National
Innovation Agenda for Security 2015

Public-private innovation for security and prosperity

The Hague Security Delta

National Innovation Agenda for Security 2015

Public-private innovation for security and prosperity

The Hague Security Delta

Foreword

The Netherlands is an attractive country to live, work and invest in. Security creates the conditions for societal stability and economic development. Without that stability, Amsterdam would not have been able to grow into a world player in the internet exchange business and the mainports Rotterdam and Schiphol would not be able to fulfil their hub function. The Hague would not enjoy its international status as City of Peace and Justice and the Eindhoven region would not be considered one of the most innovative regions in the world. All these things make for a strong position for our country; one we need to keep in a fast-moving and increasingly competitive world. This is why it is important to recognize security as a major economic sector and to understand that for this sector innovation and job creation are two sides of the same coin. To be successful in both, requires that businesses, knowledge institutions and government work together in this sector on an ongoing basis, collectively, ambitiously, flexibly and with conviction.

The national security cluster The Hague Security Delta (HSD), with its primary geographic concentrations The Hague, Brabant and Twente, has an important role in this as driver, organizer and coordinator. As such, it is obvious that HSD is the party to draft a National Innovation Agenda for Security (NIAS). It is an innovation agenda that ties together *government, research, learning institutions and enterprise*, four points specifically highlighted in the current government coalition agreement. The NIAS supports these cabinet ambitions. This public-private cooperation brings the knowledge circulation (the necessity of which is highlighted by the Academic Council for Government Policy) to fruition, creating more security and more jobs.

This agenda is a source of inspiration for all parties with a will to commit to innovation and economic growth. At the same time, the agenda provides an opportunity to identify a number of key focus areas for innovation that security parties can achieve jointly in the process. It is an opportunity for governments, businesses, and knowledge institutions to better harmonize their knowledge development, innovation efforts, and acquisition needs. For the requisitioners and clients in the security domain, this will mean more value for their money, while for the supply side, it will mean a more robust and predictable market. All in all, the agenda offers a foundation for the generation of strong, internationally operating consortia, which will keep the Netherlands in its position in Europe as a major economic player in the field of innovative security solutions. This agenda also provides The Netherlands with a perfect response to the innovation goals of the European Commission as formulated in the Horizon 2020 research programme, which also promotes the importance of the partnerships between businesses, government, knowledge institutions and academia. It therefore is a national agenda with international significance and appeal.

I am very pleased to see a public-private agenda giving direction to innovative and economic development in the field of security and I thank the authors and everyone who has contributed to this document.

Prof. Dr. Rob de Wijk
General Director, The Hague Security Delta

Table of contents

Foreword 3

Introduction and reading guide 7

1 Objective and process of the National Innovation Agenda for Security 9

1.1 Aim and outcomes 9

1.2 Roles and responsibilities 10

1.3 Production process 11

1.4 Review framework 11

2 The National Innovation Agenda for Security 2015 13

Theme 1 – Partnership in networks and systems 15

Theme 2 – Societal innovation for security in society 17

Theme 3 – Resilient critical infrastructure 19

Theme 4 – Action-oriented information provision 21

Theme 5 – Observation with unmanned systems 23

Theme 6 – Process innovation in and between professional organizations 25

3 Innovation investments and returns 27

3.1 Innovation investments in a coalition context 27

3.2 Linking NIAS and procurement agendas 33

4 The NIAS in a broader perspective 35

4.1 National Security working procedure 35

4.2 Investments in security 35

4.3 Administrative complexity and governance at system level 36

4.4 Top sector policy and the Security and ICT roadmaps 37

4.5 Towards a learning economy 38

4.6 Smart Industry 38

4.7 The European ‘grand challenge’ Secure Societies 39

5 Final considerations 43

Appendix 1 – Discussion partners interviewed in consultation and review rounds 45

Appendix 2 – Documents consulted 47

Appendix 3 – Notes 49

‘We have to work hard on inclusive, or integral, innovation. This is about innovations that not only lead to economic growth and a more robust society, but at the same time, more security as well.’[1] Ivo Opstelten

Introduction and reading guide

The National Innovation Agenda for Security 2015 (NIAS) presents a vision for the Netherlands in international perspective, of the most significant innovation projects for national security in the coming three to five years, with a look ahead to the coming 10 years. This public-private agenda focuses on a combination of technological, societal and process innovations that call for a collective approach by requisitioners, developers and end users. The goal is to create societal and economic value in the foreseeable future.

By connecting supply with demand, the NIAS creates for the Netherlands a cohesive action horizon for the central and devolved public sector, for private requisitioners and suppliers of innovative products and services, and for knowledge institutions in the security domain. This gives businesses, governments and knowledge institutions, together referred to as the 'triple helix', the ability to steer demand for innovative security solutions towards the innovative strengths they can generate through effective cooperation, while creating a valid earning model for the introduction of these solutions.

The NIAS is not only a product, but also a process: it is regularly updated based on results achieved and new insights, in order to support the primary goal of achieving the key focus areas for innovation. The Dutch national security cluster *The Hague Security Delta* (HSD) drafts the agenda, manages it as a product, and supports it as a process. The triple helix initiatives from the regions of Twente (TS&S, Twente Safety & Security), Brabant (DITSS, Dutch Institute for Technology, Safety & Security) and The Hague are united under the brand name The Hague Security Delta.

Reading guide

Chapter 1 describes the goal and positioning of the NIAS and the process behind the creation of the agenda. Chapter 2 presents the actual innovation agenda for 2015. This chapter is structured around six themes encompassing the major challenges and opportunities for innovation that require successful cooperation in the triple helix context.

For each theme, we focus attention on a few selected key focus areas that should lead to specific innovations within the next few years. Chapter 3 is devoted to the achievement of the agenda. An essential aspect is the table linking the key focus areas for innovation to the parties willing and able to develop, to apply and to market the innovation. This chapter also makes the connection between the key focus areas for innovation and the major acquisition programmes in the security domain. Chapter 4 elaborates on the context within which the NIAS has to function. This chapter helps to clarify the interaction between a number of broader societal developments and the NIAS as product and process. Finally, chapter 5 presents a few concluding remarks about the process.

Readers with a material interest in the National Innovation Agenda for Security 2015 may suffice by reading chapter 2. For a more detailed understanding of the specifics of the key focus areas, readers are advised to also read chapter 3.

‘Public-private partnership in the security arena brings out the best in all parties. The government can learn a lot from businesses, and vice versa. This productive interaction generates synergy, an important added value from which we can all benefit.’[2] Ivo Opstelten

1 – Objective and process of the National Innovation Agenda for Security

Local, regional and national governments have the core task of guaranteeing our security.[3]

1.1 Aim and outcomes

In the coming years, the Netherlands will be investing billions of euros in public funds towards increasing the security of society. But also semi-public and private institutions and businesses continue to invest in solutions to address security threats or incidents to ensure business continuity. The critical sectors (energy, telecom, water, transport and financial infrastructure) are some of the most prominent examples. These investments are being made against the background of a dynamic society with sometimes rapidly changing risks and threats, security arrangements and technological resources. Innovation is essential in taking on these challenges and being able to capitalize on them.[4] Investments in security must be innovative in nature, even where they are 'replacement investments.' Making optimal use of the innovative strength of businesses, government and knowledge institutions[5] is required.

A second key factor is the increased scale of security issues, caused by increasing dependencies, making it necessary to look beyond geographic, functional, hierarchical and systemic boundaries. Improvements will be necessary to achieve the effects intended by all actors: more value for money from every investment in security.

During the *Security through Innovation* conference on 10 October 2013, representatives of industry, governments and knowledge institutions expressed the need to combine energies and efforts in the fragmented field of public and private security partners. A shared innovation agenda is an important step towards this. Together, the Ministry of Security and Justice and The Hague Security Delta (HSD) took the initiative on behalf of this group to draft this National Innovation Agenda for Security (NIAS) based on the available material. It is built on three fundamental points:

- the needs and demands of parties with a responsibility to contribute to the security of society;
- supply-driven, technological or innovative developments and trends;
- capacity for initiatives not specified in advance.

From March to October 2014, we surveyed the available material and conducted a large number of meetings with stakeholders in the security cluster.
The result is this National Innovation Agenda for Security (NIAS).

Goals of the Dutch National Innovation Agenda for Security
The National Innovation Agenda for Security is an agenda for public and private parties designed to stimulate and organise shared innovation. The NIAS provides a framework and sets priorities that governments, businesses and knowledge institutions (the 'triple helix') can work with to coordinate their innovation efforts, strive for synergies and connect innovations to future-oriented acquisition programmes. When this interaction is functioning properly, suppliers of innovative products and services are better assured of a robust and predictable market. The NIAS offers a cohesive perspective for reaping maximum societal and economic benefits from innovations.

> *'Knowledge and Innovation is not a goal, but a means of containing societal and economic impact. This is served by cooperation between government, businesses and knowledge providers.'*[6] Erik Akerboom

Below, we will briefly look at the most significant components of this objective.

Collective agenda
The NIAS has been drafted under the banner of the HSD, the national security cluster. Over the past few years, the Netherlands has seen several different regional initiatives emerge, each with the object of promoting security innovations in the triple helix context and so furthering economic development. These are, Twente Safety & Security (TS&S) for the Twente region, the Dutch Institute for Technology Safety & Security (DITSS) in Noord-Brabant, and HSD in The Hague and environs. TS&S, DITSS and HSD have established in a covenant that they will cooperate intensively and that HSD is to represent the collective interests at the national level and as umbrella organization. To reflect this, DITSS and TS&S are represented in the board of HSD. This effectively creates a national security cluster, with The Hague Security Delta as brand name for the national and international positioning of Dutch knowledge and expertise in the field.[7]

Solution-oriented innovation in the triple helix
The NIAS takes a connecting, system-oriented approach. The agenda focuses on innovations that demand a broad, joint approach on the part of the requisitioners, developers and end-users, which constitutes a combination of technology, people and organization. Creating these combinations depends on making good use of idea factories, living labs, experiments, etcetera. The NIAS focuses on applied innovation with results in the coming three to five years. The NIAS is not a technology radar or horizon scan focusing on emerging technologies that will only produce innovations in the long term.

Perspective and priority
There are already a number of knowledge and innovation agendas in the public and private sectors that address the interests, goals, needs and potential of stakeholders in the security domain. The NIAS does not present its own analysis of the demand for or supply of innovative security solutions, but rather builds on the insights of these existing visions, agendas, roadmaps and ongoing or planned innovation trajectories. The NIAS does, however, follow its own structure to reflect the cross-connections between supply and demand and between societal and economic business cases. Within this structure, we highlight key focus areas, selected based on a review framework.

Leverage effect
An important function of the NIAS is to specify, distil and endorse the needs on the requisition side.[8] By grouping different stakeholders, each with their own innovation budget, around certain subjects and priorities (and likewise grouping subjects and priorities around different stakeholders), and by synchronizing these stakeholders' innovation efforts, the agenda becomes specific and action-oriented, and advantages of scale and leverage emerge.

Connection with acquisition processes
An essential part of the societal and economic value creation is the connection between the NIAS and the acquisition agendas of the various governmental and commercial parties on the demand side, (particularly in the critical sectors). Naturally, investments in innovation only make sense when there is a possibility of return on investment. On the demand side, this means solutions that remain effective in the future. On the supply side, there needs to be a reasonable chance of the investments turning into products and services that generate sales and return within a foreseeable timeline. Only then coalitions of parties can form with a willingness to commit to the process of development and marketing of the innovations in question.[9]

Action horizon for societal and economic benefits
There is a clear sense of urgency on the subject of security: without ongoing and focused efforts, the government will find it increasingly difficult to keep the public and society safe, the Netherlands will loose its strength as a home of knowledge and innovation and the Dutch economy will lose its international competitiveness and earning capacity.

'The government has to help speed things up. By leveraging new knowledge and innovation, we can become a leader in the world and connect our everyday operational experience to the developments of tomorrow.'[10] Menno van de Marel

The NIAS is an important roadmap for channelling this urgency into specific projects that will lead to tangible results. The key focus areas in the NIAS have been selected for their potential to create both societal and economic value. The selection is appropriate to the wide range of interests and is the basis on which a productive triple helix cooperation can be founded.

1.2 Roles and responsibilities

The national security cluster HSD is driver, drafter, facilitator and manager of the NIAS. The cluster offers an open and trusted environment in which partnerships can be built around knowledge and innovation plans and processes. This mix of openness and enhanced trust is necessary for getting the new forms of partnership and business models, relevant to implementing the NIAS, off the ground. The partners in the cluster are the recommended parties for initially structuring the cooperation around the key focus areas for innovation defined in the agenda, committing to them and leading by example in implementing them.

Another goal of the NIAS is grouping the needs and demand for security solutions. Articulating the demand and grouping its individual components from within the public sector security partners is a process that benefits from central management. The **Ministry of Security and Justice** (S&J) has a clear role here. S&J encourages government parties to ask security-oriented innovation questions and makes these accessible to interested companies and knowledge institutions. At present, S&J's directing role is primarily taking the form of support or coordination. The parties that cannot provide this for themselves and which have a need for a party to set priorities for them from a broader perspective (guidance rather than coordination) can call on S&J . At the same time, S&J does not have any system-wide responsibility here, and is not politically accountable for the NIAS.

The **Ministry of Defence** formulates the military needs of the armed forces for fulfilling their role of structural security partner. The VCMS ('Strengthening Civil-Military Partnership') has a focus on shared knowledge-building and innovation, among other things. The NIAS supports and builds on VCMS initiatives.
The triple-helix partnership in the national security cluster is backed by the **Ministry of Economic Affairs**' top sectors policy. Although its emphasis is on economic value creation, this policy also addresses societal value creation. Societal security is, for all sectors, critical for business continuity and customer protection.

'HSD stimulates, facilitates and organizes cooperation between companies, government and knowledge institutions on security issues.'[11] Rob de Wijk

On each **innovation key focus area** in the NIAS, one party from the national security cluster must take the *lead*. This entails that that party takes responsibility for initiating a partnership on that key focus area and maintaining its momentum. Coalition-forming is an important first step. The actual implementation, financing and embedding of the activities of a key focus area is and remains a responsibility of the contributing parties themselves.

1.3 Production process

We approached the parties involved in the national security cluster to make the agenda a collective product. This is not a one-time action, but an ongoing activity involving periodic updates of the NIAS. From March to November 2014, we conducted the following process.

1 Inventory and analysis of a large number of national and international knowledge and innovation agendas in the security domain. Based on the results, we drafted an initial thematic structure to provide a framework of the current challenges in the security domain, primarily from the perspective of the demand side, but without neglecting the supply side (or 'technology push'). Within this overall structure, we created a longlist of subjects and running initiatives.

2 This longlist was used as the starting point for the inventory round, for which we consulted with a large group of stakeholders (see appendix 1), asking them to identify, in the clearest possible terms, what they considered the most important innovation key focus areas from their individual perspectives.

3 We used the results of the inventory round to adapt the initial thematic structure, selecting key focus areas derived from a review framework (see next section). This resulted in a shortlist. All this was documented in a draft version of the NIAS, which was reviewed in the Executive Committee and the HSD Advisory Board. An important component of this review is the prospect of commitment of triple helix parties on making a real contribution to the implementation of the innovation key focus areas.

4 We incorporated the commentary and suggestions from the inventory and review rounds into a draft NIAS 2015, which was approved by the HSD Board on 29 September 2014. The NIAS 2015 was endorsed by a number of executives from the security domain on 26 November 2014.[13]

The production process of the NIAS encompassed more than just these four steps; it was also embedded in a number of network activities within the security cluster. These activities contributed to the form and content of the agenda. By the same token, the NIAS as process and product, stimulates knowledge circulation within the security domain. Finally, the NIAS is a living document, which we update periodically. In that sense, the NIAS should be seen as a snapshot; new initiatives and themes can arise at any time.

1.4 Review framework

The production process included a review framework designed to focus and calibrate the agenda as it developed. This was done based on the following criteria:

1 There must be an **essential and present gap or need**; the societal benefits.

2 That gap or need demands a **widely applicable and viable solution** at the system level[14], generally in combination with technological, social and process innovation.

3 This makes a **joint approach** by the requisitioners, end-users, innovators and vendors of products and services (the triple helix approach) necessary or at least desirable.

4 This approach leads to innovation processes with the potential for **significant or substantial market turnover**, economic benefits and export potential.

5 An important consideration is that there is a demonstrable **support base and commitment** among a 'coalition of the willing and able' in the triple helix with an interest in developing, using and marketing the innovation, and a will to follow investment agendas or strategic visions; the process of production of the NIAS must guarantee that this is the case.[15]

6 The innovation processes must be able to **produce results in the coming 3 to 5 years**.[16]

This means that the process was specifically not intended to be a strict valuation process of all potential options to result in the best-scoring selection. This would not only have been a very time-consuming process, but would have been exceedingly difficult to set up in an objective and inclusive manner.

2 – The National Innovation Agenda for Security 2015

The process described in section 1.3 produced a list of 16 key focus areas, which we group into six themes. Although broadly defined, together the themes reflect all current dynamics in the security domain. Within the themes, the innovation key focus areas highlight a number of more specific points of emphasis. The key focus areas are described in more detail in table 3.1.

Theme 1 – Partnerships in networks and systems
Theme 2 – Social innovation for security in society
Theme 3 – Resilient critical infrastructure
Theme 4 – Action-oriented information provision
Theme 5 – Observation with unmanned systems
Theme 6 – Process innovation in and between professional organizations

'The Dutch security sector recognizes the developments outlined in the agenda; the themes included in it are very much identifiable as areas in which innovation is desired and possible.'[18] Laetitia Griffith

Theme 1 – **Partnerships in networks and systems**

Partnerships in networks and systems

Over the past twenty years, the concept of *security* has seen a transition. It has broadened and has become interwoven with other areas as a result of new and more far-reaching threats.

Examples are many: cyber crime and attacks in the cyber domain, cross-border organized crime, global instability as a threat to trade and economic growth, and international terrorism, to name a few.

As a result of these changing threats, the response side similarly broadened and became interlinked. In 2007, the National Security Strategy was drafted to facilitate full-spectrum risk evaluations and full-spectrum capacity considerations.Security parties have expanded their working spheres both horizontally and vertically. This trend has led to the establishment of security regions, boosting of civil/military cooperation, the institution of a National Police Force, and expansion of procedures for supra-regional crisis cooperation. The comprehensive approach to security is becoming increasingly essential. An adequate approach to issues such as urban or electronic security demands close coordination between multiple policy areas and the cooperation of many parties, including the public and the business sector; see also Theme 2: Social innovation for security in society But legislation and regulations have to be able to keep up, if they are not to be a limiting factor on the necessary innovation. Also, privacy issues, ethical issues and administrative issues present important considerations, and in some cases limitations, on security solutions.

All in all, security is increasingly becoming a multi-party network challenge. Solutions have to be conceived within an ecosystem of a wide range of public and private parties that have to be able to come and work together, with or without the help of a coordinating party. The network connections are sometimes short and temporary in nature; indeed, with the increasing number of parties with a role in security (including the public and the business sector), this may well be more and more the standard. This puts additional demands on the processes, structures and systems designed to connect actors in networks and chains quickly, on an ad hoc basis, and yet still in a reliable manner. New ways of coalition-building and cooperation are required. Setting up pre-competitive experimental environments can be useful here.

Innovation key focus areas:

1 Management of demand articulation: 'one government'

The overriding role of the government in the security domain (and certainly the public security domain) is unquestionable. More focus, mass and collectivity in innovation processes starts with better coordination and aggregation of the vision of, need and actual demand for innovation in the institutions of government. It is important for the public sector security partners to combine their innovation needs where there is overlap, and be coordinated when farming them out to research institutes, the private sector, national innovation funds and the European Innovation Fund Horizon 2020. The obstacles that outdated legislation and regulations could be for innovative applications, must be reduced, but they must be reduced carefully, as well as intelligently and quickly. Innovation in our security system demands a precise balance between legal rigor and due care versus the desired or necessary speed and flexibility of action, in consideration of the distribution of roles, tasks and authorities in our security system. This is particularly important where there is a need for, or benefits or opportunities in acting jointly and/or developing and procuring scalable solutions.

2 Learning from incidents and drills

The document *Staat van de Rampenbestrijding 2013* observed that there is little to no evaluation following emergencies and disaster drills. Lessons from practice are generally either learned poorly, or learned well but not developed into improvement plans. Often, the problem does not lie within the organizations themselves, but rather in the more complex learning loops that span the network of very different organizations. The need to learn from incidents is self-evident. Serious gaming can play an important role here; see also theme 6: Process innovation in and between professional organizations.

3 Value creation in triple-helix innovation

This is an innovation task that the partners in the national security cluster must, to a significant degree, drive themselves. It revolves around three central process elements. Firstly, the business side of innovation, with elements requiring regulation such as intellectual property (IP), using results in product-market combinations, and the process from innovation to acquisition. Secondly, building coalitions that generate mutual trust. Thirdly, facilitating optimal crossovers between technologies, between and across areas of application, and between societal and economic value creation. Often, refreshing and unexpected ideas are born from interactions between people in different disciplines and fields (this is sometimes referred to as 'clash of disciplines' or 'wildcard innovation'), or between developers and end-users. Promising innovations arise when partners opt for open innovation and broad-spectrum, inter-sector, international and inclusive approaches. As they are developed, the themes set out in the agenda will be supported, enhanced and tested wherever possible with Concept Development & Experimentation processes in programmes, projects, innovation houses, networks, living labs and operational experiments in which security solutions are conceptualized, tested and/or further developed.[19]

Theme 2 – **Social innovation for security in society**

Social innovation for security in society

Companies, societal organizations and individuals are increasingly indispensable parts of sustainable solutions.[20] Social innovation in security starts with the involvement and awareness of the public, knowledge institutions, governmental agencies, civil society organizations and the business sector. These parties develop and pursue their own initiatives, which can grow when other actors and parties encounter their relevance and importance. Social networks and social media can be an important part of this, with government in a facilitative and sometimes driving role.

Security in and of society is only really embedded when questions of security are included from the earliest stages in the design of all types of societal functions, such as housing, work, transport and recreation, and all the infrastructure that each requires.

Previous initiatives have shown that individuals, companies and societal organizations are interested in playing an active role here – things like providing security around the railways, responding to aggression on public transport, coming together to provide more security in communities and urban districts, fighting nightlife violence or ensuring collective security on business parks and industrial estates. This demands new ways of organizing, daring to think beyond (individual) professional boundaries, and redefining traditional roles and responsibilities. Today's emphasis on 'fighting insecurity' will give way to a new concept of 'designing security.'

In areas such as care, education and health, customized solutions tailored to the individual needs will increasingly be the norm. The same will be true for security. Within the foreseeable future, we will move from a situation in which professionals decide what happens, with the support of the public where required, to the reverse: the people (our 7.5 million households in nearly 12,000 communities) will decide, and professionals will support. The government will maintain control over external and physical security, as well as responsibility for legislation and regulations, and will enforce them where boundaries are crossed.

Innovation key focus areas:

4 Social innovation and self-organizing capacity

Resilience and self-sufficiency in society must be enhanced.[21] This can be done by utilizing the self-organizing capacity of society, with the government in an encouraging and supervisory role. Important tasks are finding and offering new and appropriate forms of self-organizing capacity, and accessing and organizing societal strengths. Individuals can build up their own intelligence/ information position to give themselves perspective and enable themselves to actively participate in the discussion of the security issues that affect them directly. Social media, mobile applications, domotics, the 'internet of things' and the semantic web can be important aspects of this.

5 Awareness: perception versus reality

In a complex, dynamic society, new risks are constantly emerging, while others decrease or disappear. Knowing that there are risks, and being aware of them, is the first step in implementing the right measures to address them. Often, the assessment of whether, when and to what extent and in what form potential risks could come to pass is difficult. There are many areas where a general sense of insecurity and increasing risk prevails, even where the actual figures indicate otherwise. Providing society with the right range of potential responses depends on clearly conveying the reality on an ongoing basis. Open data and an open data society can be valuable tools for doing so.

6 Security by design in urban facilities and at events

Unnecessary costs at a later stage can be avoided if security implications, with an emphasis on social security, are considered from the early stages (start phase, design phase, or contracting phase) as an important factor alongside other design parameters such as privacy, architecture, aesthetics or business models. Safe and attractive events have also proven to have a demonstrable economic impact on their environments. Numerous trials have now shown that innovative technologies like Sensing[23] can make a significant contribution to safe and attractive events. However, marketing social innovations is a slow process.

There is a strong need for system integrators to combine sub-solutions into comprehensive innovative solutions and business models. One requirement for the latter is that governmental agencies from the local level up, provide room for innovation and harmonize their regulations and permitting policies.

Theme 3 – **Resilient critical infrastructure**

Resilient critical infrastructure

Critical infrastructure, which can be broken down into individual critical sectors, refers to products, services and underlying processes that, if they become unavailable, can cause societal breakdown, whether because of high numbers of casualties and major economic damage, or if restoration of indispensable products and services takes an extremely long time and there are no realistic alternatives available. As this suggests, the critical infrastructure is crucial for the proper functioning of Dutch society.

Several critical sectors are part of the government: surface water management and waterworks (including the dikes); public order and safety; fire, police and emergency medical response in the event of disasters and crises. Some eighty percent of the critical infrastructure is organised or owned by private companies over which, in many cases, the government exerts a strong influence through legislation, regulations and supervision.
A number of recent cases of foreign investments in the Netherlands (such as the potential takeover of KPN and the intention to allow international trading in shares of Gasunie and Tennet) have brought to the fore the question of how big of an impact such investments can have on national security. So far, the number of this type of situation has been small, but the interests involved are major, both from economic and security perspectives.[25]
This raises questions about where to draw the dividing lines of critical infrastructure (including in the legal sense), the distribution of roles between the government and the companies themselves, and the resources that civil and private parties have at their disposal to protect the critical infrastructure against operational and strategic threats.

One salient development is that all sectors, critical and noncritical, are now connected, although there is no clear picture of exactly what vulnerabilities this interconnectivity brings along. If everything is interconnected and linked to everything else, it remains to be seen whether the actual division between critical and noncritical sectors can continue to be a meaningful distinction. A sector thought to be safe may suddenly be hit by a massive attack for any number of reasons, not least of which because the cyber domain is rife with copycat activity, and knowledge is easy to distribute.

Although in the general sense, awareness of the risks has increased in recent years, there are significant differences in the degree to which different sectors have undertaken adequate action. This has to do with the hacker 'business case' and with actual incidents, the scope and available budgets of companies in the sector, and the level of organization of the sector. Banks have long been a target, and have long since learned to work closely together and share collective information; they have, for example, agreed to not compete in the area of security. In the energy and water sectors, there is much attention to physical security but still relatively little to cyber security.

Innovation key focus areas:

7 Identification and definition of 'critical'

Our critical infrastructure is essential to our society and our economy. Identifying and defining 'critical' is a permanent point of attention. Important aspects of this are questions such as What form should the connection between the policy-makers and the operators take? What as yet unidentified or emerging processes should be classified as critical infrastructure?How can we ensure that critical processes continue without disruption, given the increasing interdependence of all processes? Can we take advantage of common characteristics to improve our resources and the effectiveness of generic and specific protective and response measures? How can smart modularization (e.g. into smart grids) and decentralization of critical functions reduce vulnerabilities of individual critical services and service chains?

8 Cyber security of the internet of things

This key focus area relates to improving the cyber resilience of the wide range of operating systems, control systems and information systems and devices – at home, on the street, in public spaces, in companies, etc. (including ICS/SCADA systems and the like) - that collect data, and which communicate with each other without human intervention in an internet of things. Perhaps most significantly, this also refers to the systems that security organizations use themselves.

9 Chain approach to cyber security

On the one hand, the challenge is integrating information security into everything we do: security by design and cyber resilience not only in the technical sense, but embedded in all processes and structures. On the other hand, this refers to organizing and managing the cohesive series of steps: intention, information, detection and response. Investigation and comparison of best practices is needed, at company, sector, governmental and generic levels.

Theme 4 – **Action-oriented information provision**

Action-oriented information provision

The speed and ease with which we communicate and share information necessitates new ways of organizing and interacting. The military world has been experimenting with information-driven networked action for decades. Where the initial focus was strongly technological, increasingly, the human element, the manner of use (doctrine) and the actual value of networked action are being seen as the more important considerations. Other security parties, such as the police, have also experienced in recent years that they can improve and better utilize their information position with networked action. One recent development is using huge quantities of data to construct a common operational picture (COP), and directing actions based on that COP. Thanks to the internet, social media, databases, and sensors of all kinds (including smartphones), we are now generating exponentially more data than even just a few years ago – and the volume of data generated continues to grow. This is the development of Web 2.0.
But being able to utilize this data effectively requires automated processes to structure, verify, sort, combine and interpret it. This is the step to the semantic Web 3.0, built on knowledge, with the underlying foundation being the vital importance of open linked data. Algorithms for pattern recognition must be further developed. Technology enables us to do this, and is also a major driver, but must be used selectively, with interoperability as an important criterion.

Without viable methods of establishing the identity and authenticity of persons, institutions, things and information, the vast wealth of data we are collecting can easily (if we are not careful) become an impenetrable, unmanageable and invalidated jumble of information. Are people who they say they are – for example, when crossing a border, or on social media? Ascertaining the identities of individuals, and in some cases assessing their intentions, are vital capabilities for public order and security, investigation, enforcement, supervision, counterterrorism and forensics. In September 2011, the DigiNotar incident highlighted the dangers of a compromised identity of institutions and/or their products and services.
The flip side in the internet of things is the uncertainty of whether systems or electronic agents can be trusted enough to provide information to or to perform requested actions for. At the most complex extreme, we face situations in which digital information is read, augmented, altered, duplicated, and potentially replaced without leaving a trace. In all cases, access control, both physical and virtual, is key. This refers not only to the actual accessing of the information, but also to the registration of attempts to access it and the actions taken after access is obtained. Another point of attention is the question of ownership of the information and the right to use it. In a controlled information world, data must be validated, stored effectively, and destroyed when legally required. In the distributed information world with few (if any) controls on duplication of data, the question of ownership and destruction of information remains a largely unanswered one.

Innovation key focus areas:

10 Networked information at central nodes

Here, we distinguish between two types of nodes: Firstly, switchboards, control rooms and command posts of armed forces, police and urban services; in other words, physical locations (which may be mobile). Secondly, electronically supported first-line security professionals who can serve as situation-driven and task/mission-specific information and command nodes. Critical factors include information exchange between public and private security parties[26], the reliability and timeliness of the information flow, the organization of the access to information (see also key focus area 12), and, most importantly, the way in which the information flows are used to improve the information position and obtain a high-quality image of the environment. The starting point for information management in any domain is clearly: defining the terminology. In the long term, certainly as we develop towards Web 3.0 applications, working on real-time, interoperable and structured data will be an essential element of key focus areas 10, 11 and 12.

11 Identification and prediction of irregular behaviour

We need to be better capable of identifying and predicting the behaviour of individuals and groups or trends. This key focus area concerns the use of big data and data mining techniques to identify irregular, undesired and/or prohibited behaviour, and using this to predict future criminal or hostile conduct. This knowledge can then become a foundation for preventing undesired and prohibited behaviour or for intervening at an early stage to prevent escalation.
The trend in the development of this specific form of pattern recognition in human behaviour is moving towards real-time multisensor information in combination with information from open, proprietary and third-party information systems and databases. There are currently a number of trials underway in local field labs.In shopping areas, leisure zones and at events, monitors are detecting and identifying irregularities in the movements among the public, so they can focus their actions and responses on them.

12 Establishing and guaranteeing –digital- identity

Of persons: linking digital and physical identification, fighting fraud and identity theft (including digital and financial data) on the internet. Of institutions and their products and services: monitoring, transparency, review, legislation and regulations. Of ‘things’: authentication of sender and receiver in automatic processes. Of important information: this requires a model to enable the identification or reconstruction of the way in which an original piece of data is successively augmented, altered, used, etc. – in short, a model of the life cycle of the data in question.

Theme 5 – **Observation with unmanned systems**

Observation with unmanned systems

Progressing computerization and automation is helping to increase the effectiveness and control the cost of long-term or ongoing routine tasks. This theme addresses a broad range of monitoring, surveillance and detection tasks using unmanned systems, from long-term, long-distance and stand-off on the one hand to real-time, up-close and short-term on the other. Here, civil/military cooperation is also called for.

Military UAVs (unmanned aerial vehicles, or 'drones') are already being used for civil tasks such as providing aerial views in hazardous situations like natural disasters and major fires, as well as other specialized observation situations like mapping large crime scenes. Here, like many other potential partnership areas, an important motivation is that combining efforts can achieve advantages of scale, both in terms of efficiency advantages and quality gains. These advantages could potentially be achieved across the entire process: vision, regulation, defining requirements, development and testing, acquisition, infrastructure, maintenance and operational use of unmanned aerial systems. Recently, an existing partnership was intensified in the preparations for the Nuclear Security Summit 2014, a project investigating detection and intervention potential. One pragmatic reason for the police forces to seek cooperation with the military is that there are military regulations, but as yet no civil regulatory framework, to govern the use of UAVs.

Security organizations will want to, and need to, take maximum advantage of commercial developments in the field of unmanned aerial platforms and systems. Under legislative and regulatory pressure, the reliability and safety of commercially available UAVs will be improving rapidly.[27] The military will want to stay ahead of the curve on certain aspects, acting as 'smart specifier,' and potentially 'smart developer' – things like securing communication with the platforms and integrating advanced sensor payloads and processing and interpreting multisensor information in creating a common operational picture. Police forces can have a role in promoting developments in this area by including innovative components in their acquisition projects. In both cases, knowledge of the rapidly changing market in relation to the organization's own needs is required (acting as 'smart buyer'). Both parties are also concerned with UAVs as a threat. This refers to both criminal and hostile use, as well as the security aspects of UAV hobbyists.

Innovation key focus areas:

13 Vision and concept development for operations with unmanned sensor platforms

This means the development of operational scenarios, doctrine development, etc., both individually and collectively. This will dictate requirements for innovation, not only oriented towards platforms and systems, but also the ultimate use of the sensor data. This last issue touches on Theme 4: Action-oriented information provision.
One important point of attention is the relationship to and/or integration with the manned and unmanned aviation sector.

14 Operational autonomy of UAVs

There is a distinct need for maximum autonomy of unmanned aerial platforms, particularly for the long-term observation application. This is relevant not only to simple platforms, but also to the transfer (in time and/or space) of platforms and systems.

Theme 6 – **Process innovation in and between professional organizations**

Process innovation in and between professional organizations

The security professional is confronted in a number of ways by a world in flux and a dynamic, complex environment in which to act. The tasks of the job are, on the one hand, increasingly constrained by limiting conditions, but also offer increasing capabilities thanks to advances on the technological front. And of course, the working methods involve more and more network interdependencies.

This has consequences for all human resource aspects: competence profiles, recruitment and selection, education, training, practice, physical and mental capacity, specialized development processes for tasks and missions, team composition, etc. Above all, this dynamic demands an operational mindset on the part of organizations and the professional: Performing optimally in actual operations has to be the primary consideration in the design of processes and structures.

> *'The events happening every day, both nationally and internationally, prove that ongoing development and innovation in the field of security is a necessity.'*[28] Laetitia Griffith

An important subtheme is more efficient and more effective training and practice by cooperating security professionals from all types of auxiliary services, in partnership with private security companies as required. This refers to complex situations that necessitate multidisciplinary and multilevel cooperation. Complicating factors can be aspects such as violence and escalation of violence, application of new techniques, procedures and doctrines, or conflicts between ethics and effectiveness. Many relevant scenarios are not suitable for to testing in practice, and must be simulated in some way. Serious gaming and applied gaming technologies and resources may, in many cases, be the answer, provided they can be adequately validated. This may involve organic training and practice in more or less standard situations, or might be preparation for a specific mission. Outside of the training context, gaming technologies have the potential to help answer questions about the distribution of responsibilities in the event of incidents. One likely potential application would be to 'game' the themes or scenarios from the annual National Risk Evaluation specifically on this aspect.

Innovation key focus areas:

15 Integrated action with heterogeneous teams

Here, human competences and technological support come together. This pertains to structural, organic cooperation and incidental, interpersonal connections between professionals, as well as between professionals and the public. All this takes place in acute operational situations or in long-term processes, in most cases with advanced technological resources, sometimes under primitive and rugged conditions. Often, pressure and stress are major components. The individual professional encounters this during the course of his/her career, in a specific function and in some cases even within a timeframe of weeks. What innovations can contribute to a better team result at the level of the individual, the team and the supporting environment? The 'teaming' of human and intelligent machine on a basis of mutual trust will become important. What shape will this take?

16 Connecting real world and virtual environment

Particularly in the case of mission preparation, it is important to provide the participants in a serious game with a virtual environment that adequately reflects the reality. Of course, the technology must first answer to the didactic objectives, but in many cases a high level of realism is desired. Depending on the level of the game, this may require that a physical situation (for example, a building layout) must be rendered in 3D very quickly, that the actual profiles of persons involved in the situation are immediately available, etc. This area can have direct links to key focus area 2. Validation is important.

‘The Ministry of Security and Justice is highly concerned with innovation. In the security field, we are seeing more and more examples of new products emerging from the partnership between business, government and universities.’[29] Ivo Opstelten

3 – Innovation investments and returns

The National Innovation Agenda for Security (NIAS) is the result of a process of interaction with the most important stakeholders in the security domain. As a logical outcome of this interaction and the commitment it involves, the stakeholder parties try to match their own innovation agendas with the national agenda. This is the crux of the NIAS: triple-helix parties in the national security cluster need to form consortia around the innovations defined in the agenda, to leverage their individual contributions towards achieving them. The table in section 3.1 sets out some starting points for these coalitions.

Like any investment, an investment in innovation is made with a view to future returns. And like any investment, there is always an element of risk: not all investments pay off. Businesses are more willing to bear this risk when they know there is a real market for the products and services that the innovation will produce. This is the reason why the NIAS puts its emphasis on articulating, combining and highlighting the demand. An important step towards this is making the connection between the NIAS and the procurement and acquisition agendas of the parties in the security domain with the biggest demands.

Section 3.2 offers a first step towards doing so. The Hague Security Delta (HSD) supports the development of a national procurement agenda to serve alongside the NIAS in 2016 as a roadmap for the process of innovation and economic development.

3.1 Innovation investments in a coalition context

The table on page 28-32 represents a crucial element in the transition from an innovation agenda on paper to an agenda that is coming to life andis really making a difference by being put into practice. It makes the connection between innovation key focus areas and the parties with an interest in investing to make them happen. In most cases, these connections are bringing together the demand and the supply. The parties listed in the table have a sense of responsibility for achieving the innovation key focus area in question. To that end they contribute their own resources, such as budget, capacity, knowledge, access, networks and testing functionality.
The parties will develop action plans for each individual innovation key focus area. The advisable approach is to determine, at the start of an innovation process, which party will be contributing what, when, why, and how, what coordination structures between the parties will be needed, and what clauses will govern them.
Parties on the demand side, for example, can commit by explicitly stating that the lessons learned in the innovation process (for example, from testing in experimental fields/ living labs, etc.) will be factored into the drafting of specifications in relevant acquisition and procurement processes. This does not imply forced sourcing, but rather effective utilization by all relevant parties of the insights gained in the innovation process.
Organisations on the supply side commit to risk-bearing investment, but may also commit to a form of technology and knowledge-sharing with other parties in the coalition, addressing issues such as intellectual property.

'Although innovation is the core business of companies and educational institutions, a driving role of government is vital.'[30] Kees Verhoeven

Past experiences have taught us that the effectiveness of a coalition formed to develop, apply and market innovations depends very strongly on a leading party. In the table, virtually any innovation key focus area has at least one lead party, which takes on the responsibility for getting the formation of the coalition happening and developing an action plan. This is also the organisation that generally coordinates the cooperation. Ideally, there will be a triple-helix structure for every key focus area, with at least one sponsor or client from the public sector and a triple-helix supervisory group, or 'community of practice.'

In the process of coalition-building and developing the action plan, the innovation key focus area will be refined and given a focus reflecting the specific concerns, stakes and strengths of the coalition partners. Note that it is also possible for a key focus area to attract multiple coalitions. This is unavoidable, and entirely justifiable. The NIAS is more of a catalyst than an instruction manual, and in that sense can be just as useful piggyback on existing initiatives as it is as a guideline for forming new ones. In all cases, the important thing is the broader goal: societal and economic value creation.

Innovation key focus areas

	Innovation key focus area	Lead parties[31]	Partners/potential partners	Running initiatives and other considerations
1	**Management of demand articulation: 'one government'**	NCTV (National Coordinator for Security and Counterterrorism) ('Safe [through] innovation' programme)	*Regular partners of NCTV on this key focus area:* AIVD (General Intelligence and Security Service) Ministry of Defence (MIVD and Royal Marechaussee) National Police Force Police Academy IFV (Institute for Physical Safety) Security Regions Netherlands Forensics Institute RIVM (National Institute of Public Health and Environmental Protection) GHOR (Regional Medical Assistance Organization) Public Prosecutions Department Ministry of Finance (Tax and Customs Administration, FIOD, Customs Authorities, General Inspection Service) Ministry of Social Affairs (SIOD) Ministry of Infrastructure and Environment (ILT) *Other partners:* Municipalities (G4/G32) DITSS TS&S	• The development of the national security cluster HSD serves as an important base. • Running NCTV initiatives: Financing 10 to 15 projects conducted by the public security partners, ideally in cooperation with companies and knowledge institutions. The coordinated supply of input for the Horizon 2020 work programme Secure Societies for 2016 and facilitating consortium-building for submitters to the work programme 2015. The performance and financing of the Small Business Innovation Research programme 'protection against unmanned mobile systems.' Organizing and financing the Security Innovation Competition 2015. Cataloguing new issues among the security partners and contributing this information to NIAS 2015 and subsequent versions. • Articulation of security issues of organizations not identified in this overview and of the critical infrastructure (such as the transport sector with secure lane), security expertise centres (such as CCV/EVPT) must be given attention in this key focus area. Knowledge development in this area is needed; Safety Valley in cooperation with Nyenrode is also willing to participate. The security workshop method as applied by DITSS is well-suited for use within this theme.
2	**Learning from incidents and drills**	Haaglanden Security Region	Police Academy Ministry of Defence Haaglanden Security Region The Hague University of Applied Sciences RIVM TNO (Netherlands Organization for Applied Scientific Research) Twijnstra & Gudde DITSS TS&S	• The Institute for Physical Safety (IFV), based on its statutory task, under the framework of the Council for Security's Strategic Agenda, works together with the National Academy for Crisis Control, on developing programmes for employees in the security regions in areas such as crisis control. • 7th Framework Programme, DRIVER (Driving Innovation in Crisis Management for European Resilience) crisis management demonstration project, a collaboration between Haaglanden Security Region, TNO and E-Semble in a broad European consortium. • RIVM would like to use its knowledge base (public health) and position to play a co-leading and supporting role. • RIVM is developing an evaluation framework assessment strategy for chemical incidents in the form of an app for hazardous materials specialists. In 2015, with involvement of IFV, the Security Regions and GHOR, RIVM will be launching a Root Cause Analysis to gain better and deeper insight into 'what goes wrong during incidents, and how to learn from it.' • Real-time information project for Security Region Central-West-Brabant. • Smart Cities Roadmap

	Innovation key focus area	Lead parties[31]	Partners/potential partners	Running initiatives and other considerations
3	**Value creation in triple-helix innovation**	National Security Cluster HSD Municipality of The Hague	All partners involved in HSD RIVM The Hague University of Applied SciencesofSTNO	All partners involved in HSD are highly involved in this theme; examples of initiatives: • *Living labs in The Hague region, for example International Zone, CSI The Hague, testbeds ENCS and the HSD innovation houses.* • Initiatives and projects with TS&S (for example, Safety Field lab) and DITSS (for example, Stratumseind Eindhoven). • RIVM would like to act as supporter, but cannot contribute financially. • Development of HSD's international dimension is seen as extremely important; TNO wants to make an explicit contribution to this, including in the EU networks in which TNO is active.
4	**Social innovation and self-organizing capacity**	TS&S DITSS Municipality of The Hague	National Police Force Security Region Rotterdam-Rijnmond and Zeeland The Hague University of Applied Sciences (HHS) RIVM TNO TU Eindhoven Tilburg University	• A non-exhaustive list of initiatives and developments: Burgernet Amber Alert and SOS Alarm (public) and Live View (companies, private security), cooperation in the community 'know your neighbours,' project idea BART (Burger Alert Real Time) as part of the Road Map Smart City of The Hague, Cyber Community Protection Network – CyCopNet (in concept phase), Resilient Deltas in Zeeland, Safety Valley cooperation. With DITSS: Public Reporting System Challenge 'reducing unnecessary fire alarms.' Social design; gaming for safe internet use, light for behavioural influence, safety experience in tunnels. Risk Factory with TS&S. • RIVM is interested in the use of recorded material of members of the public- citizens who, using their own devices (such as smartphones) make assessments of disasters and incidents- and the significance of this data for first responders; fast detection of agents, interpretation and validation of this data and communication. The development of data and fake data can be useful for drills.
5	**Awareness: perception versus reality**	TS&S	National Police Force The Hague University of Applied Sciences (HHS) University of Twente TNO	• The Hague Showcase Secure Netherlands(a consortium of HCSS, T-Xchange, TNO, Capgemini). • In cooperation with the The Hague University of Applied Sciences , Siemens has developed a 3D-printed bridge that can be used to demonstrate the impact of a hack in bridge control or bridge control security. This bridge will be given a place on the HSD Campus.
6	***Security by design in urban facilities and at events***	DITSS Municipality of The Hague	TU Eindhoven Trigion TNO Tilburg University InnovationQuarter Municipalities (G4/G32) Future Events	• A non-exhaustive summary of developments: Broad-spectrum area security International Zone, phase 1 (TNO, Thales). Designing out crime (Stratumseind Eindhoven), Fastlane, anomaly detection, Business park Loven Tilburg, safety and community (IC3Media, VCS) Civil sensed city, civilian involvement (DITSS). Philips is active in this area, particularly on the influence of light, sound and odour on security and the perception of security (involvement through DITSS). • This key focus area requires the involvement of a system integrator, for example municipal event security services. Future Events wants to play a role here as national public-private event platform.

	Innovation key focus area	Lead parties[31]	Partners/potential partners	Running initiatives and other considerations
7	**Identification and definition of 'critical'**	KPN	TNO Siemens University of Twente	• Here, KPN experiences an important issue for the interface between policymaker and implementers in the critical infrastructure and the development of a shared perspective on the cyber aspect within the critical infrastructure.
8	***Cyber security 'Internet of Things'***	Siemens KPN	NCTV National Cyber Security Council (NCSC) Capgemini TNO ENCS[32] University of Twente DITSS Fox-IT	• A non-exhaustive summary of developments: Testbed for energy infrastructure and smart grids. Testbed for water sector and other sectors, planning phase (ENCS). Trainings for Industrial Control Systems Security, Project Cyber Attack Detector (TNO, Fox-IT). Demand-driven programme in Cyber Security Top Sectors HTSM looks at security by design for ICT-based crucial infrastructure. The Peseta project relates to the digital exchange of bank statement information. Relevant actors include the Social Affairs and Employment Inspectorate, FIOD, Living Environment and Transport Inspectorate, NVWA, Royal Marechaussee and the National Police Internal Investigations Department. • An important issue for KPN here is the development of secure networks and monitoring (sensing/scada). • The NCTV (Cyber Security Council and the National Cyber Security Center) is contributing to this theme with knowledge and consultancy as this theme is further developed. Possibilities here include an innovation case into technological detection capability to reduce failure and sabotage of communicating systems without human intervention ('kill switches').
9	**Chain approach to cyber security**	Fox-IT Thales Capgemini KPN The Hague University of Applied Sciences	NCTV/NCSC Cyber Security Academy TNO DITSS Siemens InnovationQuarter	• A non-exhaustive summary of facilities and developments: Cyber Security Lab TNO, National Cyber Security Centre (NCSC). Demand-driven programme for Safe Society – topic cyber security (TNO) and Demand-driven programme for Cyber Security (TNO). Help for online safety at home and on mobile device, including internet banking, resilience to cyber bullying (including through gaming). Example: Sweety (Dutch design award 2014). Top Sectors HTSM examines how the cyber security status of the Dutch critical infrastructure can be catalogued according to a uniform standard (DeMoS: Detection, Monitoring and Situational Awareness). There is a wide range of SCADA and ICS issues to be resolved. • The Hague University of Applied Sciences may be willing to participate in the achievement of this key focus area in a lead role, based on a jointly developed action plan. • NCTV has an active interest in this theme, and also sees considerable opportunities for companies in it (e.g. Shell, Tennet). NCTV actively encourages the private initiative for security innovation in this theme.

	Innovation key focus area	Lead parties[31]	Partners/potential partners	Running initiatives and other considerations
10	**Networked information at interchanges**	KPN iCOPP ENAI	National Police Force Thales Capgemini TS&S DITSS Siemens TNO Axis-communications Conseillers en Gestion et Informatique (CGI) Municipality of The Hague	• A non-exhaustive summary of developments and initiatives: The Regional Monitoring Area South-East-Brabant. cooperation in TS&S context; Twente Experimental Command, Control and Communication Centre for Secure Environments (Tech4se), University of Twente/Center for Telematics and Information, the concept for the emergency centre of the future (CO24). International Zone (The Hague), common operational picture (iCOPP, ENAI). • Important aspects for KPN within this theme are: monitoring and secure networks. • Setting up pre-competitive experimental environments, for example in the fields of real-time intelligence, cyber and emergency centres is called for; TNO wants to be an advocate here. • TNO is active in the theme of real-time intelligence, and is working on tools and concepts for intelligence tasks.
11	**Identification and prediction of deviant behaviour**	Capgemini KPN DITSS	TNO NFI TS&S University of Twente InnovationQuarter National Police Force	• A critical factor in the recognition of deviant behaviour is the reduction of false negatives and false positives to a minimum. Privacy, ethical and legal aspects are essential considerations in this theme. • A non-exhaustive summary of initiatives: Automatic video analysis (TNO). Video content analysis (DITSS). Digital forensics in the cloud (national police force, NFI). Digital forensic accountancy (ACM, AFM, DNB). Developments in Twente (TS&S, Tec4se and CO24). PiD project Beware (Trigion). Anomaly detection (DITSS). KPN is very interested in aspects of situational awareness.
12	**Establishing and guaranteeing–digital–identity**	Authasas KPN	TNO Fox-IT TU Delft TU Eindhoven NFI TS&S DITSS University of Twente InnovationQuarter	• An important facet within this key focus area is the design of trust, privacy and security in the complex public-private linked information flows of the internet world. • A non-exhaustive summary of initiatives and developments: Encryption techniques, Leiden-Delft-Erasmus (LDE) Center for Safety and Security. A variety of initiatives at TS&S and DITSS (NXP, FIDO, Tec4se, CO24, BRP-project, VX company forensics recognition & individualisation). • NCTV sees online identity management as an important challenge with a great deal of economic potential for innovations in this area. This theme should place a strong emphasis on the consumer perspective: trust in transactions on the internet, safe websites.

	Innovation key focus area	Lead parties[31]	Partners/potential partners	Running initiatives and other considerations
13	**Vision and concept development for operations with unmanned sensor platforms**	Ministry of Defence	TNO National Police Force National Air and Space Laboratory (NLR) Fire Service Netherlands RIVM University of Twente TS&S	• A non-exhaustive list of initiatives and developments: PiD project RAEBELL (feasibility study of low-level airspace surveillance). Measurement of particles in smoke plumes and radioactive clouds using unmanned aerial vehicles (RIVM with NCTV).Training, testing and experimenting with unmanned aerial vehicles (TS&S).
14	**Operational autonomy of UAVs**	Aerialtronics	TU Delft Ministry of Defence National Police Force Thales Nederland Business Line Above Water Systems NLR TNO University of Twente	• NCTV considers this theme important and, after specification of this theme into approach, goals and results, will determine its involvement in this theme.
15	**Integrated action with heterogeneous teams**		National Police Force Twijnstra Gudde TNO TS&S	• A non-exhaustive summary of initiatives, developments and facilities: Secure Port role-play (TNO, Leiden University, Cap Gemini). TNO is active in the field of large-scale cooperation (including civil/military) in disasters and crises. PiD project Stepping Stones for Safety and Security: continuous learning tracks in security training programmes (ROC Mondriaan, The Hague University of Applied Sciences, Trigion). TS&S has the ambition to set up the European Safety & Security Center on the former Twente Air Field. TS&S is active in the field of technology-enhanced learning/virtual training. Troned[33] and the Riskfactory offer a variety of physical and virtual infrastructures for Education, Training, Practice, Testing, Evaluation and Learning. The TS&S Safety Field lab offers a location and theoretical and practical expertise for development and testing of the functioning of heterogeneous teams and virtual/mixed reality training. This facility can also be engaged for key focus area 16.
16	**Linking current reality – virtual environment**	Thales/T-Xchange TS&S KPN	National Police Force TNO Trigion E-Semble DITSS Municipality of The Hague	• T-Xchange (Thales) is involved in four project proposals within Horizon 2020 and two calls within the Twente Security Region (including FCT-7-2014, law enforcement capabilities, pan-European platform for serious gaming and training). • KPN is very interested in aspects of situational awareness. • The municipality of the Hague wishes to play a facilitating role on this key focus area. • A non-exhaustive summary of developments and initiatives: Area Development Twente (Thales), The Hague Showcase Secure Netherlands (The Hague Centre for Strategic Studies (HCSS), T-Xchange, TNO, Capgemini), PiD project Close Protection Serious Gaming (TU-Delft, E-semble), Mayor Game IFV (T-Xchange), Safe Internet Use home and mobile (DITSS), Cyber Incident Experience (TNO/Fox-IT).

3.2 Linking NIAS and procurement agendas

Connection between the NIAS and the procurement agendas of the major parties on the demand side is an essential element for the societal and economic value creation. This can be a complex challenge in the horizontally and vertically layered security structures. Public investment in security happens at all levels of government, within departments and between departments, and in some cases in public-private partnerships. Additionally, there are the investments that are made in private firms, primarily in the critical sectors, sometimes beyond the view of government.

> *'Good security policy has to be broad-spectrum, cost-conscious and modern, and based on a short, medium and long-term vision. In today's financial climate we have no choice but to work with each other, not only as departments but also within the 'golden triangle' of government, industry and knowledge institutions.'*[34] Ivo Opstelten

We estimate the economic value of the investments that follow from the NIAS at some three to five billion euros for the coming 10 years, if we assume an equipment replacement quote of 3-5% of government expenditures. These investments must not only have a societal return (making the Netherlands secure at an acceptable cost), but also generate economic revenues from utilizing the export potential of the implemented solutions. This has the best potential to be successful when investments in innovation are aligned with or succeeded by investments in products and services.

As we have taken the future procurement agenda into account in this NIAS, much the same, the procurement processes should take into account and use the practical experience and insights obtained from an innovation-oriented preliminary process or precompetitive phases of development (see also section 4.2).

Focus points[35] for security investments	Major planned and expected investment and procurement programmes
Mobile communication (C2000 successor)	From secure speech and data to broadband (streaming video, cloud functions), utilization of LTE, Information-driven Operations 2.0. Required investments > €100 million.
Vehicle C3I	Improvement of officer on duty situational awareness, Sight programme, Information-driven Operations 2.0, digital mobile emergency response meeting. Required investments > €100 million.
Situational awareness officer on duty	Mobile, linked, real-time. Required investments €25-100 million.
Emergency centres	From 25 to 10 (11), emergency centre of the future, National Crisis Management Systems 2.0 (LCMS 2.0), link Internal Security Organisation - External Security Organisation (IBO-EBO), link Departmental Coordination Centres, Shared Security Operations Centre International Zone The Hague. Required investments €25-100 million.
Emergency and crisis networks	Modernization and capacity expansion emergency net, Netherlands Armed Forces Integrated Network (NAFIN), LCMS 2.0. Required investments €25-100 million
Drones	Operational engagement of robots, monitoring of low and micro airspace. Follow-up project Raebell (feasibility study of low-level airspace surveillance). Required investments €5-25 million.
Cyber	Preventive, active defensive and offensive capabilities. Test facility 2.0 (in development). Required investments €25-100 million
Equipping first responders	Smart functional uniforms, non-lethal weapons, Information-driven. Action 2.0, LCMS 2.0. Required investments > €100 million.
Urban facilities	Smart City programmes. Required investments > €100 million.
HSD as national security innovation facility	Facilitate incubator for national security innovation cluster (based on key focus areas in the agenda) in the geographic centres The Hague, Twente and Brabant.

‘Security involves many aspects that have to be considered in interconnection with each other. The Dutch security sector could be doing a lot more of this than it currently is. In terms of funding and results, there is still a lot to be gained.’[17] Henk Geveke

4 – The NIAS in a broader perspective

We explicitly frame the NIAS in the context of societal and economic challenges, with innovation as the most important resource for taking on these challenges. The aspects and trends we describe in this chapter address this in a broader context. This can help create a clearer picture of the specific agenda given in chapter 2 and its link to the investments described in chapter 3.

4.1 National Security working procedure

The NIAS is entirely compatible with the National Security working procedure as developed interdepartmentally under the coordination of the Ministry of Security and Justice (previously, this was the responsibility of the Ministry of the Interior and Kingdom Relations; see Figure 1). The NIAS can be a tool for generating the content of the third process block: Follow-up, by developing innovative solutions for the Capacity Need.

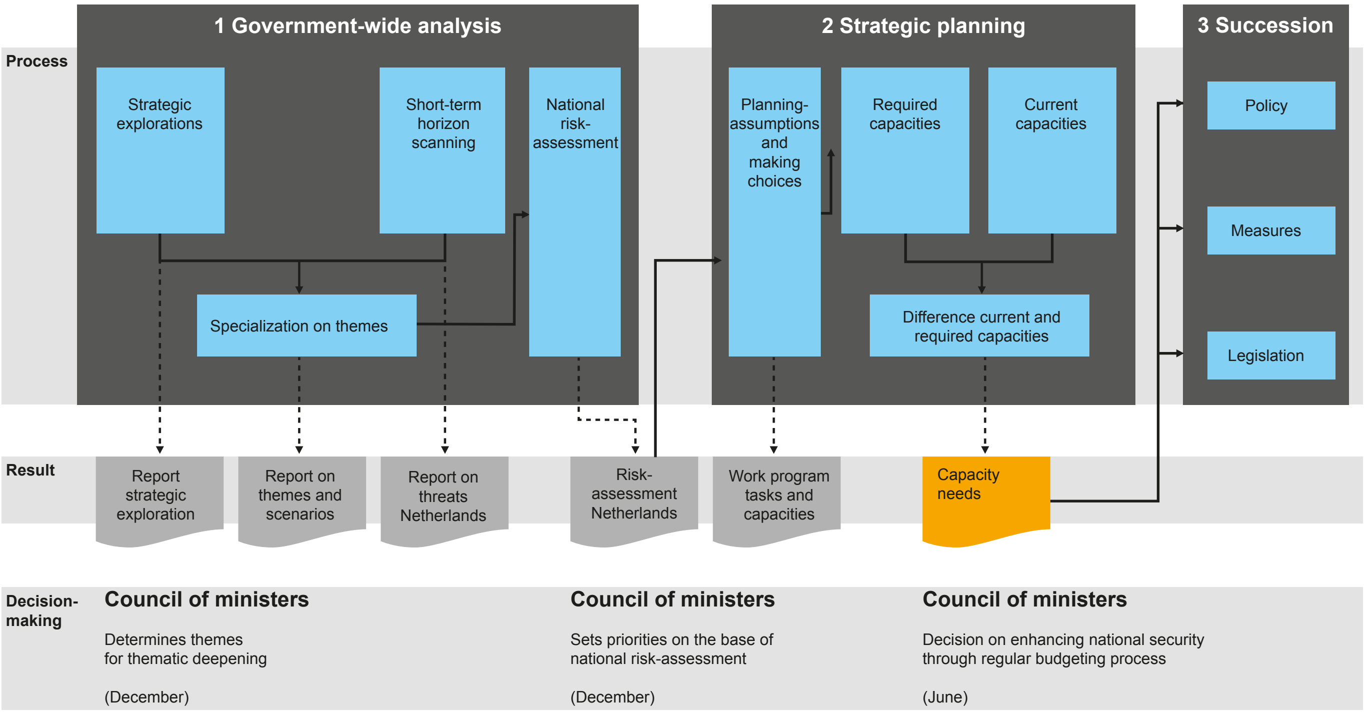
An important component of the National Security working procedure is the annual National Risk Assessment (NRA). The NRA provides and up-to-date overview of risks and threats to national security, and their potential impact. The NRA is the most comprehensive analysis of its kind, and has the most support, due to the government-wide involvement and increasing contributions from the vital sectors. Emerging new threats or shifts in the risk profile can lead to a demand for new or different capacities, which in turn lead to emerging innovation needs. Consequently, the NRA can be a source of valuable input for the NIAS. By the same token, the NIAS can be a step in the actual process of follow-up by channelling the development of capacities.

4.2 Investments in security

A requirement for making the NIAS a success is connecting the innovation agenda with the procurement and acquisition agendas of the national, regional and local governments with public and private operational services, as well as with the semi-public and private parties in the most important vital sectors:

- Energy: electricity grid administrator, gas grid administrators, energy suppliers.
- Telecommunication and ICT: telecom operators.
- Water: drinking water companies, surface water management, regional water authorities.
- Transport: mainports Schiphol and the Port of Rotterdam.
- Financial infrastructure: banks and insurance companies.

Figuur 1: Werkwijze Nationale Veiligheid overheidsbreed



1 Government-wide analysis
2 Strategic planning
3 Succession
Process
Strategic explorations
Short-term horizon scanning
National risk-assessment
Specialization on themes
Planning-assumptions and making choices
Required capacities
Current capacities
Difference current and required capacities
Policy
Measures
Legislation
Result
Report strategic exploration
Report on themes and scenarios
Report on threats Netherlands
Risk-assessment Netherlands
Work program tasks and capacities
Capacity needs
Decision-making
Council of ministers
Determines themes for thematic deepening
(December)
Council of ministers
Sets priorities on the base of national risk-assessment
(December)
Council of ministers
Decision on enhancing national security through regular budgeting process
(June)

Note: the Council of Ministers is informed and/or asked to make a decision twice a year (June and December)

This also includes the public-private approach to urban security: events, public safety, quality of life in communities. Examples of initiatives in the area of procurement and investment are:

- the Ministry of Economic Affairs' Procurement Innovation Urgency programme, intended to devote 2.5% of the relevant government procurement volume to innovation;
- the government-wide Small Business Innovation Research (SBIR), a method for developing innovative solutions for societal problems;
- the Security Innovation Competition (SIC), in cooperation and under the coordination of the ministries of Defence and Security & Justice
- the way in which the Ministry of Defence plays a stimulating role in innovation, with such tools as launching customership.[36]

To take one example, the Dutch Institute for Technology, Safety and Security (DITSS) has had positive experiences with regional security workshops and field labs for developing innovative security solutions. Such initiatives in the procurement and acquisition processes call for similar creativity.

Public-private partnership in an innovation and experimentation phase preceding a tendering process is extremely desirable in the security domain, particularly because so many products and services in the security market are relatively complex and specific. Without the knowledge and expertise of the partners and practical experience in the preliminary process, it is difficult for the requisitioner to define and appraise the desired or required innovation. The result is tenders geared for the lowest price, which are not particularly future-oriented. Another risk to be avoided is excluding companies involved in the preliminary process from participating in the tender.[37] Procurement and acquisition processes should be designed to guarantee objectivity but also encourage innovative bids. Setting up pre-competitive experimental environments, for example on aspects such as real-time intelligence, cyber security and the emergency centre domain, is recommended.

> *'It is the state, not the private sector, that is truly driving technological innovation.'*[38] Mariana Mazzucato

'Public enterprise' is not only necessary for the continuity of public-private partnership in the process from innovation to acquisition or procurement, but also because there are fundamental differences in pace between innovation and regulations. There are two potential solutions. On the one hand, it can be helpful to incorporate aspects such as regulations, privacy, ethics and governance issues at an early stage in innovation processes.

On the other hand, the legislator must allow for and utilize as much flexibility as possible. Temporary exemptions can offer the necessary freedom to experiment with innovative approaches. This helps when it then comes to formulating operationally relevant and enforceable legislation, especially in fast-moving areas such as the cyber domain, forensics, or the use of UAVs. It is striking to note that the focus and urgency attracted by high-profile events, for instance the recent Nuclear Security Summit in March 2014 in The Hague, often lead to creative solutions that are otherwise very difficult to accomplish. In combination with a focused budget, this can create a dynamic that leads to good process, chain and product innovations. Comparable experiences on a smaller scale can be found in the field labs for areas such as event security. The flexibility that this has proven to offer should be hard-wired into the system.

Sharing development and testing facilities should be a specific point of attention. Examples include the Twente Safety Campus, consisting of the Troned training facility, the Risk Factory and the Safety Field lab, the emergency and monitoring centres in Brabant, and the cyber testing facilities at The Hague. These are often expensive and difficult to make profitable due to their low capacity utilisation/ occupancy rate. Here, pre-competitive cooperation is not only feasible, but often necessary from an economic perspective. Shared investment and management need not exclude separate use.

4.3 Administrative complexity and control at system level

In the Dutch security market, the government not only defines policy, but as security provider is also the biggest party on the demand side. At the same time, the public sector is strongly layered, both horizontally and vertically, with a decentralized organization. We see a high administrative burden in a complex governance structure.

Crisis management in the Netherlands is, generally, simple in design: the party responsible for a policy area or chains within is also responsible for managing a crisis in that area. But the intricacy of the delegated responsibilities make the reality more complex, because the larger the incident, the more policy areas or separate chains are affected. There are over 50 separate chains, each with their own areas of authority. As a result, we frequently see in practice complicated coordination issues between the many different responsibilities.[39]
This complexity is further increased because each chain is organized in its own way. The result is that decentralized measures in one chain must be coordinated with central measures in another.

Cooperative form	Collective decision making	Patterns of Interaction	Distribution of Information
Network	not explicit, self-allocated, dynamic	unlimited, as required	all available and relevant information is accessible
Joint	joint processes and shared plans	broad and significant	broad, across areas collaborative areas/functions
Coordination	coordinated processes and linked plans	limited and focused	specific, on coordinated areas/ functions
De-conflicted	established constraints	very limited, sharply focused	additional information about constraints and interfaces
None	none	none	completely operationally oriented

In other words, the tasks, responsibilities and authorities (TRAs) are highly compartmentalized as compared to a reality in which these compartments are far from relevant. The TRAs of many processes or incidents are distributed among many different players, but because of this many of them turn out to go to no one. Here, 'strategic paralysis' becomes a risk: everyone understands that something has to happen, but no one is willing, able or in a position to take the lead. This applies not only to operational situations, but also to innovations that cut across chains, as well as innovations at the system level.

In practice, we observe a need for a 'system integrator,' a party to oversee the innovation of the total security landscape of the Netherlands and take the lead in the processes designed to result in cooperation. In the first paragraph of the foreword to the National Security Strategy document from 2007, then-Prime Minister Balkenende wrote: 'The authority for strengthening national security lies in the hands of government.' That may take the form of coordination and facilitating or guidance and control, but in practice usually means a certain balance in between.
To give an idea, we present in the table above the development steps that NATO distinguishes in its 'network-enabled action' process.[40] Although this model is principally used for operational cooperation, it can also be applied to cooperation in innovation processes.

4.4 Top sector policy and the Security and ICT roadmaps

The triple-helix approach underlying the NIAS is fully in line with the general policy of the Ministry of Economic Affairs (EA). The top sector policy emphasizes the importance of robust innovation for the earning capacity of our economy. In the evolution of this policy, EA expressed the desire to better link the top sectors with societal challenges, in line with the recommendations of the AWT (Advisory Council for Science, Technology and Innovation) and the WRR (Academic Council for Government Policy)[41] and the European policy on the 'grand challenges'.[42]

The top sector policy sets out commitments on how industry, government, universities and research centres must cooperate on knowledge and innovation, as set out in 'innovation contracts.' For example, the innovation contract for the 'Top Sector Theme Societal Security' states, among others: 'Societal security is an area that by definition involves the triple helix. Because on issues of societal security, the requisitioners (demand-side parties) are government parties, there has historically been ample cooperation with knowledge institutions and the private sector. The theme of societal security offers incentives to achieve crossovers, in order to have government act as lead customer or to purchase innovative products.'[43]

The top sector High Tech Systems and Materials (HTSM) defines the roadmap HTSM Security,[44] which identifies the following 'priority areas for application and technological challenge':

- **System of systems**
  The evolution to a networked security domain requires that new technologies and ICT networks evolve together into robust system-of-systems solutions.
  Management of this evolution must involve the complete value chain: vendors of components, system integrators, knowledge institutions and end users.
- **Cyber security**
  The ever-increasing impact of ICT on society increases the importance of cyber resilience and fighting cyber crime. The growing chain dependence of interconnected ICT systems demands new concepts. A large knowledge reservoir is already available, and the subject is very urgent.
- **Sensors**
  Information is vital for effective security. Both active and passive sensor technologies are relevant. There are very promising developments in the field of intelligent sensors and self-learning systems

The top sector-spanning ICT roadmap[45] is also of major importance, in part due to the following themes:

- **ICT you can count on**
  With attention to safe and reliable infrastructure, and privacy and e-identity issues.
- **ICT systems for monitoring and control**
  Focus in part on sensor-based surveillance, large-scale communication between sensor networks, and linking of heterogeneous sensor networks.
- **Data, data, data**
  Innovative data management must interpret the hidden gems within large data sets. Heterogeneous data from multiple sources demands new ways of detecting trends.

Alongside HTSM, the top sectors Water, Logistics and Energy have obvious interfaces with the security domain.
For the Creative Industry, Agriculture & Food, and Chemistry, security is at least a point of attention. Organizations in these sectors often have an interest in cyber security from the perspective of operational continuity and customer protection, a reliable –digital- identity, and learning from incidents and disasters. In practice, successful innovations in the security domain are often tied to crossovers between top sectors.

4.5 Towards a learning economy

'The biggest way to (...) increase the responsiveness of the Dutch economy is to promote knowledge circulation,' states the WRR in its report Towards a learning economy. In its recommendations, the WRR notes that this goes beyond promoting a knowledge economy.
While the desire for a knowledge economy puts a high priority on generating new knowledge, promoting knowledge circulation is about better using existing knowledge. Developing new knowledge does, of course, remain important, but beyond this, it places much more attention on mobilizing and applying the ideas and technology offered by other industries, sectors or countries.
This requires a capacity for absorption: 'the ability to identify, receive, and proficiently use new knowledge and existing knowledge available elsewhere.'

To achieve knowledge circulation, the mobilization and application of ideas and technologies across the boundaries of sectors, industries or countries, the WRR makes recommendations for increasing human capital and augmenting knowledge infrastructure and knowledge institutions. In its response to the WRR recommendations[46], the government refers to HSD as one of the 'strengths of today that can become the foundation for the strengths of 20 years from now': 'The Hague Security Delta gives the Netherlands the in-house knowledge to answer to the rising worldwide demand for solutions to security issues, for example in the cyber security area.' The national security cluster HSD is also a platform for knowledge circulation.

As the cabinet formulates, 'Within security policy, knowledge circulation is promoted by enhancing cooperation between companies and knowledge institutions and better coordinating research agendas to the issues facing society.' This last point is, for the security domain, precisely the aim the NIAS intends to address.

4.6 Smart Industry

We are currently in the midst of the fourth Industrial Revolution. This presents significant opportunities. A number of parties have taken the initiative, dubbed 'Smart Industry,' to put this subject high on the Dutch national agenda, following the example of Germany's large-scale Industry 4.0 programme.[47]
Its central tenet is the understanding that we live in a world in which everything is connected with everything else. ICT converges with sensor technology and robotics to create an internet of things composed of cyber-physical systems. Following this development, manufacturers are opening the software side of their systems to customers and suppliers. This is making the broad spectrum of specializations easily connectable to each other, to boost the rate of innovation and answer to the needs and desires of end users (even in real time). It is now becoming economically viable to market small runs of products and services, or even unique, customer-specific products and services. It should be noted that 'openness' does not only refer to an open development process of a system, but also openness in the use, maintenance and other phases of the life cycle. From a technical standpoint, this is all entirely feasible; open standards, for example, are for the largest part available.
The issue is primarily the reluctance of the manufacturing industry to work together in open environments; when anyone can take part in the open knowledge and run off with it, and many parties (including end users) can take a hand in programming a given application, the industry must rethink its business models and redesign aspects like liability, continuity and intellectual property.

This trend has an impact on the NIAS for a number of reasons, as a general framework as well as, potentially, for the definition of the innovation key focus areas:

- Although developments are described as the fourth Industrial Revolution, the reality is a type of evolution. The social and process innovation needed, not to mention the legislative framework, will not emerge from one day to the next. HSD, the national security cluster, is the preeminent platform on which the security sector can develop towards the Smart Industry concept faster than elsewhere, even if still in fits and starts. In coalitions of the 'willing and able' of triple-helix partners, technology development can be pursued in an open and trusted environment within partnerships and new business models that are compatible with the Smart Industry paradigm.

- A significant trend is that functionality is increasingly being built into software, and moving away from hardware. This approach is most successful in an environment in which everything can be connected to everything and everyone through the internet. Take the example of the success of the software-centric iPhone and Android smartphones, contrasted with the relative failure of the hardware-centric BlackBerry. In the security domain, too, this trend has dramatic consequences for private business models, the entire lifecycle of systems, and the relationship between product and consumers or between security professionals and the public, and as such fundamentally relates to existing economic models and social structures.
- The vulnerability of cyber-physical systems to cyber attacks demands much greater attention. On the interface of the virtual and physical worlds, cyber attacks can have a very direct disruptive influence on society, and even be life-threatening. This is still insufficiently acknowledged and addressed, both by the government and the private sector.

4.7 The European 'grand challenge' Secure Societies

While the Dutch top sector policy is a structure built around economic sectors, the European Union opts for a primary organization based on six 'grand challenges.' One of these is Secure Societies – Protecting Freedom And Security Of Europe And Its Citizens. In the context of the NIAS, it is relevant to consider how this challenge relates to the major European research programme Horizon 2020. The research for Secure Societies is focused on developing new knowledge and technology for combating crime and terrorism, crisis management, and the external dimension of security. The research is civil in nature, but also addresses technologies that can be used in both the civil and military domains ('dual-use' technologies).

The research for Secure Societies[48] addresses a great number of relevant issues, including:[49] for instance, as stated in the introduction of the workprogramme 2014-2015, fighting crime, illegal trafficking and terrorism, protection of critical infrastructure, forensics and use of big data, identity recognition, enhancing cyber security, improving resilience to crisis and disasters, protection of –digital- identity to prevent digital abuse and legal and privacy issues in the information age. These issues are also addressed in the NIAS.

Correlating national innovation key focus areas with European security research, as shown on the following pages, is good for two reasons. Firstly, it establishes their relationship to the international agenda, with both a societal and economic dimension. This puts the focus in the right place.
Secondly, European research funding can be leverage for obtaining contributions from national parties. This builds towards reaching a critical mass.[50]

Advancement of the international dimension of HSD is, therefore, of critical importance. Participation of HSD partners in EU networks and awareness-raising in Brussels therefore offers clear added value for HSD.

> *'Financing research and innovation is essential for the future of Europe, because it contributes to growth, employment and a better quality of life. In view of their qualities, Dutch researchers have every opportunity in Horizon 2020, which has the goal of uniting the top researchers from universities, research institutes and industry in Europe on revolutionary projects.'*[51] Robert-Jan Smits

The European Commission adjusts the direction of the research areas for each two-year working programme based on ongoing developments. The table on the following pages connects the innovation key focus areas of the NIAS with the Secure Societies 2014-2015 working programme.

Secure Societies Topics	Relevant innovation key focus areas
Topic Disaster-resilience **Part I. Crisis management**	• Management of demand articulation: ‘one government’ • Learning from incidents and drills • Value creation in triple-helix innovation • Social innovation and self-organizing capacity • Awareness: perception versus reality • Networked information at interchanges • Vision and concept development for operations with unmanned sensor platforms • Integrated action with heterogeneous teams • Connecting real world and virtual environment
Topic Disaster-resilience **Part II. Disaster Resilience & Climate Change**	• Value creation in triple-helix innovation • Security by design in urban facilities and at events
Topic Disaster-resilience **Part III. Critical Infrastructure Protection**	• Security by design in urban facilities and at events • Identification and definition of ‘critical’
Topic Disaster-resilience **Part IV. Communication technologies and interoperability**	• Chain approach to cyber security • Networked information at interchanges • Establishing and guaranteeing –digital– identity
Topic Disaster-resilience **Part V. Ethical/Societal Dimension**	• Social innovation and self-organizing capacity • Awareness: perception versus reality • Identification and definition of ‘critical’
Topic Fight against crime and Terrorism, **Part I. Forensics**	• Chain approach to cyber security • Establishing and guaranteeing –digital– identity • Identification and prediction of deviant behaviour
Topic Fight against crime and Terrorism **Part II. Law enforcement capabilities**	• Chain approach to cyber security • Establishing and guaranteeing –digital– identity • Vision and concept development for operations with unmanned sensor platforms • Operational autonomy of UAVs • Connecting real world and virtual environment
Topic Fight against crime and Terrorism **Part III. Urban security**	• Security by design in urban facilities and at events
Topic Fight against crime and Terrorism **Part IV. Ethical/Societal Dimension**	• Social innovation and self-organizing capacity • Awareness: perception versus reality
Topic Border Security and External Security **Part I. Maritime Border Security**	• Identification and prediction of deviant behaviour • Vision and concept development for operations with unmanned sensor platforms • Operational autonomy of UAVs
Topic Border Security and External Security **Part II. Border crossing points**	• Identification and prediction of deviant behaviour • Establishing and guaranteeing –digital– identity
Topic Border Security and External Security **Part III. Supply Chain Security**	• Establishing and guaranteeing –digital– identity
Topic Border Security and External Security **Part IV. External Security**	• Networked information at interchanges • Identification and prediction of deviant behaviour • Establishing and guaranteeing –digital- identity • Connecting real world and virtual environment

Secure Societies Topics	Relevant innovation key focus areas
Topic Border Security and External Security **Part V. Ethical/Societal Dimension**	
Topic Digital Security **Cyber security, Privacy and Trust**	• Social innovation and self-organizing capacity • Awareness: perception versus reality • Identification and definition of ‘critical’ • Cyber security of the internet of things • Chain approach to cyber security • Networked information at interchanges • Identification and prediction of deviant behaviour • Establishing and guaranteeing –digital- identity

‘For me, HSD has succeeded when we are known as the place to be for security and innovation in Europe; a kind of Silicon Valley that national and international governments, companies and knowledge institutions want to be a part of. To make this happen, the NIAS is an essential tool at a critical moment.’[53] Ida Haisma

5 – Final considerations

By presenting themes and key focus areas, the National Innovation Agenda for Security 2015 is a source of direction, focus and content. The key focus areas require further development, and new points of emphasis may emerge in the process. The NIAS is not an instruction manual, but something to get cooperation processes between triple helix partners going.

It is essential for parties to identify with the key focus areas, start working with them, fine-tune them if and where required, and to go on to achieve them. All triple helix partners, the government at all levels and in all relevant capacities and roles, the businesses and the knowledge institutions, have an important responsibility here

The next steps are:
Form consortia around the themes and key focus areas for the continued programming, unite the extraordinary knowledge and expertise available in the triple helix, and build a national procurement and acquisition agenda around them. Establish a working method that functions across the chains, allowing partners to work together on new solutions and towards building a security delta of international stature. Cooperation within the triple helix is not new, but cooperation of this size and scope is, and will require a lot of effort from the partners. Openness, trust and respect for each other's interests are crucial requirements for forming 'coalitions of the willing and able'. Looking from the perspective of 'Netherlands, Inc.' is important in order to be able to complete successful innovation programs that perform well both economically and for society.

'Compliments to HSD for creating an innovation agenda in which parties from business, government and knowledge institutions come together.'[52] Laetitia Griffith

The NIAS is facilitated, managed and periodically updated by the national security cluster HSD. The NIAS is an element of the HSD strategy, and as such the advancement and updating of the NIAS is a recurring activity for the national security cluster HSD.

Appendix 1 – **Discussion partners interviewed in consultation and review rounds**

Surname		First name	Position and organization	Spoken to on
Akerboom		Erik	Secretary-General, Ministry of Defence	5 Oct 2014
Asten	van	Arian	Department head and MT member, Netherlands Forensics Institute	2 Feb 2014
Barthel		Jan-Piet	Programme Manager Cyber Security NWO IPP VV	20 Oct 2014
Berg	van den	Steffie	Innovation Staff, NCTV	11 Mar 2014 17 Jun 2014
Berlo	van	Marcel	Lead, Innovation House Urban Security and senior business developer, Defence Safety and Security TNO	10 Apr 2014
Birkhoff		Kees	Senior vice-president and manager Public Sector, Capgemini Netherlands, and HSD Board Member	26 Jun 2014
Brabander-Ypes	de	Heleen	Senior advisor, industrial participation, Ministry of Economic Affairs	13 May 2014 12 Jun 2014
Brandt		Dick	Chairperson, IIP VV	20 Oct 2014
Brouwers		Joep	Deputy Director, Brainport	21 Aug 2014
Brouwers		Juul	Communication Manager, cyber security, IIPVV/NWO	20 Oct 2014
Bruinen	den	Joris	Secretary of the HSD Board	11 Jun 2014
Burger		Helen	Information Services Advisor, Strategy, Policy & Management, National Police Force	05 Mar 2014
Casparie		Stefanie	Coordinating Advisor, Innovation, National Police Force	24 Jul 2014 25 Aug 2014
Cloo		Pieter	Secretary-General, Ministry of Security & Justice	26 Aug 2014
D'Huy		Kees	Director of Smart Cities, TNO and HSD Executive Committee member	06 Mar 2014
Dobbenberg		Ernst	Head of Knowledge and Innovation Cluster, Defence Staff	2 Feb 2014
Don		Bert	Strategic Advisor National Security TNO	15 Apr 2014 3 Sep 2014
Drift	van der	Reinier	Director, Authasas	20 Oct 2014
Engelshoven	van	Ingrid	Alderman of Knowledge Economy, International, Youth and Education, and first Deputy Mayor, municipality of The Hague	27 Oct 2014
Essen	van	Henk	Member of police force management team, National Police Force	15 Jul 2014
Freriks		Leo	Lead, Innovation House, Critical Infrastructure and City account manager, Siemens	8 Jul 2014
Frinking		Erik	Lead, Innovation House, National Security and Director of the strategic futures programme HCSS	18 Mar 2014
Genet		Louis	Programme Director, International City The Hague	23 Jun 2014 10 Sept 2014
Gieling		Albert	Section head, Fire Services Twente	11 Sept 2014
Gooijer		Dennis	Director, KPN Critical Communications	15 Oct 2014
Haas	de	Robin	Cyber Security and Defence Safety & Security TNO	30 Jun 2014
Haisma		Ida	Executive Director HSD	9 Jul 2014
Heer	de	Johan	Director, T-Xchange	11 Sept 2014
IJzinga		Niek	Lead, Innovation House, Cyber Security and senior manager, Cyber Risk Services, Deloitte	30 Jun 2014
Jacobs		Gabriele	Associate professor EUR/RSM, Centre of Excellence, Public Safety Management	22 May 2014
Jansen		Frederik	Programme Manager, Twente Safety and Security (TS&S) and member of HSD Advisory Council	11 Sept 2014
Keuning		Jelle	Director of R&D, Ministry of Defence	20 Oct 2014 5 Oct 2014
Klaasen		But	Programme Manager ,Innovation, NCTV, Ministry of Security and Justice and member of HSD Advisory Council	2 Jul 2014 26 Aug 2014
Klaauw	van der	Marcel	Senior programme coordinator , Investments, International City, Municipality of The Hague	10 Sept 2014
Kool		Henk	(Former) Alderman of Economy, Municipality of The Hague	26 Mar 2014

Surname		First name	Position and organization	Spoken to on
Leeuwen	van	Michel	Department Head within board of Cyber Security NCTV	27 Mar 2014
Luijken	van	Coen	Director of Business Development, Trigion	8 Jul 2014
Marel	van der	Menno	Director of Fox-IT and member of HSD Board	8 Jul 2014
Mennen		Marcel	General secretary, analyst network, national security and department manager, RIVM	8 Jul 2014
Noordanus		Peter	Mayor of Tilburg and member of HSD Board	29 Sept 2014
Oosterom		Louis	Lead, Innovation House, Critical Infrastructure	16 Apr 2014
Otten		Jan	Strategic advisor, Dutch Institute for Technology, Safety and Security (DITSS) and member of HSD Advisory Council	7 May 2014
Oudsten	den	Peter	Mayor of Enschede, chairperson of Security Region Twente and member of HSD Board	30 Jun 2014
Putten	van	Marieke	Programme Manager, Procurement Innovation Urgent, Ministry of Economic Affairs	19 Mar 2014
Remerie		Max	Director of Business Development, Siemens, and member of HSD Executive Committee	8 Jul 2014
Reyn		Sebastian	Director of Integral Policy, Ministry of Defence	20 Oct 2014
Sluijter		Guus	Director, Dutch Institute for Technology, Safety and Security (DITSS)	2 Jul 2014 9 Sep 2014
Smits		Aart Jan	Chairperson, Roadmap Security HTMS and member of HSD Executive Committee	8 Jul 2014 21 Oct 2014
Tossings		Maarten	Director of Policy, Ministry of Defence	3 Mar 2014
Vet	van der	Hans	Deputy Director of Public Order and Security, Municipality of The Hague	4 Jul 2014
Vianen	van	John	Director, Business Market, KPN, and member of HSD Board	15 Oct 2014
Vroet	de	Stephanie	Innovation Staff, NCTV	11 Mar 2014 17 Jun 2014
Wiebes		Mark	Police commissioner and innovation manager, National Unit, National Police Force	1 Jul 2014
Wijk	de	Rob	General Director, HSD	18 Jun 2014
Wissen	van	Jaap	Security and Innovation Advisor, Directorate-General for Public Works and Water Management	20 Oct 2014
Zaal		Leo	Director, Institute for Physical Safety	8 Jul 2014
Zorko		Patricia	Head of Operations, National Police Force, and member of HSD Advisory Council	27 Aug 2014
Zunderd	van	Peter	Head of National Operational Staff, National Police Force, and member of HSD Advisory Council	21 Jul 2014

Appendix 2 – **Documents consulted**

There are a large number of documents describing the desired or planned innovation programmes in the security domain. Some take innovation as their central topic, while others address it in a chapter of a broader vision or plan document. The sources also differ in their emphasis on the phases in the process from idea to product. The Security and Justice innovation agenda from the ministry of S&J, for example, focuses primarily on the start phase of innovation processes, where creative new ideas must be developed that have the potential to lead to forward leaps in innovation, but which also frequently get bogged down somewhere in the process. Although there is a clear overlap in thematic areas with the NIAS. The NIAS places its emphasis on the use of innovation, where promising innovative ideas are converted into solutions with market potential.

There are, in short, many possible perspectives, all of which were considered in the selection of innovation key focus areas for the NIAS. By holding interviews with various parties, we have tried to show the link the NIAS has with the various documents as clearly as possible. We beg the reader's understanding for the fact that the vast number of sources and perspectives makes it impossible to adequately acknowledge every single contribution with a direct reference in the text, and hope that this summary of documents consulted, will be adequate for the purpose.

Europe

European Commission. (June 2013). *EU-research for a secure society, security research projects under the 7th framework.*

Fraunhofer Institute for Technological Trend Analysis. (2013). *Evaluation of critical and emerging security technologies for the elaboration of a strategic research agenda. Etcetera.*

Horizon 2020 Work Programme 2014-2015. (December 2013). *Secure Societies - Protecting freedom and security of Europa and its citizens.*

Netherlands Organisation for Scientific Research. (November 2013). *Call for proposals Cybersecurity 2014.*

National/Kingdom level

Bruggen slaan. October 2012. Regeerakkoord VVD-PvdA, Coalition agreement of the political parties VVD and PvdA.

Capgemini.(2013). *Trends in Veiligheid 2013, Een digitale samenleving kan niet zonder digitale veiligheid.*

Capgemini Consulting. (April 2014). *Trends in veiligheid 2014, digitale ketensamenwerking.*

National Security Think Tank. (January 2009). *Verantwoordelijkheid voor Nationale Veiligheid.*

National Security Think Tank. (June 2013). *Veiligheid als gedeeld belang.*

DigiSafe Cyber Security Centre. (May 2014). *The hub for cyber security professionals.*

Horizon 2020 Guide. October 2014. Calls 2014-2015. *Rijksdienst voor Ondernemend Nederland.*

ICT Innovation Platform "Veilig Verbonden" (September 2013). *National Cyber Security Research Agenda II.*

Ministry of Defence. (2011). *Strategische Kennis- en Innovatie Agenda (SKIA).*

Ministry of Defence. (February 2014). *Defensie Industrie Strategie.*

Ministry of Economic Affairs. (August 2013). *Programma Inkoop Innovatie Urgent, een ondernemender houding van de overheid.*

Ministry of Economic Affairs. (May 2012). *Samenvatting Innovatiecontract Topsector, thema maatschappelijke veiligheid.*

Ministry of Economic Affairs. (July 2013). Agentschap *NL, Strategisch aanvalsplan NL: Digital Gateway to Europa.*

Ministry of Economic Affairs. (July 2014). *Strategisch Kader TO2 federatie en het Strategisch Plan TNO 2015- 2018 en de kabinetsreactie daarop.*

Ministry of Infrastructure and Environment. (June 2012). *IenM maakt ruimte, strategische kennis- en innovatieagenda IenM 2012-2016.*

Ministry of Security & Justice. (2014). *Werken aan een veilige en rechtvaardige samenleving.*

Ministry of Security & Justice. (2014). *WODC, Onderzoeksprogramma 2014.*

Ministry of Security & Justice. (August 2013). *NCSC, Cybersecuritybeeld NL.*

Ministry of Security & Justice. (January 2014). *Jaarplan NCTV 2014.*

Ministry of Security & Justice. (March 2013). *Eenheid in Verscheidenheid.*

Ministry of Security & Justice. (May 2013). *Aanzet tot SKIA Ministerie VenJ. (unpublished)*

Ministry of Security & Justice. (October 2013). *National Cyber Security Strategy II, from awareness to capability.*

Ministry of Security & Justice. (October 2014). *Innovatieagenda VenJ (concept)*.

Ministry of Security & Justice. (September 2013). *Evaluatiecommissie Wet Veiligheidsregio's en het stelsel van Rampenbestrijding en Crisisbeheersing.*

Ministry of Security & Justice, NCTV. (November 2013). *Strategie Nationale Veiligheid.*

Ministry of Security & Justice, NCTV. (November 2013). *Voortgangsbrief Nationale Veiligheid.*

Ministry of Security & Justice, NCTV. (September 2013). *Trendrapportage Veilig door Innovatie, Agenda 2013.*

National police force. (December 2012). *Inrichtingsplan.*

National police force. (December 2012). *Realisatieplan.*

National police force. (January 2012). *Ontwerpplan Nationale Politie.*

National police force. (November 2011) *Police Academy, Strategische Onderzoeksagenda.*

Nederland Ondernemend Innovatieland. (June 2008). *Maatschappelijke Innovatie Agenda Veiligheid.*

OECD Directorate for science, technology and industry. (April 2014). *OECD review of the Netherlands' innovation policy, assessments and recommendations.*

Future of Technology Foundation. (May 2014). *Horizonscan 2050, anders kijken naar de toekomst.*

National Security Strategy. (October 2009). *Werken met scenario's, risicobeoordeling en capaciteiten.*

The Hague Security Delta. (October 2014). *Strategie en Urgentieprogramma.*

TNO. (April 2014). *Technologieverkenning Nationale Veiligheid.*

TNO. (August 2013). *Nationale Risico Beoordeling 2012.*

Detailed recommendations of administrative working group on supra-regional cooperation. (February 2013). *Eenheid in verscheidenheid.*

Advisory Council on Government Policy. (February 2014). *Naar een lerende economie, kabinetsreactie daarop.*

Advisory Council on Government Policy. (November 2011). *Evenwichtskunst, over de verdeling van verantwoordelijkheid voor fysieke veiligheid.*

Regional/Local level

Brainport 2020. (2011). *Top economy, smart society.*

Fire Service. (November 2012). *Strategisch Meerjaren Onderzoeks- en Innovatieprogramma Brandweer.*

Digitale Steden Agenda. (March 2013). *Convenant Smarter Cities.*

Dutch Institute of Technology, Safety and Security. (2014). *Business canvas model.*

ING. (September 2014). *Economisch bureau, na drie jaar weer groei voor Haagse economie.*

Roadmap, Smart City The Hague. (March 2014). *Samen naar een slimme stad.*

Council on Security. (February 2014). *Voorwaartse agenda.*

Council on Security. (January 2014). *Agenda van de Veiligheidsregio's.*

Council on Security. (January 2014). *Slotnotitie werkconferentie doorontwikkeling veiligheidsregio's.*

Council on Security. (June 2011). *Verbindende schakel in rampenbestrijding en crisisbeheersing.*

Council on Security. (May 2014). *Strategische agenda versterking veiligheidsregio's 2014-2016.*

Security Region Twente. (October 2012). *Beleidsplan Veiligheidsregio Twente 2013-2015.*

Industry

Hightech Systems and Materials. (31 May 2013). *Roadmap HTSM Security, revised version.*

Netherlands Enterprise Agency. (July 2008). *Innovatie Agenda Energie.*

Knowledge Institutions

Amsterdam Economic Board. (November 2011). *Kennis en Innovatie Agenda.*

Erasmus University /Rotterdam School of Management. (January 2014). *Center of Excellence for Public Safety Management.*

NFI. (February 2014). *Het Nederlands Forensisch Instituut, in feite het beste.*

Sentinels. (October 2012). *Onderzoeksprogramma gericht op verbetering van kennis over computer en netwerkveiligheid binnen Nederland.*

Technical University Delft. (April 2014). *De oplossing van de crisis kost niets, Manifest Nico Baken.*

Technical University Delft. (October 2014). *Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security.*

TNO. (2014). *Voortgangsrapportage 2013 TNO, Vraaggestuurd Programma Security (draft).*

TNO. (December 2011). *An integrated approach to national security.*

TNO. (December 2012). *Veiligheid schreeuwt om innovatie.*

TNO. (December 2013). *Advanced Risk Management.*

TNO. (February 2007). *De kracht van het Cyclische Concept.*

TNO. (September 2013). *Maatschappelijke Veiligheid.*

TNO. (September 2014). *Speurwerkprogramma 2015-2018.*

TNO. (September 2014). *Technologieradar Veiligheid t.b.v. NCTV en Nationale Politie.*

Appendix 3 – **Notes**

1 Ivo Opstelten, Minister of Security and Justice, in his address at the opening of the HSD Campus, 13 February 2014, rijksoverheid.nl.

2 Ivo Opstelten, Minister of Security and Justice, in his address at the ASIS Conference, 2 April 2014, World Forum The Hague, rijksoverheid.nl.

3 *Bruggen slaan*, the coalition agreement by the political parties VVD and PvdA, states: 'Security is one of the government's core tasks. The public has to be able to feel safe on the street and in the community. Police and the judicial authorities have to be able to act effectively and with authority… in the chain of criminal law… with special attention to…innovation' (p. 26).

4 Coalition agreement: 'The Netherlands' position in the top 5 most competitive economies has to be cemented and strengthened in the coming years. Our country is in an excellent starting position for this, with its innovative companies and excellent knowledge institutions, a robust governance… Can contribute significantly to reinforcing this position' (p. 8); 'Education and science in the Netherlands are of a high level, but our ambition goes further; we want to be among the top 5 in the world…' (p.16); 'Historically, the Netherlands has always been strongly internationally oriented... Dutch companies have significant interests abroad. Foreign policy is oriented towards promoting and protecting those interests, and furthers the international rule of law…' (p. 14); 'Europe is of major importance to our peace, security and prosperity, we earn our money from it; our jobs are to a large degree dependent on it…' (p. 13).

5 See 'De staat is de echte technologische vernieuwer', Het *Financieele Dagblad*, 6 February 2014.

6 Erik Akerboom, Secretary-General of the Ministry of Defence, in a meeting with the authors of the NIAS, 5 November 2014.

7 In this structure, the regions contribute individual strengths and key focus areas to the cluster, and thus working in complementary and distinct ways to jointly strive for value creation on the societal and economic fronts.

8 In practice, the contributions of the other triple helix partners are indispensable in defining the relevant needs.

9 The NIAS focuses more on the commercial application of innovative solutions than on conceptualizing or developing new ideas.

10 Menno van de Marel, CEO Fox-IT, 'Cybersecurity in het Regeerakkoord', Fox-IT.com, 14 September 2012.

11 Rob de Wijk, General Director HSD, *OndernemersClub*, RTL 7, 13 October 2014.

12 In some cases as an independent document, in others included in a general vision, strategy or positioning document.

13 Invitees to this administrative meeting were: the mayors of the municipalities of The Hague, Eindhoven, Tilburg, and Enschede, The Hague alderman for the Knowledge Economy, International, Youth and Education/first deputy mayor, the secretary-general of the Ministry of Security and Justice, the secretary-general of the Ministry of Defence, the National Coordinator for Security and Counterterrorism, the chief of the National Police Forces, the director-general for Business and Innovation of the Ministry of Economic Affairs, the chairperson of the Council on Security, the TNO managing director for security, the chairperson of the roadmap security HTSM, the chairpersons of the executive boards of Technical University Delft, Technical University Eindhoven and The Hague University of Applied Sciences , the deans of the universities of Twente, Tilburg and Leiden (Campus The Hague), the Director of HCSS, the chairperson of the NIDV, and the representatives/CEO's of KPN, Thales, Siemens, Capgemini, Trigion and Fox-IT on the HSD Board.

14 In the security domain, there are a number of interdependent chains and interconnected processes and structures that, taken collectively from a specific perspective, describe the security system as a whole.
Examples include the operational security chain: anticipation-prevention-preparation-suppression-follow up, the interconnected vital national interests of territorial security-economic security-ecological security-physical security-societal and political stability, the functional pillars police-fire department-GHOR (regional medical assistance organization)-public administration-armed forces, and the physical-virtual domains. The triple helix can, to a certain degree, be seen as another such chain. It is important to note here that a chain is only as strong as its weakest link. A critical function of the national security cluster and the NIAS is placing the individual links in their chain context in order to set innovation priorities that are both concrete and focused (at the link level) as contributions to resolving fundamental issues (at the chain or system level).

15 This criterion also ensures that we continue to build on existing strengths, because without this there is no way to build such an effective coalition.

16 This means the principal focus is on innovations in or after the proof of concept phase, and much less on innovations in earlier phases of development.

17 Henk Geveke, managing director Defence, Safety and Security TNO, at the presentation of the book *Veiligheid schreeuwt om innovatie*, tno.nl, 14 December 2012.

18 Laetitia Griffith, chairperson of the Dutch Security Sector, in a written response to the NIAS, 1 October 2014.

19 One good example is the international zone in which the municipality of The Hague commissioned a consortium of HSD partners to develop a schedule of requirements with several operational user organizations as part of the creation of a shared security operations centre.

20 See, for example, WRR, *Evenwichtskunst; over de verdeling van verantwoordelijkheid voor fysieke veiligheid*, 2011; National Security Think Tank, *Veiligheid als gedeeld belang*, 2013; NCTV, *Voortgangsbrief Nationale Veiligheid*, 8 November 2013.

21 This is extremely compatible with a number of developments, including initiatives in Twente such as *Secure Neighbourhoods, Community resilience, Civil participation in development of security-scenario's Smart connection and cooperation in training and crisiscommunication.*

22 National events like U-meet Cybersecurity and Alert Online contribute to this awareness.

23 See also key focus area 10.

24 NCTV, http://www.rijksoverheid.nl/vitale-sectoren.pdf

25 NCTV, *Tussen naïviteit en paranoia: nationale veiligheidsbelangen bij buitenlandse overnames en investeringen in vitale sectoren.* Working Group on Economic Security, final report, April 2014.

26 The National Police Force's programme *Sensing* is currently focused on linking information within the public services to make it easier to access. The expectation is that in the future, the images from professional private sources will also be linked to public sources. Emergency centres of security firms can then also play an important node function.

27 Many of the UAVs currently commercially available are technically being used illegally. The current lack of (law)enforcement will be increasingly unworkable as the projected growth in commercial and private use continues. Statutory safety requirements will have to be enforced more strictly and more effectively. The security specifications of commercial systems will then improve dramatically, potentially up to a level acceptable to the police and defence forces. Until then, 'individual' solutions will remain necessary.

28 Laetitia Griffith, chairperson of the Dutch Security Sector, in a written response to the NIAS, 1 October 2014.

29 Ivo Opstelten, Minister of Security and Justice, in a 3 October 2014 e-mail to HSD.

[30] Kees Verhoeven, Member of the Lower House of Parliament (D66), spokesperson for the Economy, in *Het Financieele Dagblad*, 14 October 2014.

[31] Organizations listed in this column with seats on the HSD Board have committed to being lead or co-lead on the specified key focus area.

[32] European Network for Cyber Security (ENCS), a network of Alliander, E.ON, KPN, Enexis, Westland Infra and DNV KEMA (members) and TNO, TU Delft, Applied Risk, Accenture and Wurldtech (partners), is dedicated to applied research, training, testing and consulting on the security of systems for industrial process control.

[33] TRONED, as shared facility/operational field lab, offers facilities for testing and experimentation with a range of technologies, such as RedSuit and UAVs. TRONED is also a partnership facility for discovering, developing and implementing new training concepts (serious games) and curricula in cooperation with a range of institutions, the Ministry of Defence, academies, universities of applied sciences and numerous technology firms such as Re-Lion, KITT-engineering, E-Semble, V-Step and T-Xchange.

[34] Ivo Opstelten, Minister of Security and Justice, at the presentation of the book *Veiligheid schreeuwt om innovatie*, tno.nl, 14 December 2012.

[35] Places, processes or domains where large-scale investments, crossover issues and innovation needs meet.

[36] Ministries of Defence and Economic Affairs, *Defensie Industrie Strategie*, December 2013.

[37] In theory, tendering rules allow for a certain amount of exclusivity that companies need, due to market failure in the security market, to make risk-bearing investments in innovation. This contingency has to be sought, used and justified both administratively and politically. One tool for doing so can be the new Defence and Security Contracting Act, which provides for a number of special tendering procedures that walk the line between fully ‘public’ tendering and the ‘Article 346’ tenders as described in the TFEU. The Defence and Security Contracting Act provides a structure that allows opportunities not possible under an ordinary tendering procedure, and is also Europe-proof, being that it is based on RI 2009/81. It would seem that the security domain has little to no awareness of these possibilities, so there are a number of new opportunities here.

[38] Mariana Mazzucato, professor of economics and innovation at the University of Sussex, *Het Financieele Dagblad*, 6 February 2014.

[39] Institute of Physical Safety, *Bestuurlijke Netwerkkaarten Crisisbeheersing*, 2013 (fifth printing).

[40] Adapted from NATO’s Network-Enabled Cooperation Maturity Model.

[41] Advisory Council for Science and Technology, *Waarde creëren uit maatschappelijke uitdagingen*, October 2013; Advisory Council on Government Policy, *Naar een lerende economie*, November 2013.

[42] ‘Grand challenges’ are the major challenges defined by the European Union and used as the premises for policy priorities, and feature in the innovation framework programme Horizon 2020. One of these grand challenges is Secure Societies.

[43] *Samenvatting innovatiecontract Topsector Thema Maatschappelijke Veiligheid*, May 2012.

[44] *Roadmap HTSM Security*, revised version, 31 May 2013.

[45] *Roadmap ICT for the Top Sectors*, 2012.

[46] Ministers of Economic Affairs and Education, Culture & Science, *Cabinet response to WRR report ‘Naar een lerende economie*’, 22 February 2014.

[47] FME, TNO, Ministry of Economic Affairs, VNO-/NCW and Chamber of Commerce, *Smart Industry. Dutch industry fit for the future*, April 2014.

[48] European Commission Decision C (2013)8631, *Horizon 2020 Work Programme 2014 – 2015. 14. Secure Societies – Protecting Freedom And Security Of Europe And Its Citizens*, 10 December 2013.

[49] The more monodisciplinary issues were not considered; see also the review framework.

[50] Note that Horizon 2020 is only one (although the largest) of many schemes that might possibly be tapped for budget. HSD maintains a list of financing instruments and provides assistance in accessing them.

[51] Robert-Jan Smits, Director-General for Research and Innovation, European Commission (Opportunities for NL in firstcalls Horizon 2020, 11 December 2013, rijksoverheid.nl).

[52] Laetitia Griffith, chairperson of the Dutch Security Sector, in a written response to the NIAS, 1 October 2014.

[53] Ida Haisma, Executive Director HSD, 28 October 2015.

Publication information
National Innovation Agenda for Security 2015
© 2014, The Hague Security Delta

A publication of
The Hague Security Delta
Wilhelmina van Pruisenweg 104
2595 AN The Hague
T +31 (0)70 3028180
info@thehaguesecuritydelta.com
www.thehaguesecuritydelta.com
@HSD_NL

Project management and authors
Peter Elias
Frank Bekkers

Design
Studio Koelewijn Brüggenwirth

Printing
Ando Graphic

Photography
Hilbert Krane
Nationale Politie
Aerialtronics
Third

We would like to express our gratitude to everyone involved in the production of this agenda, and in particular, to Nathalie Zeerleder for her administrative support.