ROADMAP SECURITY 2

Top Sector HTSM

Version 17 juni 2022

Contents

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, monitoring the functioning of the democratic legal order, and ensuring a level playing field. In situations where there is no longer a level playing field, caused by the actions of state actors, a role for the government is conceivable.

The impact of the *HTSM Security Roadmap* 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 consistency in joint roadmaps, creating unique products and an open exchange of knowledge and by increasing the scale.

The National key products and technologies in the Dutch security 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 national key technologies and 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 faces fundamental changes due to technological advances, geopolitical shifts and environmental developments. Due to the deep interweaving of IT in our way of life, we see that digital attacks and disinformation campaigns by state actors and criminal organizations can cause deep disruptions in our lives. We are not only confronted with technical disruptions but also see that interference by third parties via digital platforms can lead to an increasing discord in society

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 focused 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 Security Roadmap* 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

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 RH Marine exploits these opportunities through a “triple helix construction” which supports the innovation of industrial products with national and European long-term research programs. 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, RH Marine is an expert in automating and integrating systems for propulsion, power generation, navigation and electrical installations. Besides serving the Dutch navy, RH Marine 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** ‘ as addressed within the **KIA Veiligheid**. 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.

1.5 Fostering a forward looking approach in security[1]

Aligning research and innovation activities with NL security policy priorities is crucial but not sufficient to guarantee that security practitioners will benefit from newly developed solutions. To guarantee uptake of security innovations we need a hands-on forward looking approach for capability development. This capability-driven approach safeguards a far more efficient and effective response to (new) incidents than resulting from a reactive approach of just using and adapting existing technologies and capabilities. Research and innovation is a key element in this approach, as it enables forward looking development of innovative security solutions that sustain future capabilities. As Figure 1 shows, it should thus: (1) identify future needs of end users in the priority areas (see Chapter 2, 3 and 4) as these are the ones who determine the operational effect that needs to be reached in face of future threat’s, (2) develop and assess

[1] Enhancing security through Research and Innovation: https://ec.europa.eu/home-affairs/system/files/2021-12/SWD-2021-422_en.PDF.

options for innovative solutions that require the capabilities required by end users, and (3) produce the interface with (financial) instruments that will make it possible to implement the solutions.

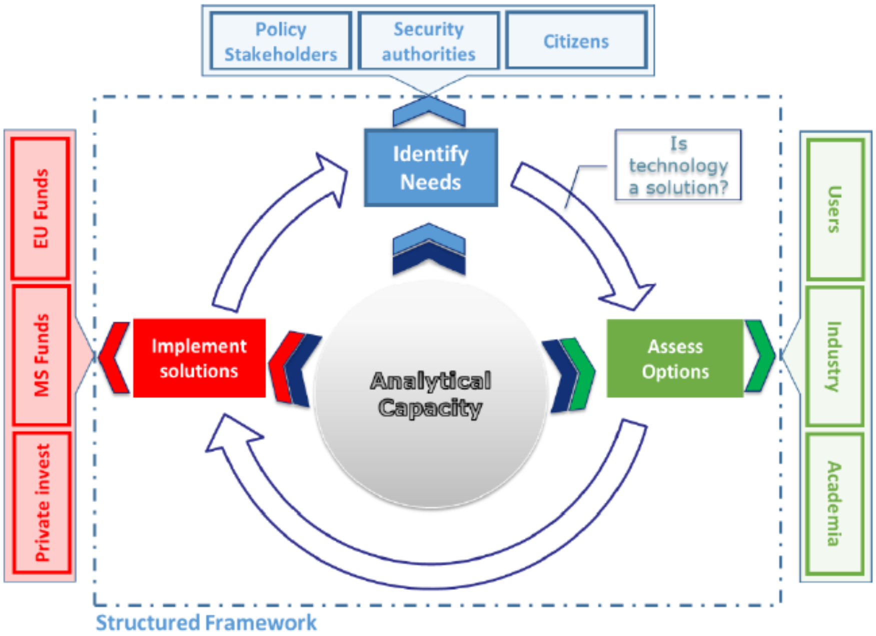


Figure 1. Parameters to identify needs, assess options, and implement solutions (source: services of the European Commission)

2 Cybersecurity

2.1 Context

The world is rapidly digitalising. 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, businesses and also societal transitions are built.

The impact of digitalisation is usually perceived through the benefits it brings. Digitalisation 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, this also yields new cybersecurity challenges. Cyberspace provides new opportunities for malicious actors to destabilize organisations and society as a whole and take advantages of vulnerabilities for criminal gain (e.g. ransomware) or state interests. As our hyperconnected society will become wholly dependent on digital systems and services, our traditional views on cybersecurity will need to be updated. Especially because nowadays disruption in the digital domain can cause effects in other domains like the physical or economical domain.

Besides these cybersecurity developments there has also been a slow shift of ICT- industries through the past decades, the manufacturing industry of ICT products has been concentrated in Asia and the cloud and data industry has been concentrated in America. This brings the question to the Netherlands and also to Europe what the impact is of these dependencies.

Therefore, an updated arsenal of instruments and practices for a responsible way of digitalising is necessary in the Netherlands . We will need to develop a new understanding of digital security and build appropriate capacities to safeguard the wellbeing of society, business and individuals.

Three main motives drive R&D on cybersecurity in the Netherlands (and the EU in a wider perspective): 1. strategic autonomy, 2. secure digital society / businesses / individuals and 3. economical growth. All are important, but depending on the specific cybersecurity topic their mutual weights will differ. The same is true for actors in the cybersecurity domain.

Strategic autonomy: there is no specific list yet of cybersecurity topics for which the Netherlands pursues autonomy, though cryptology and offensive cyber capabilities for law enforcement, intelligence and Defence are in scope of this document. In any case a minimum level of autonomy requires that Dutch public institutions and industries can make an informed choice for security technologies (smart buyers).

Digital security has an international, national, organizational and individual perspective. Internationally this is for instance about cyber capacity building in bilateral or EU constellations. On a national level security concerns amongst others the protection of critical information infrastructure (CIIP), information sharing (cyber intelligence), fighting cybercrime, cybersecurity of weapon systems and of classified networks. Key stakeholders are the ministries of Foreign Affairs (BZ), Justice & Security (J&V), Defence and Home Affairs (BZK). The KIA Security is a guiding instrument here.

For organisations (businesses), all nine ‘top-sectors’ are susceptible to cybersecurity challenges (e.g. protection of intellectual property, personal data and business continuity) and require ample cybersecurity capabilities 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 cybersecurity section of the HTSM security roadmap is closely connected to the **HTSM Roadmap ICT**, in which cybersecurity is also mentioned as an essential capacity for businesses, government agencies and other organisations to thrive. In addition, cybersecurity challenges create new business opportunities for novel cybersecurity products and services. Other KIA's, like Energy Transition, are also relevant guiding instruments.

The overall 'Topsectorenbeleid' of the Ministry of Economic Affairs and Climate Policy is focused on creating the conditions in which businesses can thrive and grow. **Earning capacity** is a leading motive. Cybersecurity is still been seen as a cost item instead of an opportunity to create improved earning capacity, although it is a precondition for transitions and growth in other sectors, it saves costs (direct costs and withdraw of knowledge) and minimalize risks. In addition, specifically for the roadmap Security of HTSM, strategic autonomy and safety motives are relevant too. For this reason the ministries of Justice and Safety and Defence participate in the core team of this roadmap.

In all, the growing challenge to cope with cybersecurity requires well-coordinated cybersecurity research, development and innovation initiatives across sectors and (inter)national governmental institutes. Given the wide range of possible topics and the limited capacity of the Dutch cybersecurity community, (widely supported) priorities are important.

2.2 Areas of application and technological challenges

Cybersecurity encompasses several key capacities: the ability to design secure systems, withstand attacks (and to execute them in a legal and ethical responsible fashion), combat cybercrime, fake news, safeguard privacy and identity, govern effectively and the ability to provide society with cyber defence capabilities. It also includes the capacity to maintain and adapt systems during their operational life-cycle. These capacities should be developed and provided to businesses as well as government Aim is that they can acquire the (NL build) tools and knowledge needed to enhance cyber resilience and thereby contribute to the cybersecurity of the Netherlands, whilst also supporting NL earning capacity and strategic autonomy.

Each of these capacities mentioned above requires smart technological innovation and active participation in public private partnerships to collaboratively work towards implementation. Important to realize that the challenges are not only technical. With increasing digitalisation in society, the number of non-technical challenges of legal, economic, social and human nature are also rapidly increasing.

Challenges in cybersecurity are therefore multidisciplinary by nature and the required research and development should therefore be as well. A guiding document for multi TRL research in the Netherlands in this area is the National Cyber Security Research Agenda version 3 (NCSRA III)[2], published in 2018 by the former dcypher and written by a broad team of authors with input from several field consultations.

At the cross section of the NCSRA III and the Knowledge and Innovation Agenda's, that were created in the context of the in 2019 launched mission oriented innovation policy, the most relevant research topics for cybersecurity in the Netherlands emerge. Other relevant national and international policy documents and agendas act as input for the agenda's above.

[2] NCSRA III | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl)

As a result the following list of cybersecurity research subjects has been identified, addressing areas of application and technological challenges in cybersecurity, arranged along the NCSRA III structure, that consists of five pillars. For a more extensive list we refer to the NCSRA III. 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. The topics marked in italics have been added in this update.

In more detail, grouped by NCSRA III pillar:

- **Design**
  - **Horizon scanning and predictive analysis of innovations.** As the cybersecurity landscape evolves, 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.
  - **Cybersecurity and resilience concepts**. Our hyperconnected society has become very dependent on critical (information) infrastructures (OT, IoT and IT[3]), 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.
  - **Security by design/Life-cycle security.** 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.
  - **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.
  - **Supply chain security.** Understanding and mitigating risks in the supply chain of the producing industry (manufacturing, energy etc..) has become much more important, next to that of critical infrastructure and defence and security agencies, as much of the components used in the supply may contain cyber vulnerabilities. The mixture of IT/OT/IoT systems in the supply chain further complicates this.

- **Defence**
  - **Cybersecurity Monitoring & Detection (by Design).** 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 advanced analytics provide powerful opportunities to understand network traffic and threat actor behaviour and support a timely response in order to limit or even prevent damage.
  - **Security automation.** As far as it is not covered above, automation and AI technology offer many opportunities to tackle one of the key issues in cybersecurity: the shortage of

[3] Operational Technology, Internet of Things and Information Technology

skilled experts, in combination with the vast amount of data to be processed in very short times.

- **Attacks**
  - **Automated Vulnerability Research.** Discovering and patching vulnerabilities as soon as possible in the lifecycle of software is an efficient way to prevent future cyber attacks. As soon as possible means: during the software development phase, but could also be a periodic preventive measure during the deployment phase.
  - **Quantum secure technologies incl. post quantum crypto.** As current cryptographic solutions will be impacted by quantum computing in the near future. The NIST competition should lead to new quantum safe algorithms in 2023, but that still requires solutions for migrating towards quantum safe crypto implementations. Besides new “classical” algorithms, also quantum key distribution could be considered here.
  - **Offensive cyber capacities** To effectively combat cybercrime and to exercise lawful authorizations, verifiable trustworthy and secure products must be developed. Examples are protection against and detection of CIO-fraud with highly sophisticated spoofing and deep-fake technologies, money laundering with complex international transactions with crypto-currencies mixtures and digital economic espionage.

- **Governance**
  - **Governance, data privacy and ethics.** The digital society poses significant challenges to current approaches to governance, privacy and ethics and duty of care These aspects need to co-develop with technological innovations and be an integral part of RD&I in the cybersecurity sector.
  - **Cybersecurity testing and certification (assurance).** 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 also after updates. Especially end-to-end cybersecurity, for instance in IoT applications or automotive/mobility, still needs development. This also requires the build up of national security testing infrastructures to bring the worlds of security systems development and operations closer to the modern hacking perspective
  - **Cyber workforce development.** Attaining and maintaining sufficient levels of cybersecurity requires the build-up of a wide class of capacities, ranging from technological development to strategic planning. This build-up demands a suitable workforce, and necessitates the development of educational courses, practical training, pooling & sharing concepts, and a good understanding of the man-machine teaming
  - **Cyber dependencies and cascade-effects.** Insights in the dependencies of cyber with the physical (and other) domain(s) for an effectively security approach by incidents, attacks and disasters.

- **Data protection**

- ***Privacy protection.*** Cooperation and protection of interests such as privacy are often in conflict. To protect the privacy and also stimulate further (digital) cooperation new and future proof technologies and procedures need to be developed and implemented such as *Privacy by design, Privacy enhancing technologies, Privacy friendly identity management and Algorithmic accountability and transparency.*
- ***Crypto and quantum.*** With the wider access to digital data protection of sensitive data is necessary. High assurance crypto- and quantum safe products are therefore necessary.
- ***Information security.*** With the increasing self-regulated systems and autonomous devices protection of information security is growing in importance. This requires development of future proof products to protection the information security of sensors such as time and location in road systems and as well the protection to correct interpreted signs by sensors.

Jointly, these areas of application and technological challenges are meant to form a first basis upon which the partners in the HTSM Security 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)[4], as published by the Ministry of Justice and Security in May 2018, and the 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. Furthermore, research will be aligned with the priorities set forward by dcypher 2.0 (the Dutch public-private agenda setting, programming and valorisation platform for cybersecurity research and higher education).

This section of the HTSM Security roadmap will be implemented in close cooperation with key stakeholders from research, government and industry, both cybersecurity suppliers as well as end users. Academic cybersecurity scientists are organized in the Academic Cyber Security Society (ACCSS). Relevant government stakeholders that should be mentioned are the Netherlands Cyber Security Centre (NCSC), the ministries of Defence, Justice & Security and Economic Affairs and Climate and the National Cyber Competence Centre (in formation). Finally there is cooperation with regional cybersecurity communities, such as The (Hague) Security Delta, Het Twentse samenwerkingsverband TUCCR and Cybersecurity Noord.

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 Research and Technology Organisations (RTO's) are very active in the EU Research and Innovation Framework programmes (such as the Horizon Europe, European Defence Fund and Digital Europe programmes) and will link the innovations from this roadmap into forthcoming research proposals.

Furthermore, the work in this roadmap will be synchronised to EU cybersecurity policy directives where possible, and in cooperation with other research organisations and stakeholder networks, such as the European Cybersecurity Competence Centre and ENISA.

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 future-proof, adaptive armed forces. The Defensievisie 2035 states: “*Technologische trends, geopolitieke machtsverschuivingen, economische, demografisch-maatschappelijke en ecologische ontwikkelingen zorgen voor nieuwe kansen, risico’s en dreigingen. Rusland is agressiever, China assertiever en de terroristische dreiging blijft bestaan. Partnerschappen zoals de NATO, de EU en de VN, waar onze vrede en welvaart op zijn gestoeld, zijn geen vanzelfsprekendheid meer. We hebben te maken met grootschalige cyberaanvallen, dreigingen tegen onze vitale infrastructuur en beïnvloeding door buitenlandse mogendheden*". In practice this means that threats develop rapidly and continuously and the nature of threat scenarios will become highly complex. Specifically, this includes the threat of hypersonic weapons from Russia and China, ballistic threats from Russia and Iran, but also low-tech threats, the use of air weapons and swarms of drones for which the necessary technology is easily accessible, also for terrorist groups. In addition, Europe is on a course to become technologically independent from Asia and the United States. New sensor and radar technology is necessary to cope with these (future) threats in an operational environment that is increasingly challenging, where the EM spectrum is congested and contested and stealth technology as well as advanced countermeasure continue to develop very fast.

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. 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. New concepts of radar operation are required to grow with future needs and threats and are made possible by new waveforms and algorithms, advanced filter structures and antennas, custom RF, mixed-signal, digital assisted RF and digital electronics. RF electronics (a.o. dedicated GaN and SiGe designs) where needed and embracing state-of-the-art COTS technologies when possible, combined with new algorithms and processing techniques. These enabling RF 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.

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 *Defence Strategic Knowledge and Innovation Agenda 2021-2025* 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.

Under the umbrella of the NATO Science and Technology Organisation, long-term research is performed into radar classification of air targets. This research is carried out in an international context with European and U.S. research institutes and industries. In the last years, the focus is on classification and intent assessment of slow and low flying drones. Although small, these drones pose a threat since they may act as a covert forward observer or they may deliver (improvised) explosive devices. Robust detection, tracking and classification of such drones, against a complex background, is crucial for the deployment of appropriate countermeasures.

A recent 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.

An example of a small but focused ecosystem is the co-operation for fuze research by TNO, semiconductor manufacturer and Rheinmetall that has led to an integrated radar sensor in cubic cm volume for future ammunition in airborne platforms.

Furthermore quantum technology has the potential to be a disruptive technology for a wide range of application domains, including defence, security, pharmaceutics, medical, finance, energy/oil&gas. At the core of this "second quantum revolution" is information: its acquisition (quantum sensors, quantum imaging), its transmission (quantum communications) or its processing (quantum computation). Sooner than quantum computing, quantum sensors are expected to offer advantages. Thanks to quantum physics, new sensors are tested in laboratories with precision not achievable before or even new capabilities, like precision navigating under GNSS-denied conditions (including under water and underground). Also very precise timing and detection of underground cavities will be possible

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, space situational awareness, 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.

Future radar and sensor suites will have to operate in an increasingly challenging operational environment where the EM spectrum is crowded and electronic warfare is an advanced threat in itself. On top of this, the (simultaneous) threats that the same sensor has to deal with will vary largely, even within the same mission, ranging from the high end of the spectrum (hypersonic and BM) to small, and slow UAVs. Radars will have to be build and deployed with the consciousness that they are no longer stand-alone sensors, but part of a system whose ultimate goal is to provide high quality information at the right time to the right person.” The same radar hardware needs to be able to deliver a wide range of capabilities, resulting in the need for ad-hoc functional updates and upgrades that might vary from mission to mission, or in other words: “designed for change”. In this context, a software driven and based system can deliver always the right functionalities for different missions even if the sensor hardware is unchanged.

In the period ahead, radars will have to deliver high quality information instead of data. The type and quality of the information needed will depend on the specific mission and operational environment. To this end, functionalities will have to be updated from mission to mission in a dynamic way by means of software upgrades. Next to that, the radar must be aware of its operational environment, and exploit existing information to improve its own information stream. Cognitive sensors will be able to identify the most appropriate waveforms and processing algorithms, and to adjust those adaptively to deliver information of a given quality, regardless of the changes in the surrounding environment. Novel waveforms and advanced algorithms for target detection, tracking and classification will be required to deliver radar information that contributes to achieving the ultimate system goal enabled by new concepts of active antenna systems beyond AESA. Radars will also be increasingly used in networked environments and as part of a distributed network of sensors. Within this network, each sensor has to optimize its own performance in relation to other sensors in the network, and no longer as stand-alone. Eventually, in a system centric approach, the system as a whole has to deliver the correct information, and the individual sensors have to contribute to it in relation to one another. Advanced methods for signal transmission and reception will be necessary to optimize the information quality of a sensor that needs to be aware of its environment and able to respond to it by reconfiguring itself adaptively.

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.

Intelligent passive sensors require increased processing power, which can lead to undesired heat dissipation. Novel concepts like "green ICT" can cope with this drawback by working on architectures beyond the traditional Von Neumann.

Green ICT is achieved by developing novel hardware platforms for unconventional computing paradigms beyond that von Neumann paradigm and by exploiting, next to electrical charges, also photons and spins for energy-efficient data processing. Developing new algorithms fitting this energy-efficient data processing is mandatory.

Achieving Green ICT may take 5-10 years before becoming fully operational. Until then smarter architectures can help reducing the amount of data to be processed in the sensor itself. Wide Area Motion Imagery (WAMI) System contains technology using passive sensor containing multiple sensors, each with more than 50 MPixels. Typical WAMI sensor produces imagery with a frame rate of 2-7 frames/second with a total image size between 120 MPixel and 400 MPixel. Until now , using local (in-situ) and distributed (ground station) processing is mandatory.

Due to the growing amount of deployed passive sensors, a growing demand has arisen to let passive sensor provide information (actionable intelligence) instead of signals or images. Prediction of certain behaviour, e.g. intent) is a valuable future outcome of near-future R&D efforts.

For getting such new R&D results valorised, close cooperation between TO2 institutes, universities and companies is mandatory.

Companies in the Netherlands, like Adimec, Photonis, Nedinsco and Grass Valley NL are already active in the above areas and TNO has cooperated with Adimec, Grass Valley in different project , in which the base for getting information from a sensor had been established. Those companies are eager in seeking cooperation on being the first to show their (now future) developments during trade shows. In 2021, Photonis started a heterogeneous sensor project for the NL-MoD with a consortium consisting of TNO, Microflown Avisa, Demcon and TNO. This project focuses on the creation of a distributed passive sensor suite, with 'ears and eyes' packaged in modular payload ('shoebox') to manned and unmanned systems, and supporting autonomous navigation of (unmanned) systems in demanding (combat) situations.

3.2.3 Quantum Sensing

The second quantum revolution also impacts sensing technology. The possession and deployment of quantum technologies will be a game changer in many application domains, which means that maturing and mastering these technologies is a geopolitical must (strategic autonomy) in terms of industry competitiveness and/or (military) mission superiority.

The *Defence Strategic Knowledge and Innovation Agenda 2021-2025* identifies quantum technology as the most disruptive technology in the long run. This mirrors the conclusion of the *NATO Science & Technology SET (Sensors & Electronics Technology) Panel*: quantum technology is one of eight for defence and security very relevant emerging and disruptive technologies. Within quantum technology four focus areas have been identified: communication, information science (quantum computing), precision navigation and sensors. The latter two are quantum sensing.

Value chain and competitive landscape

The quantum sensing value chain in general is composed of research (universities, RTO's), suppliers of quantum sensing components, suppliers of 'classic' sensing technology, suppliers of larger systems (like weapon platforms, medical systems or cars, the OEM's) and end-users.

Although the US and China are heavily investing too, **Europe** has a competitive knowledge base on quantum sensing, with many (polytech) universities and RTO's active in this field. Some of the most innovative companies also derive from the EU, like Muquans (now iXblue, FR), Robert Bosch (DE), Skye Instruments (UK) and Campbell Scientific (UK). The market is fragmented in nature due to the increasing penetration of start-ups engaging in the manufacturing of the sensors. Multiple market reports predict that Europe will dominate this market, though analyses differ on key driver market segments (Defence? Automotive?).[5]

In the **Netherlands** UvA, TUDelft, TNO and several SME's (like Lionix International and QUIX Quantum) work on quantum sensing knowledge and components. Quantum Delta NL aims to foster this nascent ecosystem in the Netherlands within CAT-3 Quantum Sensing, with amongst others four concrete quantum sensing testbeds (run by UvA, TUD and TNO).

Quantum sensing technology comes in many forms

In essence, a quantum sensor is a quantum device that (very precisely) responds to stimuli. For a sensor to be considered a quantum sensor it has to be able to either **measure a physical quantity** using quantum coherence OR **use entanglement** to improve traditional measurements taken with classical sensors.[6]

Scientists dealing with quantum sensors generally apply four criteria to classify whether or not a quantum sensor works: 1. the system being used has to be able to resolve energy levels; 2. a sensor has to be initialized and be able to provide a measurable answer; 3. a user must be able to manipulate the sensor; 4. the sensor must be able to interact with a physical quality and be able to respond to that quality.

While the sensing methods of the first quantum revolution (20th century) were applicable for technologies such as magnetic resonance imaging (MRI), nuclear magnetic resonance spectroscopy, and for the development of transistors, LEDs, solar panels, and lasers, the second quantum revolution builds on the control and detection of individual quantum states in microscopic systems.

Such emerging techniques in quantum sensing are expected to lead to the improvement of multiple sensing technologies, ranging from accurate atomic clocks, sensitive quantum gravitometers, and low-noise quantum interference microscopy. But also sensitive magnetic, rotation, temperature and imaging sensors. Some technologies are already quite mature (like gravimeters), others still are at low TRL's.

[5] Like Data Intelo 2019, Mordor Intelligence 2021, Precision Reports 2021.

[6] Allen, J., An Introduction to Quantum Sensors, 2019, https://www.azoquantum.com/Article.aspx?ArticleID=165

Quantum sensors can be applied in various sectors

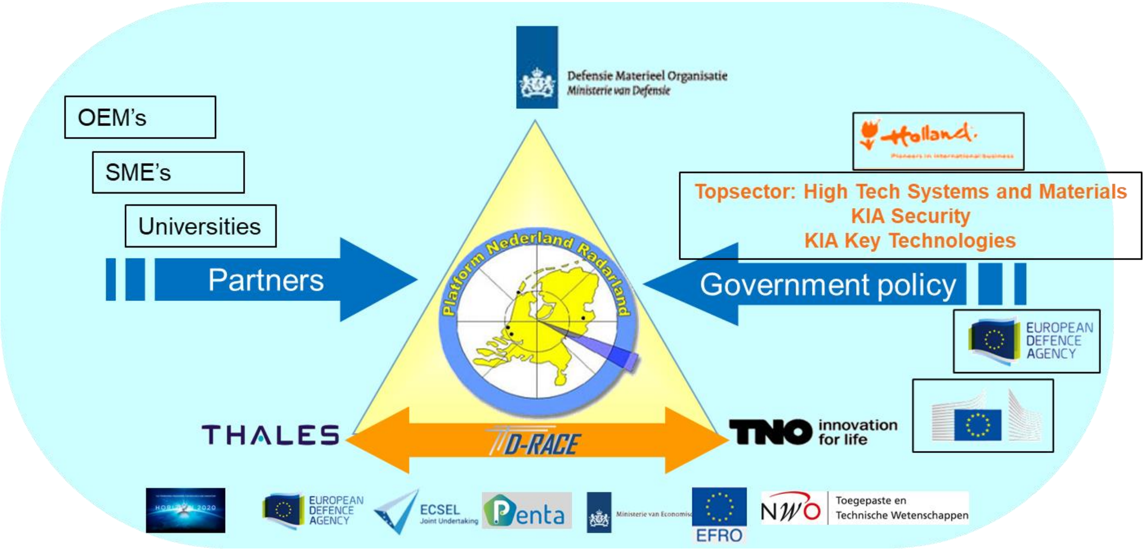
For many sectors application of quantum sensors is either predicted or already in place. These sectors include: Defence, Law Enforcement, Automotive, Agriculture, Oil & gas, Transportation, Construction, Medical & Healthcare and IT & Telecommunication.

Part of the reason why the market reach is so wide, is that quantum sensors vary in function considerably. Some examples: quantum enhanced positioning, navigation and timing (PNT), quantum radio frequency sensing, quantum optronics sensing, quantum magnetometers (detecting differences in the earth's gravity field), measuring photosynthetically active radiation (PAR).

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 general RF front-end technology for AESA antennas, algorithms and processing and more specific initiating steps beyond AESA based systems) 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 and beyond. 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 programs 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 European Defence Fund.

Intelligent passive sensors require increased processing power, which can lead to undesired heat dissipation. Novel concepts like “green ICT” can cope with this drawback by working on architectures beyond the traditional Von Neumann.

Using Green ICT requires new algorithm types adding intelligent processing to (or close to) the sensor. Developing such algorithms should start n 2022, possibly by using a simulated Green ICT architecture.

New algorithms in the area of detecting “intent” locally must be developed to offload observers

Focus areas for research and development in quantum sensing are:

1. Identifying trends in, industry use cases for and ultimately the quantum advantage within the wide range of available and nascent quantum sensing technology;
2. Technology and application driven research & development of quantum sensor systems themselves (or in the context of hybrid systems), amongst others in the promising field of quantum enhanced positioning, navigation and timing (PNT), RF sensing and cold atom based inertial sensors;
3. Quantum enhancement of ‘classic’ sensor systems, for instance by utilising quantum sensor components or exploring advantage of quantum algorithms for sensor systems;
4. Industrialisation of quantum sensors, for instance reducing size, weight, power requirements.

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 by enabling as yet unthought-of functionality.

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, virtualization techniques, 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 intelligent decision support for the so-called external battle, with decision support for the internal battle (such as platform damage repair) in a way that supports optimization of systems and crew.

4.2 Areas of application and technological challenges and priorities

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, RH Marine, Damen Schelde Naval Shipbuilding (DSNS) 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 enable replacement of the stove-piped IT architectures by an open IT architecture that integrates the two key naval systems, i.e. the combat management and platform management systems. As a result, resources for combat and platform functionalities, computations, electrical power and ship propulsion, can be managed as to optimize operational effectiveness and crew size.

Thales, RH Marine, DSNS, TNO and DMO have defined their research activities for the period 2022-2027 in the MCS roadmap, which one-to-one relates to the '*Bedrijfs- en Commandovoering*' roadmap in the '*Kennis Plan Zee'* of the Dutch 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 a number of **application areas.**

Traditionally, all information onboard navy vessels is created, processed and stored in system stovepipes. Sharing and integration of information are done manually which is laborious and therefore expensive. The aim of the RNLN is to remove these stovepipes and work towards an Information integration infrastructure called the Integrated Mission Management System (IMMS). The IT backbone of the IMMS provides common services and hardware as well as sharing of information between naval systems, which forms the basis for better or new applications (listed below) for integrated mission management.

In warfare operations it is important to collect information, assess the situation outside of the vessel for the external battle, the situation onboard of the vessel for the internal battle, and select the most appropriate course of action that enables to win both battles at the same time, as fast as possible. For this purpose, sensor networks for situation assessment and automated decision support tools for assisting the command team are developed. Important issue for the design of these support tools is the interaction with the operational user, requiring innovations both with respect to explanation facilities and user experience design.

Nowadays naval systems have become so complex that onboard technical personnel cannot always repair system components. Offshore personnel can assist either immediately, e.g. by performing analyses as a remote service, or as part of a logistic process, e.g. by flying over a technical team to provide onboard support. Important innovations in this area will originate from the use of eXtended Reality techniques, including both Virtual and Augmented Reality.

The future vessels of the RNLN are designed for mission flexibility. This means that naval systems should adapt during the mission preparation or even at runtime whenever required by operational or technical conditions. Because of the complexity of naval systems this means that the decision when and how to adapt in many cases has to be made autonomously, i.e. by the system itself.

Mission adaptivity will eventually lead to extensive system autonomy and hence to a changing role of the onboard crew who will have more of a supervising role. This requires new interfaces and interactions between crew and naval systems in which this role is incorporated by design.

Successful development of the above-mentioned applications onboard Dutch navy ships relies on solving a number of **technological challenges**.

For naval systems to adapt either autonomously or as decision support to the crew, means that the entire functional chain from mission goal to situation assessment and mission effectiveness of the platforms, sensors, and effector has to be modelled. For a modelled chain, all courses of action are evaluated at runtime leading to the optimal allocation and settings of the available resources. For intelligent decision support, this requires explicit knowledge representation and associated reasoning techniques, which also forms the basis for advanced explanation techniques. This is essential to create trust in the reasoning and decision support. In that respect, also Human Factors and User eXperience design are important. For optimization of intricate functional chains, sophisticated techniques are employed that combine reasoning and optimization to find the optimal solution within time constraints and within the available computational resources.

During the extensive modelling of the mission goal, situation assessment, and mission effectiveness of the resources, modelling errors are introduced which lead to inaccurate decision making. Learning the system if there are data available or assimilating scare data in the functional chain, allows to remove these errors, in any case to the extent that better decision can be made. The issue of trust, by the user, in the system remains essential.

With increasing complexity of autonomous systems, formal verification and model checking techniques can not easily be applied at design time. However, customers will still require verification and validation of the system, to some significant extent, before accepting it from industry. This is an important challenge for both autonomous systems, and system that include Machine Learning technology. In the long run, verification and validation may have to be done at runtime on the basis of generic and domain-specific software monitors. How to design such monitors is an emerging research field.

In the future, the RNLN will increasingly make use of collaborative organic assets such as groups of small or medium UAVs and USVs. The mission tasks of these organic assets are much more flexible than those of high-end naval systems. Scalable integration of unmanned assets, with varying degrees of autonomy and varying degrees of control, is a major challenge. For the software design of collaborative assets, agile design, based on the method of model-based systems engineering, may become a success factor: one mission of e.g. a few months may contain a number of different specific mission profiles, hence, a full engineering cycle (mission profile specification, generic and domain specific software for mission management, and verification and validation) may have to be accomplished during the mission.

4.2.2 Land-based vehicle platforms

In the Defense Vision 2035 there is a clearly articulated role for the information-driven actions – paradigm of the RNLA (IGO: "Informatie Gestuurd Optreden"). This describes the vision to be in the forefront of better and quicker information analyzing, and filtering and realize desired effects as a result of combining information from different sources. This has its impact on the Land Vehicle Platforms that have become 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 & Cloud, Collaborative Combat 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 FOXTROT, where improved radio and communication equipment is being introduced, TEN (Tactical Edge Networking), DLBO (Digital Land Based Operation), and mid-life upgrades of CV90. In addition, 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 sharing of authenticated and trusted sensors from the (military) "Internet of Things", and reliably controlling actuator, National and coalition interoperability (network & air interface), Security (information and communication), and (wireless) Network performance and management. Here, it becomes important to have secure information sharing of information with different classification levels, not only inside manned the land-vehicles, but also between vehicles, in the concept of joint manned- unmanned teaming where (semi)-autonomous vehicles cooperate in a coordinated fashion with manned vehicles.

The second challenge is *Open platform architecture*, mainly addressing the issue of Scalability, adaptability, configurability, maintainability, and that of Security (cyber, infosec, separation/). The concept of MLS (Multi-Level Security) where over a single physical network, there will be multiple security levels, is expected to become even more pronounced. The issues related to the "Information Gestuurd Optreden"- paradigm, leads interesting questions on security separations at different places in an open platform vehicle architecture. Clearly the introduction of new gateways could solve some of these technological challenges, but it is also very interesting to look for other means of separation, such as content -based security, that provides ways to flexibly define COI (Community of Interest) for information that can be shared.

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. The introduction of softwarized networking as a means to support optimized operations further confirms the need for enhanced software and communication security. Also within the (manned) vehicle there is a call for the introduction of mini-Security Operations Centre, for anomaly and intrusion detection & prevention in and around vehicles. In this AI is going to play a role.

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

- Intra-Platform and inter-platform architecture framework for applications and services
- Softwarized networking and Tactical Cloud in the tactical and deployed domain
- Using new communication radio technologies (SDR, LTE, 5G, sub..) integrated in the (secure) communication architecture
- New HMI concepts to optimize situational awareness and decision making
- Cybersecurity hardening
- Distributed high available communication and information Trust relationship inter- and intra-vehicle and with sensors/effectors (Military IoT)
- Security monitoring for mobile platforms using AI for intrusion and anomaly detection
- Comprehensive mission configuration for and in mobile domain

- Information security/separation (content-based security) in mobile (platform) domain
- Infosec/cyber and C8I architectural concepts for unmanned/autonomous platforms land platforms, including secure, resilient/robust and trusted communication
-

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.

For the **protection of Naval systems/platforms**

- 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)

4.3 Programmes

For **naval systems** within the timeframe 2022-2027, each of the application areas in the MCS roadmap contains a number of projects which are prioritized and selected according to cooperation strategies between Thales, RH Marine, DSNS, TNO, and DMO. Programmes that support these projects are listed below.

The most important programme that supports naval systems is Manning & Automation of DMO/Technology Integration. A wide variety of research projects are included in this programme with strong focus on combat management systems and platform management systems. By nature, this programme concentrates on the navy domain. Nevertheless, whenever possible, research applications in cross-domain sectors like the army, air force and security domains are also exploited, either because there is direct need of a solution or as a funding or knowledge multiplier for naval systems.

Another important programme is the National Growth Fund within which the Dutch government will spend €20 billion over 2021-2026 in three main areas: fundamental knowledge, research & development, and infrastructure. Because naval systems is based on an ecosystem that includes end users, a research institute and industry innovators, it aligns quite well with the Growth Fund's main areas. Especially in the field of artificial intelligence (AI) and AI applications such as autonomous air and sea surface vehicles or predictive maintenance, the Growth Fund is expected to support naval systems.

Besides national programmes, naval systems is supported by the Framework programmes of the European Commission and the European Defence Agency as well. First there is Horizon Europe 2021-2027 with its Civil Security for Society work programme. Within this work programme, the Border Security Call focusing on maritime technologies is of special interest to naval systems. Thales, RH Marine, DSNS, as well as TNO, all hold impressive track records in the European Framework programme and expect to continue these records in Horizon Europe. Second there is the recently launched European Defence Fund 2021-2027 of the Commission and EDA. Topics of interest in the EDF include: information superiority, artificial intelligence, naval combat, and disruptive technologies. Thales, RH Marine, DSNS, and TNO are all involved in several topics of the EDF's 2021 Call and intend to do so in the forthcoming years.

Also the **land-based vehicle platforms** and the **protection of IT infrastructure** may benefit from the EU funding instruments.

EU funding instruments play a key role in ensuring the uptake of the results of security research programs. These instruments can facilitate technology suppliers in industrialising and commercialising their security products and services and scale-up. These instruments can also facilitate security practitioners in testing or validating, and in acquiring new security solutions.

In the course of the implementation security solutions the funding of Horizon Europe, intend to actively pursue synergies of cluster 3 (civil security for society) of the Horizon Europe work programme.

Among the synergies to be created with other parts of the Horizon Europe programme, those with the European Innovation Council (EIC) will be particularly interesting for SMEs. Using the EIC, in particular the EIC Accelerator, start-ups and innovative SMEs could benefit from funding for innovation uptake of solutions with high entrepreneurial risk and high impact in the security domain.

Synergies with other programmes will cover, first and foremost, the security relevant programmes such as:

- the Digital Europe Programme, 78 projects addressing cybersecurity, artificial intelligence and strategic digital capabilities;
- the EU Civil Protection Mechanism with the rescEU instrument 80 projects, enabling a strengthened EU response to disaster risk management; and
- the European Defence Fund, for technology areas of common interest for civil and defence stakeholders;

- the European Space Programme, notably via its Horizon Europe (cluster 4) dedicated to the development of downstream applications for Galileo and Copernicus services, both of major relevance for security-related applications.

Furthermore, within cluster 3 of Horizon Europe, the services of the Commission intend to focus on the use of innovation procurement and standardisation, and other catalysts for market uptake in the security domain

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, RuG, UTwente, Radboud University, Tilburg University
Cooperative platforms	e.g. TUCCR, HSD, Cybersecurity Noord, dcypher, ACCSS
Institutes	e.g. TNO, AIT, Institut Mines Telecom, KTH
Security Industry	e.g. Thales _Nederland BV, RH Marine, Microflown, Adimec, CGI, Cyberveilig Nederland, Compumatica, EclecticIQ, RISCURE, IBM, BizzDesign, KPN, VMWare, Qbit, Mnemonic, F-Secure, ATOS, Centric, Secura, Foreseeti, Sightlabs, Nedinsco, Demcon, NCIM, Grass Valley Netherlands (GVN), Contour Advanced Systems, Geomaat, Quest Innovations, CroonWolterenDros, Innovative Technical Solutions (ITS), Lahoux optics, ZIUZ Visual Intelligence. Quix Quantum, Lionix
Government	e.g. Ministry of Defense, Ministry of Justice and Security, Ministry of Economic Affairs, Royal Netherlands Navy, Platform Nederland Radarland, National Police, Coast Guard, MoD – DMO, critical infrastructure providers, NCSC, Dutch Tax Office
Industry	e.g. Prorail, Alliander, Schiphol, Havenbedrijf Rotterdam, Vattenfall, ASML, ING, ABN Amro, Volksbank, Achmea Bank
International Programmes	e.g. European Defence Agency (EDA), EU Research and Innovation Framework (H2020, Horizon Europe), CELTIC Plus, ECSEL, PENTA, NATO STO

Additional partnerships and relationships:

- The Roadmap Security is linked with the Missiegedreven Topsectoren en Innovatiebeleid, including the KIA Veiligheid and the Kennis- en Innovatieagenda Sleuteltechnologiën.
- The Roadmap Security is linked to the various HTSM R&D Roadmaps, such as Roadmap Electronics, Roadmap ICT, Roadmap Systems Engineering. 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 ”Samenwerkingsverband Manning & Automation”. The results are disseminated approximately every 18 months at a dedicated national event.
- 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	**2022-2025**
Industry	20
TNO	4
NWO	6
Universities	4
Departments and regions (excluding TKI)	16
Grand total	**50**