is required.
- **Cybersecurity Monitoring & Detection.** To counter cybersecurity threats, governments and businesses still need better tools to monitor their digital assets, in order to respond quicker to threats. In the mid to longer term the challenge is to develop automated / autonomous response mechanisms (based on AI systems).
- **Data analytics and AI for cybersecurity.** AI and advances analytics provide powerful opportunities to understand network traffic and threat actor behaviour.
- **Understanding societal challenges in an era of hybrid and cyber warfare.** Hybrid and cyber warfare test the resilience of our new digital society. The intents, practices and implications of hybrid warfare by foreign actors needs to be understood.

Jointly, these areas of application and technological challenges are meant to form a first basis upon which the HTSM partners in the Defence and Security Systems roadmap can contribute in order to build a strong foundation for cybersecurity in the Netherlands.

2.3 Priorities and Programmes

The activities in this section of roadmap will be implemented in close alignment with key roadmaps, knowledge-, research- and innovation agendas in the cybersecurity domain, and in close collaboration with primary national and international stakeholders.

National

The work in this roadmap will be aligned with the primary objectives of the Netherlands Cybersecurity Agenda (NCSA), as published by the Ministry of Justice and Security in May 2018[1], and the forthcoming Netherlands Cybersecurity Research Agenda III (NCSRA), the national research agenda that will be the frame of reference for cybersecurity research and innovation programs both nationally as well as with international partners.

This section of the HTSM Security roadmap will be implemented in close cooperation with key governmental stakeholders such as the Netherlands National Police, The Ministry of Justice and Security, The Ministry of Defence and the Netherlands Cyber Security Centre (NCSC). Furthermore, research will be carried out in Cooperation with dcypher (the Dutch public-private agenda setting platform for cybersecurity research and higher education, established by the ministries of Economic Affairs and Climate Policy, Education, Culture and Science, Justice and Security and the Netherlands Organization for Scientific Research), and in partnership with centers of expertise, such as The Hague Security Delta and the forthcoming Cross-Sector Security Testbed[2]

International

Because of the international dimension of cybersecurity, it is important to link the work in this roadmap to international cyber capacity building activities.

Dutch RTOs are very active in the EU Research and Innovation Framework programmes (such as H2020 and the upcoming Horizon Europe programme) and will link the innovations from this roadmap into forthcoming research proposals. Cybersecurity is a key topic in the Secure Societies and ICT work programmes, and thus offers ample options for alignment and dissemination.

Furthermore, the work in this roadmap will be synchronised to EU cybersecurity policy directives where possible, and in cooperation with other research organisation and stakeholder networks, such as the cPPP European Cybersecurity Organisation (ECSO) and ENISA.

Additionally, cooperation will be sought with international networks such as the Global Forum on Cyber Expertise[3] and Interpol to results from this roadmap contribute to global cyber capacity building.

[1] NCSA: https://www.nctv.nl/ncsa

[2] Cross-Sector Cyber Testbed: https://roadmapnexteconomy.com/project/cross-sector-cyber-testbed/

[3] GFCE: http://thegfce.org

3 Active and Passive Sensor Systems

3.1 Context

Sensor and data integration together with a capability to transform (sensor) data into user required information are crucial for Operational security to modernize the strength of a future-proof, adaptive armed forces. Operational Security being next to Digital Security and Physical Security one of the primary challenges of the Societal Theme 'Safe Society'. The Ministry of Defence has indicated in their February 2017 memorandum "*Houvast in een onzekere wereld – Lijnen van ontwikkeling in het meerjarig perspectief voor een duurzaam gerede en inzetbare krijgsmacht*" that their strength should be modernized and that a future-proof, adaptive armed forces is necessary.

This is particularly applicable in the maritime domain where new naval ships require advanced sensor technology to carry out war and peace keeping missions as effectively as possible and against minimal risks. Particularly standalone sensors and interoperable networks of sensors rely on dedicated Active Electronically Scanned Array antennas (AESA is also often referred to as phased-arrays) for radar systems, including custom RF, mixed-signal, digital assisted RF and digital electronics. RF microchips on Si, SiGe, GaN and on GaAs semiconductor technologies are enabling technologies for those new systems solving performance issues around range, robustness selectivity, efficiency, spectrum purity and signal generation and which are dealt with in the HTSM Roadmap Electronics (Components and Circuits).

Netherlands Navy and Netherlands industry and research institutes have an excellent and renowned position worldwide in this area. Often referred to as 'Worldclass Navy, Worldclass Radar, Worldclass Innovations: Dutch Design'.

This cooperation is strategic and the importance of the aforementioned domain and method of cooperation in the ecosystem is anchored in the Defence Industry Strategy (DIS) and the Strategic Knowledge & Innovation Agenda (SKIA) 2016-2020 of the Ministry of Defence.

An excellent example of a PPS program within this scope was the project STARS (Sensor Technology Applied in Reconfigurable Systems). STARS was running from 2010 – 2015 in which more than 70 researchers from Thales, NXP and TNO worked together with SME's and all technical universities to build up knowledge about reconfigurable sensor suites End users of the technology were continuously involved. STARS led amongst others to more than 100 peer reviewed publications, an accepted world standard, and spill-over effects in other economic sectors like ICT and telecom.

A current H2020 project is ALFA, a project dealing with protection European borders against drug trafficking, which is currently aggravated by the increasing use of small aircraft that allows for almost undetected border crossings, especially coastal borders. Therefore, a system is needed that can add to existing surveillance means and significantly increases the detection probability, particularly for small aircraft. Moreover a prediction of the landing or dropping zone of the aircraft is also required.

3.2 Areas of Application and Technological Challenges

The effectiveness of security measures is increasingly determined by the availability and quality of information. Information dominance is widely seen as the most critical factor for successful action in the public security and military domain. The targeted introduction of innovative sensor technologies

and sensor-data, information and communication networks is crucial to optimise the information chain of observing, analysing, deciding and acting. Sensors such as radar and integrated sensor suites, and passive sensors, such as acoustic (vector) sensors and (day and night vision) cameras, are essential to this process.

3.2.1 Radar and Integrated Sensor Suites

As radar is an active sensor, it is pre-eminently suitable for the detection and classification of so-called non-cooperative objects in a large area in all weather conditions. Radar can be deployed in a wide range of applications, such as defence, coast and harbour surveillance, peace and humanitarian missions, the prediction of extreme weather and the control of traffic on land, water and in the air, and is often essential for our security and quality of life. This wide range of applications does not only generate direct economic activities but is generally one of the preconditions for the creation of a climate that stimulates the economy. Market research shows a substantial global market potential of many billions per year with an annual growth of >10%. In the Netherlands relevant economic activities are developed in which Dutch industry positions itself as a serious contender on the global market.

In the years to come the range in which radar operates is to be further enlarged. For instance, to enable the detection and classification of objects that constitute a threat from the higher layers of the atmosphere or space and objects, such as (improvised) miniature UAVs with reflecting characteristics that make them very difficult to distinguish from their natural background or from birds. New challenges must be addressed, for instance if radar is to be deployed in an operational environment with a high asymmetrical character to support flexible defence systems or where free propagation is restricted, for instance the observation of the lower airspace or deployment in urban environments. Radars will more and more be at the basis of heterogeneous (i.e., active and passive) sensor suites, among others, for multispectral observation. To respond to a continuously changing world where radars are deployed and to prevent that systems will have to be developed over and over again, research will have to be made into reconfigurable and resilient systems that enable the quick and simple change of the system's inherent functionality.

In the period ahead, developments in radar signal processing can be summarized as the step from detection to classification and identification, in which more and more information in the very signal will be used to generate an ever increasing quantity of usable and reliable radar output. In most instances, increasing use of operational and context information will be made and systems will be given a more cognitive and intelligent quality. Examples of enabling technology to attain this are: particle filtering, compressive sensing, use of micro-Doppler and coloured space. Radars will also be increasingly used in networked environments.

Developments in radar front-ends are strongly dominated by Active Electronic Scanning Antenna (AESA) that is to be deployed in a wide scope of applications during this planning period. AESA developments are strongly related to the European Key Technology and the HTSM Roadmap Electronics (Circuits & Components). This is to yield low profile / thin AESAs that can be easily integrated in a platform or an operational environment. Another path in the AESA roadmap is the reconfigurable antenna array that is to facilitate the multi-domain deployment of one and the same system.

3.2.2 Passive Sensor Technology

In the security domain, the Netherlands has distinctive global market- and technology positions in both passive sensors and passive sensor systems. CCD/CMOS daylight cameras are used for high resolution (airborne) surveillance. Night vision is enhanced by image intensifiers and/or infrared

sensors. Unlike active sensors, passive sensors do not emit energy, making them robust against electronic warfare. Their relatively low power consumption makes them stepping stones for widely distributed arrays of autonomous sensors, and candidates for unmanned platforms. Acoustic directional sensors can increase 3D situational awareness, both in air and underwater.

The ongoing growth in data gathering necessitates novel concepts for data processing that can cope with the growing volumes of data. However, innovation in this area is seriously constrained by privacy regulations and the computational workload that is needed for interpretation of data. A technical solution on the part of the sensor is to automatically process and interpret data locally, and to only report relevant data to control rooms. Sensor fusion is a powerful concept in reducing false alert rates by combining data to filter out irrelevant information. Relevant technologies are biometrics for recognition and identification, sensor fusion and signal processing, especially the currently used modalities video, person-tracking in outdoor and crowd-scenarios.

In many developments in this area, smart combinations with human observers are the key for successful innovation. For instance, Intelligent passive sensors are able to detect the simultaneously occurrence of a number of weak deviations of the “normal” situation, while surveillance operators are concentrated on strong deviations. Automated intelligent passive sensors enable the direct and reliable detection of certain types of incidents (e.g. a shot of a gun, breaking of a pane of glass, indications for behaviour related to dealing of drugs), while human observers will have difficulty with recognition of incidents they never experienced. A remarkable milestone in this field has been reached as a result of the developments in this roadmap: the early detection of pickpockets in a crowded area by automatic analysis of the observations of a CCTV-system has been demonstrated.

Some human observation competences will not likely be replaced by instrumented observations. Therefore, research into optimal human-machine interaction in sensing applications will remain important. Such research needs to be complemented with effective training programs for professionals that interact with sensor applications.

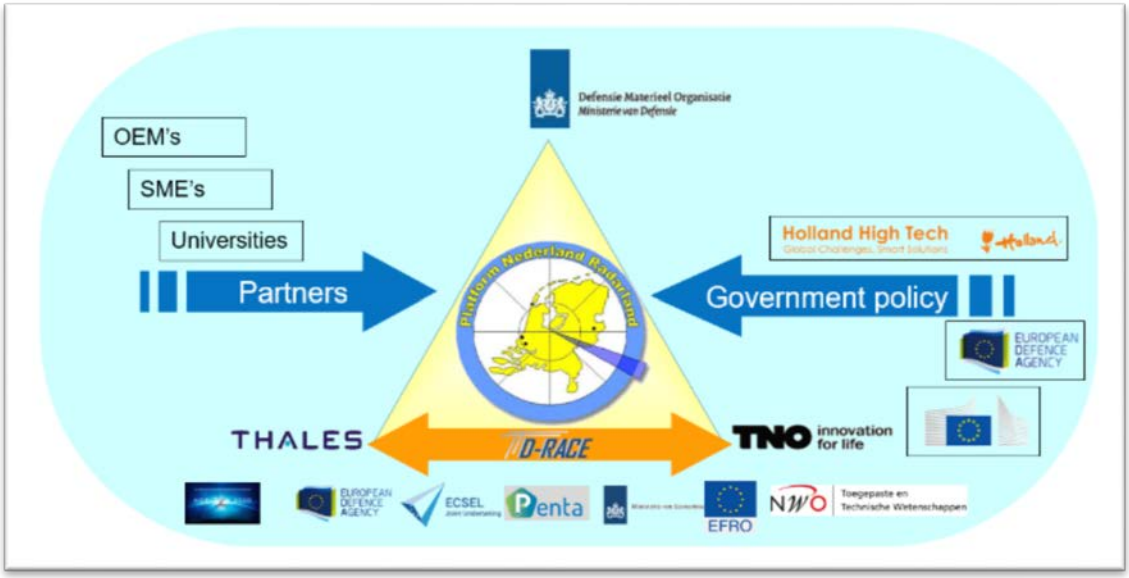
There are also promising perspectives for self-learning sensors, self-adaptation of sensors, and the application of autonomously moving clouds of passive sensors and reconfigurable sensors. The challenge of applying new generations of intelligent passive sensors is to support professionals on several tasks such as surveillance, maintenance, detection, forensics and incident handling. These tasks involve identification, observation, detection of people or other objects, behaviour and behaviour patterns that (might) lead to threats and incidents. A special challenge is to support professionals in charge of security in crowded, complex locations such as train stations, airports, celebrations, or during (inter)national events such as King’s Day.

A new development is the embedding of intelligent passive sensors in products and systems for protection of vulnerable locations. After the attacks at Charlie Hebdo in Paris the need for improvement of entrance control systems is broadly recognized. Of high priority are high risk locations of authorities and enterprises, and locations that are essential to the continuity of critical infrastructures. Such novel entrance control systems should be cost effective, and should not hinder the passage of employees and visitor. Additionally, innovations in in this area should link to other sources of intelligence such as sensor observations in and around the location. Embedding of passive sensors is also relevant to strengthening of the observation capacity in situations with a significant enhanced risk level. Personal equipment, cars and special mobile platforms as UAV’s can be provided with sensors; challenges to protect the sensing devices and also to monitor the enormous streams of images in a privacy compliant way.

3.3 Priorities and Programmes

R&D in the area of radar will focus on the implementation of the national *Roadmap Radar en Geïntegreerde Sensorsuites 2030* and in particular to the sensor suite for the next generations of frigates of the Royal Netherlands Navy. This roadmap is drafted by the Platform Nederland Radarland, an initiative founded by the Ministries of Defence and Economic Affairs and Climate, Thales Nederland, TU Delft and TNO. The three main innovation themes that are defined in this roadmap are: new concepts of radar and integrated sensor suites, sensor technology (in particular RF front-end technology, algorithms and processing) and life-cycle cost management. In the 2018 – 2023 timeframe, research in this roadmap will be characterized by necessary, perhaps even disruptive, fundamental and low TRL research that is necessary to obtain the required results in 2030. This work will be complemented by remaining work from the preceding, current roadmap that runs until 2020.

Cooperation is carried out in an ecosystem around Platform Nederland Radarland that consists of



various programmes and partners as indicated in the figure below.

The roadmap focuses in particular on the development of knowledge and technology, which is relevant for the maritime domain. However, possible applications and spin-offs outside the maritime domain and in other economic sectors will also be examined.

The activities are fully aligned with the Strategic Research agendas of the European Defence Agency (EDA). In particular in the fields of radar (EDA CapTech Radio-Frequency Sensors Technologies), miniaturized electronics (EDA CapTech Components), Electro-optical systems (EDA CapTech Electro-Optical Sensors Technologies) and command and control systems (EDA Captech Communication Information Systems & Networks). Alignment will be sought with the priorities of the future European Defence Fund in the 9th Framework Program of the EC that is foreseen for the period 2021-2027.

4 Mission Critical Systems

4.1 Context

Innovation of high-tech systems is of crucial importance to industry. In the first place because it leads to bigger opportunities in wealthy countries, and second because it allows companies to penetrate markets in developing countries easier and faster. European companies and research institutes are known for their technology excellence, each in its own specific market segments. Furthermore, a balanced economic strategy by the European Commission motivates cooperation between specialist companies which promotes European independence on a global scale.

However, there is also a consequence to growth of economic and social welfare: it needs to be protected. Being a global market player requires international stability and the guarantee of safe global trade routes against adversaries abroad. It also requires a well-organised network of people and infrastructure in the home countries that prevent adversaries like criminals or terrorist to disrupt society.

Operational security refers to the capability of security and defence coalition forces and their systems to adapt to varying circumstances during mission preparation and mission execution. With Mission Critical Systems (MCS), adaptivity by design is accomplished by the partners working together on an open IT architecture to exchange information between otherwise vendor-locked combat, platform, and other functions. Not only does this allow optimization of effectiveness and crew size, it also supports economy of scale, reduction of lifecycle cost, and an increase in innovation pace.

Digital security is essential to safeguard the sensitive information in defence and security IT systems against sabotage by third parties. Data security in onboard systems has to be guaranteed, especially during transfer between systems and during exchange between ships and shore. In MCS, the partners work on IT security solutions including multi-level security protocols, encryption, and detection of network anomalies resulting from third party activity. In this effort, adaptivity by design and security by design go hand-in-hand to establish comprehensive digital security.

Defence and national security personnel and their systems have to be protected against the effects of hostile actions through extensive physical security measures. In MCS, a fair amount of work is spent on autonomous situational awareness and decision making. This allows for a fast and accurate recognised picture of what is happening on and around the ship as well as an inventory and selection of adequate actions. As such, MCS integrates situational awareness and decision making for e.g. platform damage repair with the compilation of the recognized battlefield picture to support optimization of systems and crew.

4.2 Areas of application and technological challenges

With MCS, there are three areas of applications: naval combat and platform management systems, land-based vehicle platforms, and protection of IT infrastructure.

4.2.1 Naval systems

The Royal Netherlands Navy (RNLN) delivers an important contribution to the protection of economic and social welfare of the Netherlands and its allies, home as well as abroad. To support the RNLN in this task, the partners Thales, RHMarine, and TNO have initiated the Mission Critical Systems (MCS) collaboration, with support of the Defence Materiel Organisation (DMO) of the Netherlands Ministry of Defence (MoD). The overall aim of MCS is to replace the stove-piped IT

architectures onboard of the Dutch navy ships by an open IT architecture that integrates combat and platform management systems. As a result, resources for combat functions, computations, electrical power and ship propulsion, can be managed as to optimize operational effectiveness and crew size.

Thales, RHMarine, TNO and DMO have defined their research activities for the period 2015-2020 in the MCS roadmap, which one-to-one relates to the Manning & Automation roadmap in the '*Kennis Plan Zee*' of the MoD. In this roadmap, much attention is given to the operational, digital, and physical security aspects of the societal challenges from the perspective of both security and defence.

With MCS, **naval systems focus** on combat management systems, platform management systems, and integrated mission management. *Combat Management Systems (CMS)* provide situational awareness onboard or around the ship by fusing sensor information with other information types such as own ship data (OSD), nautical charts, battle damage information, or information from shore e.g. from the MarSitCen. Furthermore, mission planning and analysis are done in the CMS during mission preparation by calculating system parameters for e.g. signature management, sensor management, and communication management. Engagement planning of the sensor and weapon systems and the organic assets is also done in the CMS. *Platform Management Systems (PMS)* include the following functions. Navigation management to combine information from nautical charts with the OSD to calculate the manoeuvre space for autonomous navigation which contains the safety limits for e.g. rudder, speed and course. Energy management which is a necessity if the design of a maritime power generation system allows for more than one way to generate, distribute and/or consume energy, choices have to be managed continuously. Onboard maintenance in case the reduction in crew size and very limited time for education hamper efficient maintenance of complex onboard systems by the crew. In such cases, monitoring and analysis of system parameters against baseline performances allows to advice crew members on when and how to replace system components. *Integrated Mission Management System (IMMS)* in which the following integration functions are included. Integration of combat management and platform management functions. To optimize resources over the entire ship, a hierarchical management structure is developed for integrated management of sensor, signature, energy, engagement, and navigation functions. Integration of unmanned systems to ensure effective integration of air, surface and subsurface unmanned systems with the CMS without an increase in crew size. This means that UXVs have to collaborate autonomously across these three domains. It also means that the CMS has to develop new functions for UXV control and for UXV mission planning and analysis.

Successful implementation of the above-mentioned CMS, PMS and IMMS systems onboard Dutch navy ships relies on solving the following **technological challenges**. First of all *General Artificial Intelligence (AGI)* has to be created. Over the past decades, Artificial Intelligence (AI) has made much progress. However, progression is limited to the AI components of reasoning, learning, optimization, and knowledge representations. These components are referred to as narrow AI whereas in the near future, a CMS, PMS and especially an IMMS requires a form of intelligence that integrates these components into one mathematically grounded framework called AGI. Second, there is the challenge of *Generic and scalable software algorithms*. To effectively develop CMS, PMS and IMMS functions, as many system specific functions as possible have to be removed. Hence, generic and scalable software will be developed based on the grounded mathematical framework of AGI. Finally, there is the *Integration of AGI with Systems Engineering and Software Architecting*. Up to now, autonomous systems are developed by specifying in design time the options that the system has in runtime. By logging the system performance and analysing these loggings, the system learns about

its behaviour. This experience can then be included in the design process allowing for more effective design choices.

4.2.2 Land-based vehicle platforms

In the previous years and certainly for the coming 5-10 years the role of Land Vehicle platforms are becoming a critical asset for enabling (horizontally and vertically integrated) C4ISR in the mobile domain during (coalition) operations in all force projection categories starting from peace keeping to higher levels.

While the current technology focus is on extending C2 (including COP) and platform centric C2ISR optimization, the **future focus with land-vehicle platforms** now is to create platform and network technology to grow *from C2 to (networked) C4ISR to ultimately C8ISR* capability (Communication, Command, Control, Computer & Collaborative engagement, and Cyber).

Where current capability/technology has greatly enhanced the survivability and deployment/operations efficiency, new threats and/or new requirements are unanswered. Cybersecurity and system wide infosec requirements and the need for open architectures enabling mission flexibility and adaptability are mandating a new (information and communication) integrated Land platform capability.

The Royal Netherlands Army (RNLA) is already addressing relevant capabilities in programs like DCMO, CV90 and standardization initiatives like ESSOR and NGVA and using research platforms/consortia like EDA where TNO and Thales are strong NL partners and representatives.

The main focus for research in this area is on the following three **technological challenges**. First there is *Collaborative engagement/operation* which includes: Inter platform sensor/actuators information sharing, National and coalition interoperability (network & air interface), Security (information and communication), and (wireless) Network performance and management. The second challenge is *Open platform architecture*, mainly addressing the issue of Scalability, adaptability, configurability, maintainability, and that of Security (cyber, infosec, separation/MLS). The last challenge is that of *Optimized operations* to support Situational awareness and decision making which deals with New HMI Concepts to integrate all (role, mission, situational) information to present and control for vehicle crew. It also deals with Separation of communication and information within platforms.

4.2.3 Protection of IT infrastructure

The physical and information security of national (defence) assets is vital to protect the integrity and availability of the (governmental) capability to create effect from military deployment in on homeland or abroad. The electronic security concept forms together with structural and operational means the capability to provide a 100% protection.

The **focus of Protection of IT infrastructure** is on the challenge to *provide electronic means to maintain the infrastructure integrity*, i.e. to maintain access control, intrusion detection, command & control, communication and relevant aspects of authentication, availability and confidentiality to protect the system against unauthorized use, loss of (or comprised) C2 and loss (or compromised) information via classical and/or cyber attack means.

For research in this area, the following **technological challenges** are identified. First there is *Cyber hardened availability for critical capabilities*. This includes Network and datacentre (application) high availability (IT) architectures and mechanisms robust against partial disruption or degraded performance. It also includes Distributed early warning Cyber-attack detection and/or counter

measure functionality and mechanisms. Second, there is *Next generation authentication technologies* which contains Architectures with new technologies for (multi-factor) authentication means for humans, devices, applications and/or services. It also contains Technologies for ad-hoc authentication without pre-sharing/configuring the information systems. Third, there is the *Next generation intrusion and access control technologies*. This includes Architectures with new intrusion detection technologies to improve the false hits. It also includes Architectures with new (non-intrusive) access control technologies and/or automated real time multi source verification mechanisms to prevent unauthorised access. Finally it includes HMI concepts enabling optimized AI supported centralized operation and maintenance operating centres with minimalized operator manning.

4.3 Priorities and Programmes

For **naval systems** within the timeframe 2015-2020, the MCS roadmap of Thales, RHMarine, TNO, and DMO contains the following programmes. Each programme contains a number of projects which are logically prioritized over 2015-2020:

- Optimal open IT architecture
- Integration of internal and external battles
- Integrated communications
- Remote services
- Mission adaptivity
- Autonomous functions
- Man-machine teaming

Moreover, where possible, each of the above programmes draws funding from the EU, EDA, and PADR Research Programmes. Hence, the MCS roadmap is strongly embedded in HTSM as well as in the European Research Programmes and so supports the MoD with funding as well as with international knowledge. Examples of projects that the MCS partners have won include MARISA and OCEAN2020 with a total worth of about 4 million Euro.

For **land-based vehicle platforms, c**urrent priorities, topics and initiatives are:

- Intra-Platform and inter-platform architecture framework for applications and services.
- Using new communication radio technologies (SDR, LTE, sub..) integrated in the (secure) communication architecture
- New HMI concepts to optimize situational awareness and decision making
- Cybersecurity hardening
- Comprehensive mission configuration for and in mobile domain.
- Information security/separation in mobile (platform) domain
- infosec/cyber and C8I architectural concepts for unmanned/autonomous platforms land platforms

Moreover, where possible, each of the above programmes draws funding from the EU, EDA, and PADR Research Programmes. Hence, the roadmap is strongly embedded in the European Research Programmes and so supports the MoD with funding as well as with international knowledge. Examples of projects that Thales with international partners have won include MIDNET, IN4STARS, ESSOR/OCCAR and LAVOSAR.

For **protection of IT infrastructure**, current priorities, topics and initiatives are:

- Cyber hardening of critical infrastructure security and information systems.
- Human factor centric research on AI and optimizing on cognitive human capabilities
- Machine learning, big data techniques, data analytics and automation on (predictive) availability for critical electronic system assets & applications (IT environment)

5 Partners and process

The table below presents an overview of the ecosystem including partners from academia, institutes, foundations, international cooperation, SME's end users. It includes also the European programmes in which we seek cooperation with other European universities, SME's and OEM's.

Academia	e.g. TU Delft, TU Eindhoven, RU Nijmegen, VU, UVA, Universiteit van Leiden,
Institutes	e.g. TNO
Security Industry	e.g. Thales _Nederland BV, RHMarine, Microflown, Adimec, CGI, Compumatica, eCleqtiq, RISCURE, IBM
Government	e.g. Ministry of Defense, Ministry of Justice and Security, Royal Netherlands Navy, Platform Nederland Radarland, National Police, Coast Guard, MoD – DMO, critical infrastructure providers
Industry	e.g. Prorail, Alliander, Schiphol, Havenbedrijf Rotterdam Smart Industry
International Programmes	e.g. European Defence Agency (EDA), EU Research and Innovation Framework (H2020, Horizon Europe), ECSEL, PENTA, NATO STO

Additional partnerships and relationships:

- The Roadmap Security is strongly linked to the HTSM R&D Roadmap Electronics, Roadmap ICT and the Roadmap ESI. Furthermore, there are links with other topsector roadmaps, ranging from energy to agriculture and health.
- Road-mapping in the field of Radar Technology development is coordinated within the *Platform Nederland Radarland*. The results are disseminated every 2-years at a dedicated national event.
- Mission Critical Systems are coordinated in The Steering Committee of the Platform Mission Critical Systems
- To leverage with European agenda's, this Roadmap is closely linked with the Strategic Research Agendas of the European Defence Agency, The H2020 Program Secure Societies and the priorities of the Joint Undertaking ECSEL and the EUREKA clusters PENTA and CATRENE.

6 Investments

R&D in public-private partnership, including contract research; all figures in million-euro cash flow per year (cash plus in-kind contribution)

Roadmap	**2015**	**2016**	**2017**	**2018**	**2019**
Industry	20	20,5	21	21,5	22
TNO	3,2	3,2	3,2	3,2	3,2
NLR					
NWO	6	6	6	6	6
Universities	4	4	4	4	4
Departments and regions (excluding TKI)	16	18	19,5	21	22
Grand total	**49,2**	**51,7**	**53,7**	**55,7**	**57,2**

European programs within roadmap	**2015**	**2016**	**2017**	**2018**	**2019**
Industry	1,5	1,5	1,6	1,7	1,8
TNO	1,4	1,3	1,5	1,5	1,5
NLR					
NWO	1	1	1	1,2	1,4
Universities	1	1	1	1	1
EZ co-financing of European programs					
European Commission co-financing	3,2	3	3,4	3,8	4,2