

The Value of Cooperation

Innovation in Dutch Security in Perspective



The Value of Cooperation

Innovation in Dutch Security in Perspective

Foreword

The Netherlands is a country of contrasts. Small in size, yet it is the 24th largest economy in the world, and has the 18th highest GDP per capita income.¹ At the same time, the Netherlands is also among the most liberal social democracies in the world, ranking among the world's best 'global citizens'.² It is a society that has proven to be largely resilient in the face of security challenges—not just physical, but also social, economic and in cyber, to name a few. But this is no reason to become complacent. On the contrary: one of the key challenges we face now is how to prepare for the security risks of today and tomorrow whilst protecting the Dutch way of life: safe, secure, harmonious, and prosperous.

Meeting these challenges is not an easy task. First of all, it requires that we have a grasp of the broad spectrum of potential security risks—both nationally and internationally. It means that we recognise the various security concerns that citizens worry about, those that are visible and those that are less visible. Some of these concerns may very well extend beyond, and sometimes even contradict, traditional state security concerns. It also requires an appreciation of the capabilities that we already have, and the capabilities that we can and should further harness to safeguard our security.

The key to staying ahead of the curve in this regard is to make sure that we work together: business, citizens, civil society, knowledge institutes and the government at various levels.³ What is more, while security can be instrumental in safeguarding our prosperity, security innovation in itself can also be an engine for economic growth. This is where The Hague Security Delta, the national security cluster that promotes innovation and knowledge for security and economic development, comes in. As its 2014 annual report summarises: 'No innovation without knowledge, and no economic development without innovation.'⁴ Stimulating such innovation in the area of security through triple-helix cooperation constitutes HSD's core mission.

This report addresses some important questions: what is security, and which different dimensions can be distinguished? What are some key trends and risks that we face, and what is their likelihood of occurring? What means do we have available to face these risks, and, most importantly, what can HSD partners do to contribute to confronting the security challenges our country faces tomorrow? Hence, if the question is what you can do for our country, and what we can do together, this report will provide some useful guidance in that endeavour.

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

A Guide to the Report

The report is structured so as to achieve three objectives:

- 1 to introduce the reader to the security context in which HSD operates;
- 2 to provide an overview of where HSD stands and what its assets are; and
- 3 to show directions for development of the cluster and opportunities to reinforce its mission: to bring together triple-helix-partners with the aim to achieve synergies, bring economic benefits to the Netherlands as a hub for security innovation, and, ultimately, to generate security and economic benefits for society as a whole.

The first part of the report starts out by describing what is meant by security, how thinking about security has evolved, and how ever more vital aspects of our daily lives have become part of the security realm. It then briefly surveys some key themes of security, showing how they are interlinked. Subsequently, we survey how these various security themes are currently incorporated in our national security strategies, and reflect on the priorities that are set by the government, but also within civil society, the business world and among citizens.

The second part focuses on The Hague Security Delta: what makes it well-equipped to deal with the security challenges that were described in the first part? Where can it make the most meaningful contributions and produce the most value-added, and how is it positioning itself to capitalise on existing and potential opportunities? Subsequently, we investigate some of these opportunities by focusing on how other security clusters have evolved and by highlighting some innovation projects and initiatives that HSD partners and others are engaged in. Finally, some of the highest-potential projects are highlighted that can help consolidate or expand the reach of HSD, and help to improve security provision in a way that adds value to our economy and society alike.

The conclusion will recap the objectives of HSD and provide some highlights from its 2015 agenda.

Introduction

The Netherlands is, in many respects, one of the safest and most peaceful countries in the world. This is why security has traditionally not been a primary concern for the average Dutch citizen.⁵ Recent international developments, however, mark a departure from the past. Upheavals in the Middle East, the terrorist attacks in Paris, the resurgence of Russia and the shooting down of Malaysia Airlines flight 17 on July 17, 2014—killing 196 Dutch citizens on board—all contributed to this sea change. Where the crisis in Ukraine appeared at one time to be in ‘a far away country about which we know nothing’, it then tragically brought devastation to people across our country. If anything, such events remind us that we do not live on an island, and that the illusion that we are ‘safe behind our dykes’ definitively belongs to the past.

Apart from international events directly affecting Dutch security, there were plenty of security and safety issues of domestic origin that worried people in the past year: from the release of notorious convicts such as Volkert van der Graaf and Benno L., the explosion at Shell’s chemical plant in Moerdijk in June⁶, and the gas drilling-induced spike in earthquakes in Groningen. In cyberspace, attacks on networks of banks, theft of sensitive personal information, serious privacy intrusions as well as rumours of large scale foreign industrial espionage raised widespread societal concern.⁷

On top of this all, climate change continued to encroach upon the security agenda. Traditionally the focus lay on protection against rising surface water—sea, lakes, rivers. But the apparent increase of extreme weather events such as heavy rainfall or extreme heat is prompting a rethinking about how to absorb more sudden climate-related shocks. Attention is also shifting to the indirect security effects of climate change which run land degradation, changes in food and energy production and migration flows, to name a few.⁸ In sum, following a decade in which domestic safety and security topped the national agenda, the interconnectedness of domestic and international security is becoming clearer than ever before.

At the same time, the gap between perceptions and reality of security has been widening for some time now. For instance, while there has been a noticeable downward trend in the number of crimes reported between 2008 and 2012⁹, the general feeling of insecurity increased in that same period from 25% to 37%.¹⁰ Hence, a good dose of clear-headed realism is called for when making policy priorities relating to safety and security, and when deciding what innovations to invest in.

All of the above challenges require robust and above all concerted responses. As the largest security cluster in Europe, HSD aims to ‘develop and implement a long-term vision on integral security policy that serves societal security by looking ahead and anticipating new threats, and to link this vision at the appropriate levels to the national security agenda.’¹¹ HSD will thus be able to provide a substantial contribution to improving Dutch security, and to help push forward innovative security solutions here and abroad.

Table of Contents

Foreword	4
A Guide to the Report	6
Introduction	7
PART ONE: The Dutch Security Landscape: Trends, Threats and Thinking	11
1 What is Security?	
A Matter of Trust, Resilience and Economic Viability	13
1.1 Thematic Overview of Security Trends	14
1.1.1 Territorial Security	15
1.1.2 Physical Security and Safety	15
1.1.3 Societal Security	15
1.1.4 Economic Security	16
1.1.5 Environmental Security	16
1.1.6 Cyber Security	16
1.1.7 International Security	17
2 Consolidation of Security Policy: the Key National Strategies	19
2.1 National Security Strategy	19
2.2 International Security Strategy	19
2.3 Implementing Security Policies	20
3 Assessing Safety and Security: What Are the Issues, and What is Needed?	20
3.1 Some Key Government Studies Framing the Security Debate	20
3.2 Views from Parliament, Civil Society, and the Private Sector	23
3.3 Some Conclusions	28
PART TWO: HSD in the Security Landscape: Roles and Prospects	29
4 Aims and Strategies of HSD	31
4.1 Meeting Threats and Challenges: Shoring up Knowledge and Capacity	32
4.1.1 How to Prioritise	32
4.1.2 Where HSD can Contribute	33
4.2 The National Innovation Agenda for Security	35
5 Clusters Worldwide	37
5.1 HSD in a Comparative Perspective	37
5.2 A Typology of Clusters	42
5.3 Factors for Success	42
6 Innovation Projects and Financing Initiatives	45
6.1 The National Innovation Agenda for Security as Identification Tool	45
6.2 Implementing the NIAS: From Ideas through Investments to Social Impact	45
6.3 Projects in Security Innovation Linking to the NIAS	46
7 HSD Infographic	57
Conclusions	61

PART ONE —

The Dutch Security Landscape: Trends, Threats and Thinking

1 – What is Security? A Matter of Trust, Resilience and Economic Viability

In an ever more complex world, it becomes harder to say what security *is*. The first inclination is to think about security in the traditional, Hobbesian sense of the word: protection against physical harm. Today however, security is defined in much broader ways, essentially denoting the material and immaterial integrity of individual persons, groups or even the nation or society as a whole.¹²

Material and immaterial integrity refer to protection against physical harm, but also include protection of fundamental rights, socio-economic means and individual or collective identities. This broader definition also requires a more comprehensive approach where ensuring security is concerned. This is because the different kinds of security to be pursued can lead to conflicting priorities: for instance, protection against terrorism needs to be balanced against potential infringements of individual privacy.

A second issue is that complexity brings uncertainty, which affects our ability to prepare for security threats that we know. Some of the threats we face are intangible to some extent: how and when do we suffer the impact of climate change? When and how do we know whether our internet traffic is safe? This dilemma is spelt out in the illustration below.

To tackle these issues, we need to build a flexible toolbox of capabilities that help us prepare against known and unknown threats, irrespective of when they will arrive.

Finally, when it comes to providing security against all these different kinds of threats, it may not be easy to assign responsibilities or to make someone or an agency solely accountable. Threats to security materialise at different levels; they can sometimes be all but impossible to detect beforehand, or their scale can be beyond anyone's imagination. This is why it is important that both citizens and public authorities are equipped with a realistic perspective when it comes to thinking about security solutions.

Security policies are often crafted as remedies against infringements of security, rather than preconditions to safeguard security.¹³ In other words, they are more reactive

instead of anticipatory. But a secure society is not built on combating symptoms and threats, and needs to move towards thinking in terms of interests and how to prevent societal dislocation or breakdown, which is more cost-efficient in the process. In a recent report, The Netherlands Scientific Council for Government Policy recommends moving away from an 'incident reflex' induced approach towards a 'good governance' approach that emphasises the purpose of policies and how these could be best achieved.¹⁴ Simply put, when security becomes multi-faceted, responses need to be comprehensive, flexible, anticipatory and efforts need to be joint.

How is this to be achieved? The key lies in how security is conceived of, built on a basis of trust, resilience and economic viability. **Trust** refers to the fact that individuals can freely interact with one another without unduly needing to be concerned about unforeseen negative consequences of such interaction. In essence, trust provides the backbone of a society's fabric, and is a sine qua non for it to function. Indeed, society as such cannot exist in absence of trust that undergirds a commonly agreed set of values.

The second key element, **resilience**, refers to the ability of a society to bounce back from shocks to its fabric and to maintain or restore its basic structure *ex ante*.¹⁵ This ability depends to a great degree on how a society is structured (the strength of networks of cooperation), the levels of trust that are present, and the availability and organisation of the right capacities to deal with shocks to its security infrastructure, whether these are societal, economic, cyber-related or otherwise. Resilient societies have the right means in place to anticipate unforeseen threats in such a way that the basic fabric of society remains solid and functioning.

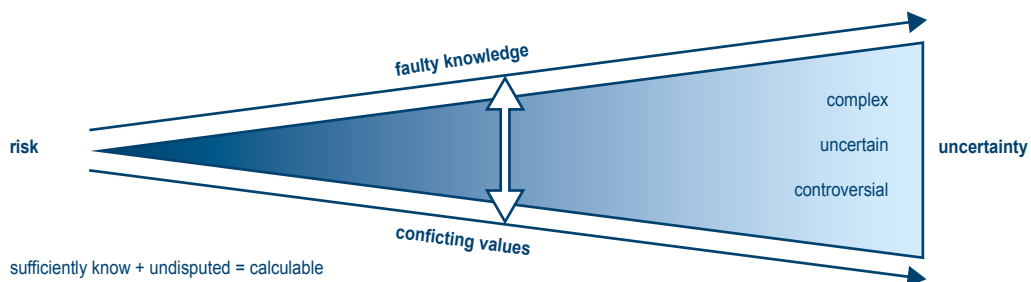


Figure 1: Risk-Uncertainty continuum. Source: WRR report, *Physical Safety*, p. 13



Economic viability addresses the need for a proper balance between the costs and benefits of security. When security becomes a broader term, and more complex and more difficult to frame in terms of risks and threats, it is easy to spend inordinately on implementing new security measures, or to increase capacities where their usefulness is as of yet uncertain. At the same time, economic viability also invites us to think about security not in terms of costs, but also in terms of benefits: for instance, more security helps to enhance prosperity, while an innovative security technology sector provides direct benefits to economic growth. The key to promoting economic viability lies in working together to achieve smart interaction between stakeholders.

Maintaining a secure society is thus not merely a matter of authorities protecting their citizens, but entails a collaborative effort requiring active cooperation from citizens, civil society and business as well. These efforts can differ depending

on the issue area, as is described below. Even so, in order to be able to respond adequately to changes in the security landscapes—say emerging threats or shifting priorities—a collective approach remains indispensable.

1.1 Thematic Overview of Security Trends

Based on the definition of security, seven thematic areas of security are distinguished¹⁶: territorial security, physical security, societal security, economic security, environmental security, cyber security and international security. Of course, in many ways there are overlaps between these dimensions—as is reflected in the work of HSD. The last dimension, international security, has been singled out here for the sake of highlighting Dutch peacekeeping and related operations and to suggest linkages between international security and domestic security.

1.1.1 Territorial security

Territorial security, a cornerstone of foreign policy, is understood to mean the protection of a country's territory against foreign interference. For many years, territorial security was considered more a theoretical than a real issue. Last year however, that dramatically changed. Russian incursions into Ukraine and veiled threats towards NATO member states have brought home the message that safe borders and the territorial integrity of Europe cannot be taken for granted. The advances of ISIS and the proclamation of the so-called khalifate not only reinforced that message, but also raised the spectre of potential for conflict spilling directly over our borders as a result of jihadi activity.¹⁷ Third, increasing migration to Europe from the global south also puts more pressure on our ability to control who crosses our borders.¹⁸ The key point here is that our territorial security does not stop at the borders with Germany and Belgium, but extends to the very borders of NATO alliance and EU territory, creating an obligation on the Netherlands and our defence forces to contribute to the defence of NATO/EU member states, whether in the Baltics, Turkey or elsewhere.¹⁹

For HSD partners, the angle to address challenges under this lead lie principally under 'national security' and 'forensics', for instance in addressing the need to be able to better monitor migrations flows, border controls, supporting intelligence operations (both domestically and abroad) and enhancing communications between law enforcement units.

1.1.2 Physical Security and Safety

Physical security and safety are for most citizens the most immediate concern. These include petty crime, burglaries or feelings of insecurity as a result of criminal activities such as local drug trading.²⁰ But lack of safety can also be a cause of physical harm, examples being incidents such as fires and traffic accidents, or weather and climate-related emergencies.²¹ Because of the generally dispersed nature of such incidents, the attention and urgency of policymakers is often relatively low for such kinds of security and safety issues.²² However, the number of related casualties are much higher than in any of the other areas mentioned above. In the case of climate-related emergencies, the impact can be catastrophic.

Physical security and safety issues cannot be considered in isolation, since they also affect socio-economic security, cyber security and societal security. For instance, elevated crime rates in particular neighbourhoods can affect prosperity and social capital.²³ Cyber theft of critical data could lead to physical harm if someone's steps could be traced by criminals. And societal security can be at stake if a local increase in crime rates deepens divisions in society. Safety issues can also have an impact in the security realm: for instance, if vital infrastructure fails due to issues in cyber transmission and control, this could have knock-on effect on traffic control.²⁴



Industrial zones may be more prone to fire hazards, and thus less desirable to live close to.

For HSD partners, addressing physical security and safety issues offers many opportunities for engagement: smarter methods for monitoring safety and security in public areas; reinforcing hard infrastructure to protect people and cities against the climate-change related weather events; or developing new methods for early warning and gauging public sentiment in particular neighbourhoods could provide opportunities that HSD partners could contribute to.

1.1.3 Societal Security

As a concept, societal security is still young, but its significance cannot be underestimated. In essence, societal security concerns reassurance about intangible things such as culture or identity, and thus touch on the very foundations of society. A common definition defines it as 'the ability of society to persist in its essential character under changing conditions and possible or actual threats.'²⁵ According to the ETTIS project, societal security has as its ultimate objective to ensure people a 'meaningful existence.'²⁶

More so than other thematic areas, societal security is very much a matter of perceptions and trust. As a rule, perceptions take facts as a reference point, but their significance and nature can be interpreted very differently depending on one's point of view.²⁷ As a result, fissures can emerge that can split societies or lead to fragmentation.²⁸ An example here could be immigration policies: some see these as beneficial and an economic necessity, while others see generous policies as a threat to core values of society.²⁹ The more societies are in flux, the more societal tensions can grow as uncertainty about security and about the future increase in various segments of society, in particular those that are socially weak or vulnerable.³⁰ Among the most serious threats to societal security today is jihadist ideas taking root in our societies and in European countries in general.³¹ Another potentially divisive development is rising inequality and decreasing social capital.³²

For HSD partners, opportunities would lie in supporting national and local authorities with cyber technology to monitor jihadist activity, or, in relation to urban security, to detect potentially adverse trends in society, for instance in identifying forms of radicalisation, or in monitoring neighbourhoods where social tensions are on the rise.

1.1.4 Economic Security

Economic security matters in different respects. First of all, economic security is about a country's security of critical supplies, such as energy and raw materials. The current crisis over Ukraine amply shows how this cannot be taken for granted today. Former EU Commission President Barroso underlined this point, saying that '[t]he Ukraine crisis confirms that it is in our own interest to (...) increas[e] our security of supply (...). It is vital for our prosperity, for our strength and our credibility.'³³ Secondly, economic security is about ensuring that economic growth matches the needs for socio-economic stability, that is, that people in need can be supported, and that there is a manageable level of inequality.³⁴ Thirdly, economic security concerns the physical protection of key economic assets, whether at home or abroad. Examples could be protecting airports, seaports, industrial installations and even ocean tankers.³⁵

For HSD partners, there would be a variety of ways in which to contribute to economic security. Given the business angle of HSD, such contributions could be extensive. Obvious angles include critical infrastructure, for instance in integrating energy preservation by design in developing smart city concepts, or through securing financial transactions systems and supporting law enforcement agencies in protecting key infrastructural assets.

1.1.5 Environmental Security

Environmental security concerns 'measures designed to provide safety from environmental dangers (including diseases) caused by natural or human processes due to ignorance, accident, mismanagement, or intentional activity.'³⁶ In the Dutch context, the most obvious connotation it evokes is keeping us safe against the dangers of rising sea levels and to protect us against river inundations. In that respect, it stresses the need for solid vital infrastructure, both physically and in cyberspace. However, environmental security also relates to finding a proper balance between economic growth, supplies of key goods (food, water, electricity and others) and livability. This thematic area also has a clear international dimension, both in terms of sharing best practices and technologies, as well as in achieving common environmental standards.

HSD partners can contribute to this area in various ways: from developing climate-change resilient critical infrastructure to cyber-based monitoring systems of protective infrastructure (dykes, barriers) including the use of UAVs to thinking through more environmentally friendly and efficient transportation infrastructures.

1.1.6 Cyber Security

The issue of cyber security rapidly captured the attention of policymakers and security specialists alike in recent years. Fast-paced technological developments often leave authorities scrambling to maintain a level of control over what is happening in cyberspace. The contrasts are stark: on the one hand, the world wide web is arguably the freest and most important platform of exchange in the world, yet the freedoms that it embodies also create massive risks for disruptions to society and the way we live now.³⁷ Security concerns in regards to cyber are not limited to hacking and spying, but also extend to use by criminal and terrorist organisations and the ability to disrupt vital infrastructure.³⁸ Another cause for concern is the fact that control over data distribution and storage can also have security implications. In some countries, this has been a reason for supporting initiatives to create home-grown data networks that are easier to control, and not to surrender control over data to foreign countries.³⁹ Given the multiplicity of issues that are affected by cyber, this will remain a key priority in the years to come.

On this issue, the government has drawn up a specific National Cyber Security Strategy (NCSS), which in many ways builds on the National Security Strategy. An updated second edition was released in late 2013 (NCSS2). The general approach of the NCSS2 is to seek to broaden the use of cyber communication in the Netherlands, and promote safe use of internet services. It also lays out some strategic focus areas, including risk analyses in conjunction with managers of critical infrastructure systems; more attention to cyber espionage (both for public and private interests); conducting a feasibility study on setting up private networks for better protection of vital infrastructure; enhancing civil-military cooperation; promoting security and privacy by design; and for the Netherlands to become a centre for expertise on international law and cyber security.

NCSS2 also identifies some key threats and challenges. Among the principal threats listed are cyber theft, cybercrime and cyber-espionage. Both states as well as private parties can be behind such threats.⁴⁰ Apart from the threats, some challenges are formulated based on future developments: the internet of things, the increasing capacity to store information (and the consequences thereof), as well as the greater risk of cyber attacks and the risks this involves given greater interwovenness between the civil and military domains. On the theme of cyber security, the government's ambition is for the Netherlands to remain a global leader. It strives for



the implementation of a full-fledged European cyber-strategy, and focus on the hosting of the fourth international Global Conference on Cyberspace (GCCS).⁴¹

Potential contributions to be made by HSD partners should help boost economic growth prospects.⁴² Cyber-based solutions can also help reduce resorting to the risk-regulation reflex by further developing homeostatic cyber solutions. Given the increasing reach of cyber and the potential for adverse use and abuse of IT infrastructure, the needs for added protection will only increase, whereby the robustness of cyber infrastructure systems can give an edge to Dutch businesses overall.

1.1.7 International Security

Finally, the Netherlands is also involved in international peace and security efforts elsewhere in the world. Some of these missions, such as the recent police training mission in Afghanistan, the anti-piracy mission off the coast of Somalia, the current deployment in Mali, or Dutch contributions to UN peacekeeping or OSCE monitoring have less of an immediate evident impact on security at home. However, the scourges that these missions are out to combat can also reach our own shores.⁴³ This is most evident where fighting terrorism or extremism is concerned. Engaging in international counterterrorism operations can be a double-edged sword, however. On the one hand, such operations, when effective, contribute to

our own security as they help pacify volatile regions of the world. On the other hand, engagement abroad can also lead to calls to commit terrorist acts in the Netherlands, for instance in the shape of jihadist attacks. Nevertheless, given the continuing and often increasing turbulence that the world is witnessing today, it is very likely that international engagement will remain necessary, and be expanded as well. It is therefore conceivable that in the coming year, demands for Dutch contributions to military operations worldwide will increase.⁴⁴

For HSD partners, contributions to international security efforts can be found in the areas of forensics, information technology and cyber-security where there could be opportunities to help information-gathering exercises, which become ever more central to peacekeeping efforts.



2 – Consolidation of Security Policy: the Key National Strategies

In view of the new security threats that we face as a society, the Dutch government adopted two security strategies, one focusing on national security; the other on international security. The National Security Strategy (NSS) proved to be instrumental in changing thinking about security in terms of interests rather than mere risks and threats, and triggered the drafting of more specific sectoral strategies, such as for cyber. Together, the security strategies provide a framework for organising the Dutch security infrastructure and to set policy priorities.

2.1 National Security Strategy

The **National Security Strategy** (Strategie Nationale Veiligheid, NSS)⁴⁵ catalogues various risks and provides guidelines to help prepare the Netherlands for different types of crisis. It approaches national security from the point of view of vital interests. These are 1) territorial security, 2) economic security, 3) environmental security, 4) physical security, and 5) social and political stability.

The strategy is updated on an annual basis by so-called *progress reports* to Parliament (voortgangsbrieven) as well as annual risk assessments, scenario planning and strategic surveys (strategische verkenningen). The latest progress report⁴⁶ outlined where capacity could and should be improved: cooperation in crisis management, improving information positions, awareness and training, crisis communication and capacity development as such to be put on the international agenda. In addition, the report stressed the need to improve international cooperation in the area of cyber security. An analysis of the most relevant policy-related terms in the NSS renders the following overview:



Figure 2 Word cloud of relevant policy terms in the NSS (2007)

Source: HCSS

This illustration shows for instance that already back in 2007, the international dimension of national security was well taken into account in crafting an overarching security policy. Other striking terms that stand out include threats, information and capabilities, signaling a concern to be well prepared to deal with a variety of security challenges.

2.2 International Security Strategy

The **International Security Strategy**, (Internationale Veiligheidsstrategie, ISS) called *A Secure Netherlands in a Secure World* and first issued in 2013, builds on the NSS and distinguishes three key interests for the country's foreign policy: 1) defending its own territory and that of its allies; 2) promoting an adequately functioning international order based on the rule of law and 3) economic security. Based on an analysis of today's international environment by think tanks such as HCSS and others, the Ministry of Foreign Affairs identified a number of macro trends and risks that will likely dominate the policy agenda in the years to come:

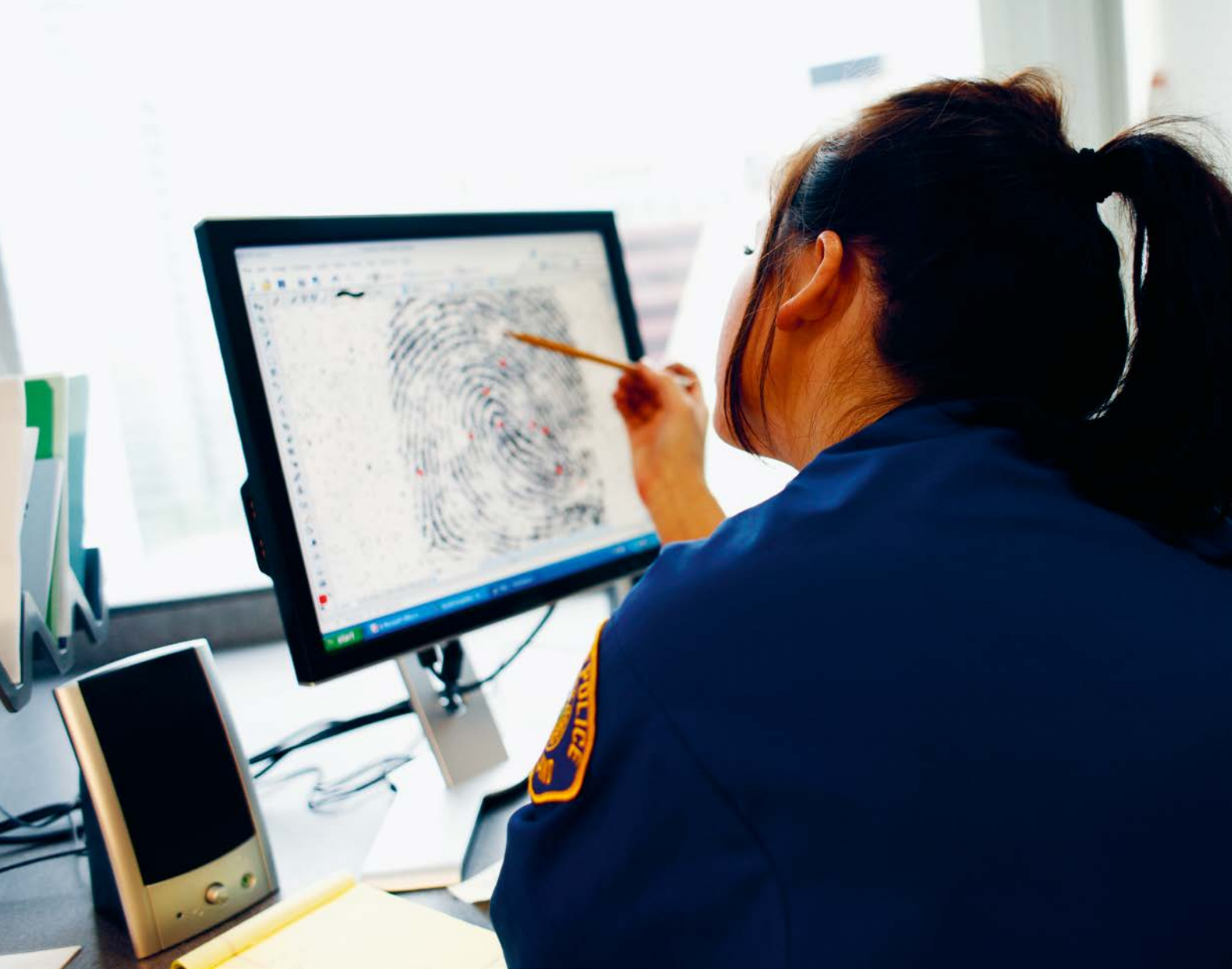
- shifts in the international balance of power and a move towards multipolarity;
- changing patterns in the world economy;
- the rise of cyber;
- weapons technology and the threat of weapons of mass destruction;
- natural resources;
- fragile states (in particular in the wake of the Arab spring).

These issues all have one thing in common: they all represent challenges to traditional ideas of world order, heralding a world of competitiveness, instability and uncertainty. Based on the above trends and challenges, the government identified six key focus areas as well as an overview of the various instruments it plans to bring to bear. Analysing the most frequently mentioned terms helps to highlight the key international concerns according to the ISS:



Figure 3 Word cloud of relevant policy terms in the ISS (2013)

Source: HCSS



Standing out here are terms such as economic, preventing, and cyber, all of which have a strong domestic as well as international dimension. In November 2014, the government issued an addendum to the 2013 ISS, which highlighted fresh challenges such as Russia's military operation against Ukraine and the rise of ISIS in Syria and Iraq. This letter also highlighted developments such as the Ebola crisis, the rise of new non-state actors and of China, as well as the increasing importance of cyber, and demographic and climatological trends.⁴⁷

Clearly, not only do the two strategies overlap, but they also require cross-sectoral and international cooperation. A word analysis of the ISS shows an emphasis on the need for preventative and early warning mechanisms—areas where security innovations can make a difference, both at home and abroad.

2.3 Implementing Security Policies

Implementation of security policies is in the first instance a responsibility of the government. Given the role of the government—at the national and lower levels—as a key launching customer, the priorities it sets have important consequences for how security provision and innovation evolve. In the latest budget (September 2014), the government explicitly stresses the impact of geopolitical events on our economy, increasing the Defense budget with € 100mn per year, while AIVD (the Dutch General Intelligence and Security Service) is to receive € 25mn extra per year.⁴⁸

In the area of domestic security, the agenda for 2015 stresses the importance of combating 'the jihadist threat' based on the action plan *Integrale aanpak jihadisten* (Comprehensive Approach to Jihadists), which aims 'to protect the rule of law, combating and weakening jihadism in the Netherlands and to eliminate the breeding ground for radicalisation.'⁴⁹ In this regard, the government calls for 'cooperation between all partners, both at the national as well as local levels and with civil society.'⁵⁰ Another focus in 2015 is the implementation of the 'Security Agenda' (veiligheidsagenda), which focuses on

national and local societal security issues. Other key areas of attention that are highlighted are cyber security, where the need for 'adequate protection (...) as a precondition for economic prosperity and the involvement of the government, citizens and business' is stressed, as well as the need for tackling high-impact crimes such as robberies, burglaries and violent incidents.⁵¹

In its budget, the Ministry of Economic Affairs underlines how rising economies in Asia will affect the Netherlands in terms of the need to consolidate its position as a network hub, and that competition for raw materials will only increase. Other important initiatives include seeking closer linkages between the Top Sector Policy and the EU's Horizon 2020 programme; to support innovative SMEs and start-ups through a € 30 mn stimulus fund; and to present legislation supporting 'data-driven innovations and revenue models.'⁵² The Ministry of Infrastructure and the Environment focuses in 2015 on water safety and promoting expertise in hydro-engineering abroad. Another priority is to cooperate with cities to create smart, safe and sustainable urban areas that provide an enabling environment for innovation.⁵³

This snapshot of government initiatives demonstrates that in various respects, a broad notion of security is already present in policy planning. Tackling these challenges requires cooperation both vertically and horizontally. Vertically, in terms of moving from diagnosis to solution; and horizontally by involving all relevant stakeholders. On these points, the Dutch Scientific Council for Government Policy came up with a list of key questions to think about how to deal with risks, including how to identify them, how to weigh policy options, and who to involve. The Council also stressed the importance of integrating business and civil society, as well as the fact that the international dimension of issues and solutions (i.e. seeking best practices) should also be taken into account.⁵⁴

The Dutch Court of Audit concluded in a report that in implementing the National Security Strategy, proper measurement of targets is absent.⁵⁵ The report also notes that 'the Minister of Security and Justice is unable to indicate which human and physical capacities, as well as methods needs to be strengthened or developed at the operational level since he lacks a comprehensive view of what can be supplied by the security regions and their partners.' As a result, policy decisions by the Government remain general in nature, and provide little guidance to their addressees.⁵⁶ The Minister responded that the National Security Strategy will be updated and from 2016, include a quadrennial national risk profile as well as an inventory of available capacities.⁵⁷

In the latest budget (September 2014), the government explicitly stresses the impact of geopolitical events on our economy, increasing the Defense budget with € 100 mn per year, while AIVD (the Dutch General Intelligence and Security Service) is to receive € 25 mn extra per year.⁴⁸

3 – Assessing Safety and Security: What Are the Issues, and What is Needed?

Given the kinds of security and safety threats we face, how well is the Netherlands prepared, and are we focusing on the right issues? Various government agencies publish annual assessments of security trends and threat levels, providing policy makers and citizens alike with indications what the authorities are focusing on, and how they respond to citizens’ concerns.

3.1 Some Key Government Studies Framing the Security Debate

One joint effort is the **Rijksbrede Trendverkenning** (National Trends Survey), first undertaken in 2010 and updated in late 2013. One trend it highlights is that across society, the acceptance of risk is decreasing, and that this could be a reason for the increased demand for repressive security measures.⁵⁸ More in general, this phenomenon is part of a trend towards people vesting more reliance into the government to provide for their safety and security. As a consequence, the survey notes that this social trend could 1) increase the growth of a ‘claims culture’ as in the United States and 2) that this creates a moral hazard problem on the part of private actors, since they will increasingly assume that the government will step in when things go awry.⁵⁹

As a general overview, the *Trendverkenning* mapped out some megatrends in relation to the geographical levels that they are likely to impact. (see below)

In the area of cyber security, the National Cyber Security Centre (NCSC) has issued a number of relevant reports, including an annual overview called the **Cyber security report**, the 4th edition of which was released in July 2014. In this report, the NCSC drew attention to key findings such as the fact that the threat of disruptions as a result of dependence on cyber technology is still increasing; that this is partly the result of developments such as the ‘internet of things’, whereby ever more devices are being linked up to the internet; that the largest threats emanate from states and cybercriminals and that privacy is coming under pressure due to data-gathering and storage trends.⁶⁰

The annual report of the **Dutch General Intelligence and Security Service AIVD** (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) focuses in its most recent issue on the dangers emanating from Syria, on cyber-espionage and on how the modes of operation of the intelligence services need to be reviewed and/or reformed in the wake of the Snowden revelations. In regards to radicalisation of

	Global	Europe	Netherlands
Demography		The metropolis as center	More households, different compositions
Economy		Economic dynamics Development of the knowledge economy	
Social		Fragmentation, detraditionalization, deinstitutionalization	New dividing lines throughout the society Mediation of the society Healthcare The search for the ‘perfect human’
Technology		Converging technologies	
Ecology		Disputes regarding natural resources Climate change and decreasing biodiversity	
Politics		Changing world systems Dense world Reshuffle the playing cards	Europe under pressure

Figure 4 **Megatrends and Impact dimensions** Source: Rijksbrede Trendverkenning 2014, p. 7

Muslims in Europe, the report notes that ‘[t]he proselytizing salafist *dawah* (call to Islam) movements active in Europe and the Muslim world (...) have clearly distanced themselves from international jihad of the kind propagated by Al-Qaeda, [but] take a far more positive attitude towards what they regard as defensive jihad against the supposed advance of Shi’ism and against Western occupation of “Muslim lands.”’⁶¹ Hence, the threat from such movements do not so much emanate from their propensity to foment jihad in Europe, but rather that potential recruits are encouraged to join the jihadist struggle in the Middle East.

AIVD also addressed this issue in a separate report entitled *Transformation of Jihadists in the Netherlands*⁶², which warned principally against new developments domestically and abroad that have given a new lease of life to jihadist movements active in the Netherlands, amongst others the rise of Salafist ideology. Furthermore, AIVD not only points at the risks related to jihadis returning to the Netherlands as such, but also more generally to ‘the [increasing] acceptance of the use of violence as a legitimate course of action, [and] the intolerance towards other citizens and rejection of the democratic legal order.’⁶³

Finally, the **National Coordinator for Security and Counterterrorism** (NCTV) issues a survey that measures public sentiments entitled *Barometer*. The latest edition was released in October 2014 and concluded that major events abroad such as the MH17 incident, the rise of IS and the Ebola crisis have a significant impact on people’s threat perceptions. As a result, ‘fear for a terrorist attack has increased.’⁶⁴ At the same time, the ‘sense of security’ and related worries for families did not markedly increase, and remained roughly the same compared to June 2014.⁶⁵ These findings correspond to those from the *Trendverkenning*.

People’s confidence in the government stepping in to rescue them in case of disasters somewhat increased since 2013, and is now at 45%, against 38% in June 2013. Confidence in the government stepping up to the plate in case of a serious crisis decreased somewhat, from 69% to 63%. Meanwhile, citizens think that they themselves are not nearly as well prepared, only 26% expressing confidence.⁶⁶

On the one hand, the fact that people by and large trust the government to protect them against various kinds of threats to their livelihoods is reassuring. On the other hand, the fact that citizens apparently believe that their safety and security is primarily a matter for the government, and not something that they themselves can or should contribute to more, warrants further reflection not just on the new kinds of security threats we face, but also how a changing society deals with these. Indeed, the Dutch Court of Audit already signalled the a need for more realism in terms of the levels of protection that the authorities can provide to citizens and businesses.⁶⁷

Taken together, these reports show that there is a strong awareness of the interplay between external and internal security threats, but that from the point of view of the government, what is happening today in terms of international jihadism and associated warfare is still largely being seen as something that happens in faraway places, and that we are still safe behind our dykes.⁶⁸

3.2 Views from Parliament, Civil Society, and the Private Sector

In putting together its security strategies, the government consults with all kinds of stakeholders in society to gauge their views. One important survey in this regard is the earlier mentioned *Barometer*. In its latest edition, the survey showed that, when prompted spontaneously on what they consider the main security threats of the moment, people mentioned the conflict against ISIS in Iraq and Syria 35% of the time, followed by economic concerns. This is a dramatic change from June 2014, when the financial crisis still dominated the headlines and the crisis in the Middle East hardly registered.

A list with pre-selected crisis-related topics also shows dramatic swings. Whereas in November 2013, 43% of respondents expressed fear about an international crisis, in October 2014 this was 68%. Chances of a terrorist attack are also seen to have increased, since 65% of all respondents considers this a likelihood, against 43% in November 2013. In the wake of the recent spate of attacks in Paris, these figures can only be expected to increase further.

Figure 5 **Estimated Chances of major events occurring**

	Oct '14	Jun '14	Nov '13
International crisis	68%	51%	43%
Terrorist attack	65%	48%	43%
Economic crisis	59%	62%	64%
Cyber attacks	47%	49%	52%
Widespread epidemics	45%	36%	40%
Public disorder	39%	35%	41%
Traffic accidents	34%	35%	37%
Accidents with hazardous substances	33%	39%	40%
Extreme weather	29%	39%	37%
Disturbance of Electricity, Gas, Water or ICT infrastructure	26%	29%	32%
Nuclear incident	25%	29%	30%
Big scale fire	23%	30%	30%
Floods	21%	29%	32%

Source: NCTV Barometer October 2014, p. 8

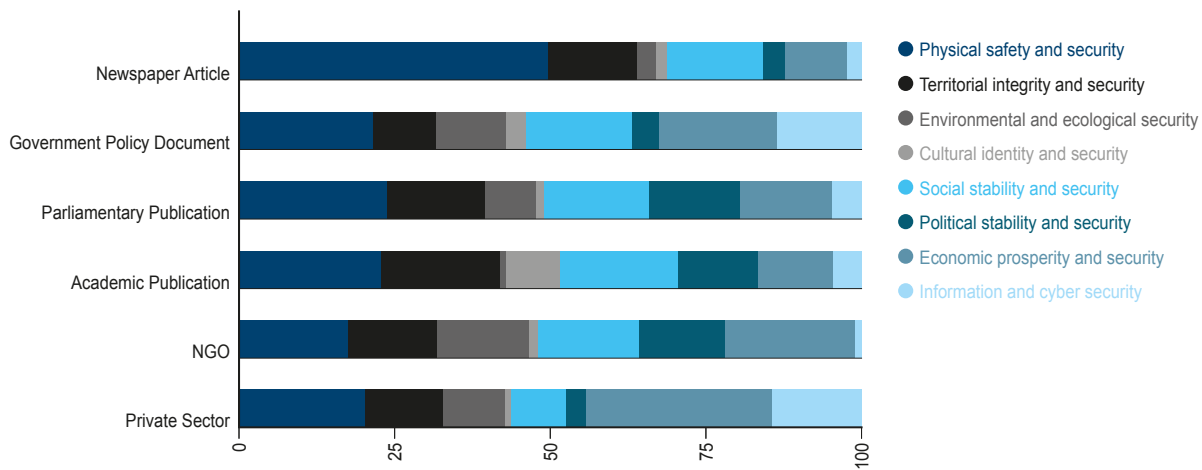


Figure 8 Core values mentioned for different sources in EvoCS study Source: HCSS

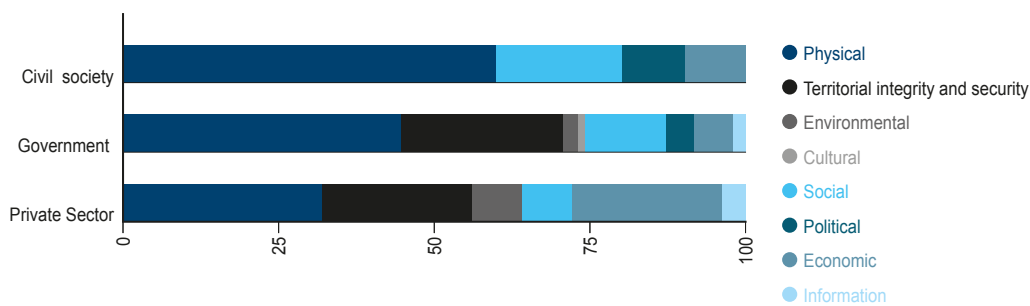


Figure 9 Relative number of actors addressing a particular core security value in newspapers Source: HCSS

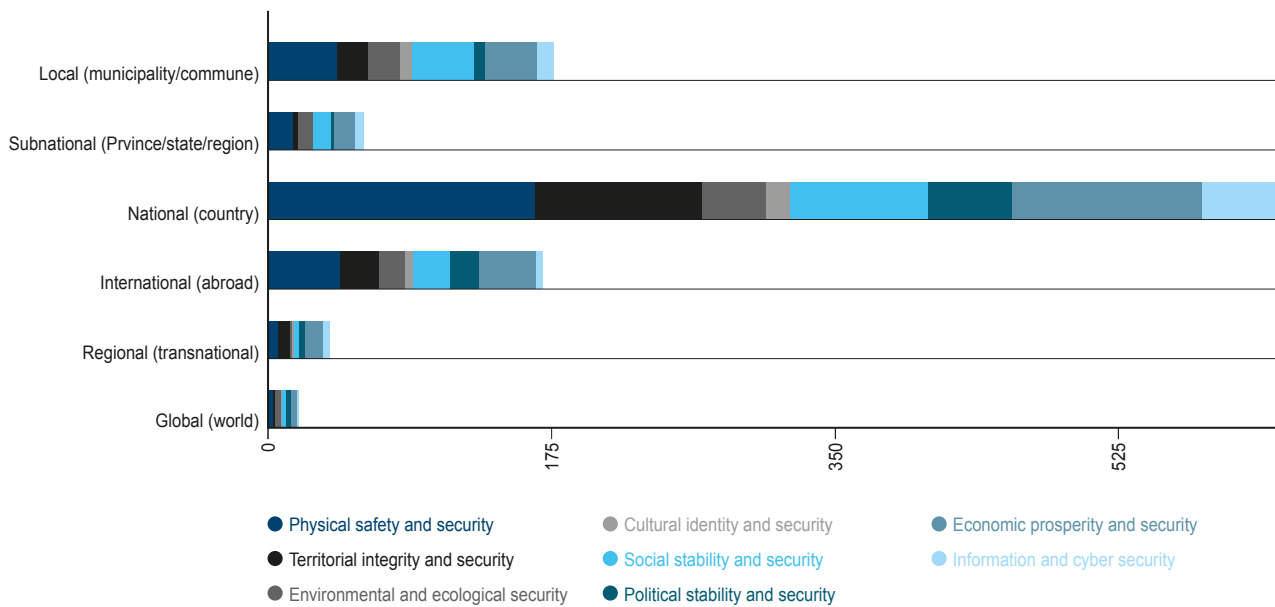


Figure 10 Main levels and respective core values considered by all actors based on all sources of the Dutch Security discourse Source: HCSS

Looking at how Parliament and two major newspapers in the Netherlands (*Volkscrant* and *De Telegraaf*) reflect security issues⁷¹, a few important differences can be noted from Figure 8 (left). One is that newspapers register much more concern for physical security issues than any of the other publication sources do. This is likely a reflection of the fact that physical security is not addressed by any institution specifically, but tends to be a dispersed topic.

Secondly, concerns about cyber security receive much more attention from government and the private sector, but receive less attention in the press. Third, economic security receives relatively more attention—in particular from the private sector—than some other issues such as identity and environmental issues. Finally, the attention given to territorial security is striking, no doubt induced by the war in Ukraine and, to a lesser extent, the conflicts in the Middle East.

In Figure 9, the relative number of actors addressing a particular core security value is indicated, as registered in newspapers. The first striking observation is the dominance of physical security for all three actors. It is apparent that newspapers especially focus on actors addressing physical security, including issues such as street violence and the threat of terrorism. Also striking is the concern about territorial security among government and private sector actors, and the fact that this issues does not register among civil society actors. Political stability however is addressed by civil society and the government and not considered by the private sector.

Figure 10 indicates the main levels and the respective core values considered by all actors based on all sources of the Dutch security discourse. It makes clear that the main focus of the Dutch security discourse lies at the national level, even considering that half of the data that was gathered for this analysis dates from post-MH17.

There is no dearth of information on security threats, risks and trends. Results from some key government surveys are in various respects corroborated by the results from the EvoCS study: physical security dominates security concerns overall, and in particular among civil society and the general public at large. But we also see that physical security takes up the largest share (about 45%) when government addresses security issues. These findings are not reflected in for instance the NCTV Barometer. Another interesting finding is that information security still constitutes a rather small share of all security issues, albeit that if the NCTV Barometers are any measure, this is set to change. Overall, the results of the EvoCS study show that physical, territorial and economic security tend to be the top concerns among security actors, while information (i.e. IT) is lagging somewhat.

3.3 Some Conclusions

This first part of the report leads to some important conclusions. One is that security, in all its different guises, is more than ever back on the national policy agenda. Secondly, recent events as well as the examination of the various thematic areas has shown that domestic and international security concerns are interlinked, and that the issues overlap. Third, while the concerns and related threats may differ per thematic area, this is not to say that concerted efforts between triple-helix partners are not warranted.

At the same time, the abundance of information has not always translated into more clarity on the part of the authorities on what is needed to enhance security, as the report of the Dutch Court of Audit demonstrated. Hence, there is a continuing need to improve metrics, adjust strategies, enhance capabilities and create coalitions. The larger goal is then of course to improve our resilience to safety and security threats. For all of these points, there is a clear role for HSD in pushing security innovation further ahead in the Netherlands.

(..) there is a continuing need to improve metrics, adjust strategies, enhance capabilities and create coalitions. The larger goal is then of course to improve our resilience to safety and security threats. For all of these points, there is a clear role for HSD in pushing security innovation further ahead in the Netherlands.

PART TWO —

HSD in the Security Landscape: Roles and Prospects

4 – Aims and Strategies of HSD

The rapidly changing security environment at home and abroad poses several challenges in terms of crafting adequate responses. The first is to ensure sufficient and clear understanding about the nature and scope of the security threats that our societies face. The second is to ensure that we have the right organisational structures and strategies in place to coordinate adequate responses. The third is to muster and develop the right capacities and means to tackle these security challenges. At all of these levels, the Hague Security Delta, being the national security cluster, can make a substantive and substantial contribution.

In its *Strategie- and Urgentieprogramma*, which sets out a strategy and priorities for the coming five years, the Hague Security Delta describes as its twin key objectives to generate economic and societal benefits. Concretely speaking, this translates into the creation of jobs and economic activity in sectors that promote and provide security and safety and at the same time, contribute to improving security by stimulating innovation.⁷² In its approach to enhancing security, HSD reflects the shift in thinking about security from responding to threats to thinking about how to anticipate security challenges in a comprehensive and integrated sense, and in the process, to create economic opportunities that benefit society.

To achieve these objectives, HSD defined a threefold strategy: one, to further expand the HSD network; two, to stimulate and sustain joint investments into innovation and knowledge development projects; and three, to achieve a better match between supply and demand in security provision.⁷³ The guiding framework for implementing this strategy is the National Innovation Agenda on Security (NIAV, in Dutch).



To succeed in its mission and to realise its objectives, HSD has devised a strategy for its own organisational development. First of all, it aims to establish itself as ‘the most important security cluster in Europe and one of the most important in the world (...) and to be the gateway to Europe for international organisations and businesses alike in the area of physical and cyber security.’⁷⁴ At the national level, HSD aims to be the central ‘knowledge hub’ and ‘innovation

platform’ for safety and security issues, contributing to the Dutch government’s Top Sector Policy. In that regard, the Covenant on National Cooperation for Security and Innovation is instrumental in forging cooperation between the key hubs in security and innovation in the Netherlands, bringing together The Hague Security Delta, Twente Safety and Security (TS&S), and the Dutch Institute for Technology, Safety and Security (DITSS).⁷⁵ The core is the HSD Campus, the national innovation centre for security in The Hague. Twente focuses on nano technology in particular, while DITSS in Brabant has its key strengths in high-tech solutions and camera and sensor technology.

Having been named among the top 10 leading innovation hubs in the Netherlands⁷⁶, HSD’s ambition is to triple the number of jobs, students and company turnover by 2025 for all of the partners in the cluster. Some of the key figures of HSD include some 400 companies being located in The Hague region. Total turnover among businesses in security innovation in the Netherlands is around € 6bn, with € 1,7bn generated in The Hague; annual turnover growth figures averaging 4,1% between 2006-11; and comprising 61,500 jobs, 13,400 of which are located in The Hague. HSD Foundation⁷⁷ as such includes around 200 partners at present, 70% of which are SMEs.⁷⁸

Another theme for HSD is to facilitate knowledge circulation, an idea that was developed by the Dutch Scientific Council for Government Policy in a recent report. In practice, it means that ‘the focus cannot be on knowledge generation alone; it will be just as important to see that that knowledge is properly absorbed and circulated.’⁷⁹ Through the HSD Cafés, its publications and its convening powers, HSD seeks to work towards this objective.

Where the availability of knowledge is concerned, HSD’s human capital agenda makes a critical contribution to provide HSD business with enough and adequate human resources.⁸⁰ To achieve this, it reaches out to various research and educational establishments. Some concrete results include the creation of the Cyber Security Academy, run jointly with Leiden University, Delft University of Technology and the Hague University for Applied Sciences.⁸¹ The Academy offers an MA programme, and is taught by both academics and private sector professionals. Another initiative of the human

capital agenda is the creation of a *Security talent community* that seeks to bring together students and professionals in the Dutch cyber community, as well as the Hague Security Academy.⁸²

In sum, HSD aims to be an enabler, facilitator and multiplier in what is called the triple-helix of stakeholders that need to make it all happen: knowledge institutions, government and the business sector. Knowledge institutions contribute by thinking through new responses to existing, changing or newly arising challenges. Government and its agencies are essential not just because they are indispensable in setting the security agenda, but also because they are a principal launching customer that helps spur innovation and investment in security technology. Business can help the government and other stakeholders devise new technologies and applications to enhance our security and safety.

Close cooperation between these stakeholders in the triple-helix will in turn have a multiplier effect on innovation. The envisaged result is that better security can be provided in a more cost-effective way, and that the cluster helps to stimulate the competitiveness of triple-helix partners at the international level.

4.1 Meeting Threats and Challenges: Shoring up Knowledge and Capacity

In view of the range of security challenges that Dutch stakeholders and society confront, the Netherlands is quite advanced and well prepared in some areas, while in others, progress needs to be made where HSD can play a facilitating role. Given the range of security issues, a focus needs to be applied in terms of the threats which should receive priority; the areas where there is a significant lack of knowledge or capacity and, more particularly, the areas where HSD partners can make the most meaningful contributions.

4.1.1 How to Prioritise

A critical question is how to prioritise. This can be done in different ways and depend on needs perceptions as well as capacity available. Indeed, the latter is determinative for how resilient a society is. From a national perspective, priorities can be set based on the following three criteria⁸³:

- impact of events
- likelihood of events
- perceived importance by citizens, business and the government

To refine the outcomes, a differentiation as to whether the impact is personal, local or even global, and the duration can be included. Another key factor linked to available capacity is resilience, i.e. the capacity of persons, structures or systems to bounce back from adverse impacts. This dimension is

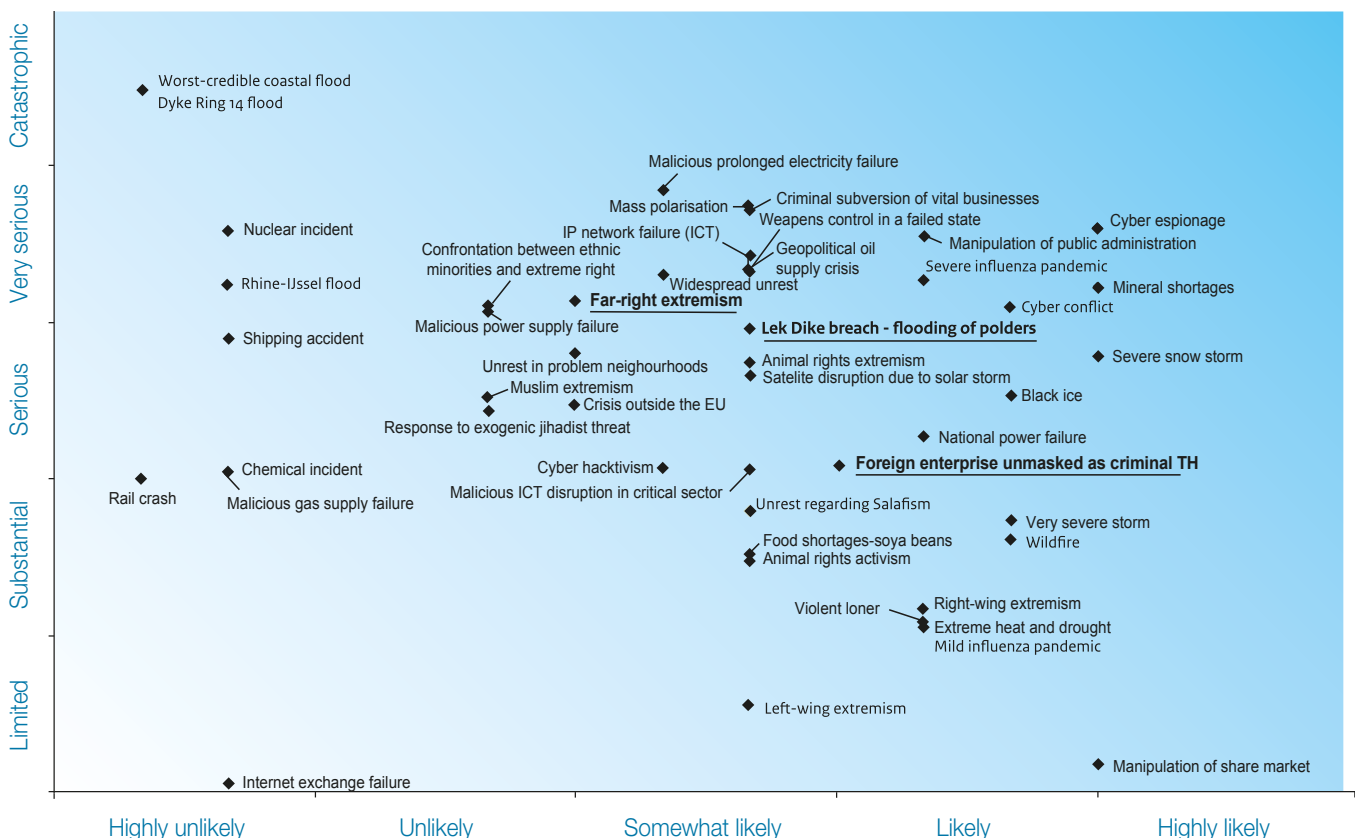


Figure 11 Matrix of likelihood and impact of risks Source: NCTV⁸⁵



relevant for all three factors: resilience should help to blunt the impact, decrease the likelihood of, and lower the perceived importance of adverse events. As a result, what could otherwise be a catastrophic event may not be equally considered a priority if a society or a country deems itself sufficiently resilient to bounce back from its impact. In its National Risk Assessment, the Dutch NCTV created an overview of all risks measured against their impact and likelihood to occur.⁸⁴

According to this visual (figure 11), the most worrying events that could occur are cyberconflict and -espionage, a lack of natural resources (minerals) and severe weather events, such as snow storms, rain storms and forest fires. Hence, it shows that many of the greatest and most acute threats that we face do not necessarily relate to geopolitical, socio-economic or jihadist threats (as is the focus of the public authorities), but rather relate to challenges to our critical infrastructure.

Prioritising between these three different areas should proceed on the basis of existing resilience capacity. For instance, while the impact of massive floods is potentially huge, the Netherlands does have a solid water management infrastructure in place to deal with such calamities, as well as a plan to upgrade existing infrastructure in the decades to come (led by the Delta Commission).⁸⁶ However, in other areas, capacities could use reinforcement, examples being cyber and jihadist threats.

4.1.2 Where HSD can Contribute

HSD aspires to be the *secure gateway* to Europe's hinterland. It will contribute to the Dutch Top Sector Policy (*topsectorenbeleid*), in particular the High-Tech Systems and Materials sector. In addition, through an innovation contract, the theme *Societal Security* is addressed as well.⁸⁷ Some of the objectives of the Top Sector Policy are to contribute to improving resilience and disaster preparedness in the Netherlands, and to have a measurable contribution to attracting international businesses to the city of the Hague.⁸⁸ The convening powers and substantive focus of HSD can make a critical difference here.

HSD is embedded in a broader environment in which triple-helix partners seek to promote security-related innovation. These partners include the Dutch Institute for Technology in Safety and Security (DITSS), Twente Safety and Security (TS&S), regional development agencies, chambers of commerce, the Netherlands Foreign Investment Agency (NFIA), the Netherlands Enterprise Agency (RVO), NWO's ICT Innovation Platform Security and Privacy (IIPVV) as well as some sectoral organisations such as the Netherlands Institute for Defence and Security (NIDV), ICT Netherlands and FME/CWM, who represent the Dutch technology sector. HSD can support these organisations by stimulating knowledge exchange and synergies.⁸⁹

In addition, HSD concluded an agreement in 2014 with InnovationQuarter (IQ), an initiative launched by the province of South Holland focusing both on innovation and investment. Specifically, IQ focuses on cross-sectoral innovation (in conjunction with HSD), one sectoral focus being *smart industry*, and seeks to advance integration of IT in existing production processes. It also hosts an investment fund aimed at supporting tech startups and SMEs to market new technologies by providing venture capital.⁹⁰

In order 'to support the development of the security cluster'⁹¹, HSD formulated some strategic objectives to be pursued in the coming years. These are:

- 1 Further developing a visible and operational knowledge cluster built on the five innovation houses national security, critical infrastructure, urban security, cyber security and forensics.
- 2 To actively facilitate consortia and to contribute to cooperation between consortia, innovation funds and instruments of financing.
- 3 To develop a Human Capital Agenda in Security.
- 4 International acquisition and branding.

In its development strategy, this is illustrated as on the next page.

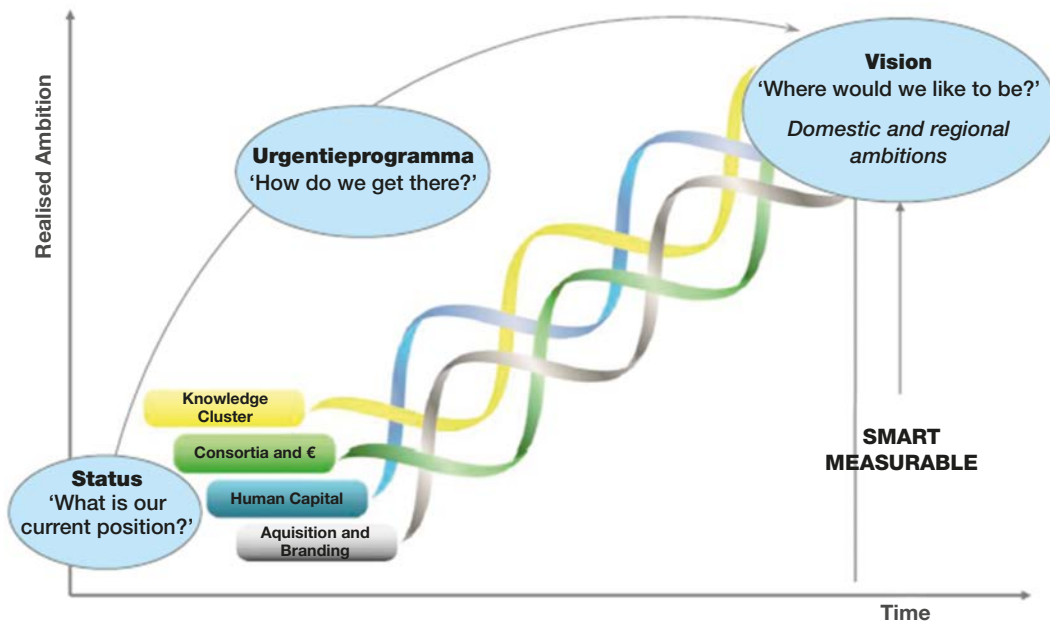


Figure 12 **Plan of Action for HSD Urgentieprogramma 2015-17** Source: HSD⁹²

One more way for HSD to position itself at the international level is to become a lead agent in creating a Knowledge and Innovation Community (KIC) in security. The impetus for creating such KICs comes from the EU Commission, which seeks to promote economic growth through innovative initiatives. KICs consist of nodes between 5-6 countries which cooperate around a certain strategic theme. Criteria for KICs include substantive focus (clarity of purpose), cluster quality (critical mass, and regional support) and political support. The strategy to achieve this is called *smart specialisation*. For the security industry, there is a specific investment plan developed by the EU, called the Action Plan for an Innovative and Competitive Security Industry.⁹³ The *European Institute for Innovation and Technology* (EIT), based in Budapest, is meant to provide guidance to these KICs. In the coming six years, a budget of about € 2,5bn is allocated to supporting KICs.

While the EU has no plans for a KIC Security yet, HSD has already moved forward in building *knowledge bridges* with the USA (Homeland Security/Baltimore cluster), Canada (Ottawa Invest), and Singapore (Economic Board), and created a security acquisitions platform to further expand its international reach and collaborations.⁹⁴ In its annual report, HSD announced that a partnership has been concluded with the European Organisation for Security that brings together some 50 companies and knowledge institutions in the area of security.⁹⁵ At the same time, HSD has also established strong ties with a host of security clusters and organisations elsewhere in Europe, including the UK, Belgium, Finland, Estonia, France, and with some of the EU Institutions.⁹⁶

According to the Policy Research Corporation report, the global security provision sector will expand by 2020 so as to reach a turnover figure of about € 300-350bn, 70bn of which is generated in Europe. Most growth in the coming decades is expected to be in the Asia-Pacific region, while the European





and North American shares will decline.⁹⁷ This suggests that striking up further cooperation agreements with Asian partners can be part of a sustainable strategy for European security providers and clusters such as HSD, whereby the existing arrangement with Singapore can be a start.

4.2 The National Innovation Agenda for Security

Among the principal achievements of HSD in 2014 and key for its agenda-setting capacity in the years to come is the National Innovation Agenda for Security (NIAS). It sets out what role HSD could and should play in stimulating the development of the security innovation sector in the Netherlands through joint cooperation between the public and private sectors. Part of its strength is derived from the fact that it came about following extensive consultations with stakeholders at all levels and across all relevant sectors—including senior civil servants, CEOs and others—and that it drew on various sectoral innovation agendas. This guaranteed that the NIAS would enjoy broad support from the start, and this should facilitate its implementation.

Being the custodian of the NIAS strategy, HSD is playing a key role in this process by stimulating and encouraging cooperation among the quartet of government, research, learning institutions and enterprise.⁹⁸ The key ministries involved in pushing the NIAS agenda forward are Security & Justice and Defence followed by Economic Affairs. In addition, HSD should help to stimulate Public Private Partnerships (PPPs) and link its activities and initiatives to Horizon 2020. The guiding idea behind this is that progressively better security requires progressively better innovation.

The estimations for value added as a result of investments made on the basis of the NIAS are considerable. '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 more secure at an acceptable cost), but also generate economic revenues from utilising 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.'⁹⁹

'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'

5 – Clusters Worldwide

Reflecting on its growth potential, HSD and its partners consider and monitor developments regarding security innovation initiatives around the world. Existing security clusters elsewhere can be competitors, but also potential partners. It is therefore essential to consolidate and build on one's niche capacities.

Worldwide, security clusters achieve a combined gross turnover of around € 180bn, of which 45bn is realised in Europe. This implies that about 4% of total global turnover in security provision is created in the Netherlands, and about 1% in The Hague. The global potential of the market and the fact that the security cluster managed a growth figure of 4.1% even during the years of economic crisis, provide further incentives to look abroad for opportunities.¹⁰⁰

The combined strength and expertise of HSD's members make it the largest security cluster in Europe. But HSD is certainly not the only security cluster out there in the world. This chapter provides for a comparative perspective between HSD and a number of other clusters in the world that help to illustrate where HSD stands, where competition is located, where opportunities lie, and which niche capacities are worthwhile to develop in order to further boost HSD's international profile.

5.1 HSD in a Comparative Perspective

At the national and international levels, there is a number of clusters that is comparable to HSD in terms of the number of companies involved, their capacity to innovate, and the make-up of companies that contribute the lion's share of the cluster's revenues. Whereas a number of these clusters can be classified as genuine security clusters, others have more hybrid characteristics. Table 1 lists a selection of these clusters.¹⁰¹

Table 1 Selected Clusters Worldwide

Cluster	Quick Facts	Background
SIGNUM (Sicherheit aus der Hauptstadtregion), Berlin, Germany	<p>Leading Members</p> <ul style="list-style-type: none"> • Land Berlin & Brandenburg • Fraunhofer Institute • Free University Berlin • Daimler AG • Telecom AG <p>Total: 124 (2009)</p> <p>Turnover and employment¹⁰²</p> <ul style="list-style-type: none"> • 3 Billion Euro • 25.000 Employees <p>Expertise</p> <ul style="list-style-type: none"> • IT Security • Production of Security and Defense • Technology and Systems • Service and Consulting <p>Fact Sheet file:///H:/Downloads/Sicherheitswirtschaft_en.pdf</p>	<ul style="list-style-type: none"> • Founded in 2008/2009 in Berlin and Brandenburg, Germany with over 124 companies involved. • Several companies take on a leading role in the sub sectors. SIGNUM has a strong record in public-private partnerships, whereby the private sector takes on a leading role; • SIGNUM's earning model is based both on public, as well as private funds. SIGNUM is also eligible for (European) subsidies. Projects are partly financed by subsidies amongst others in the framework of the European FP-7 Budget contributing 3.3 million Euros (until 2009).¹⁰³ • SIGNUM is run from Berlin and Brandenburg. Externally however, SIGNUM operates as a network with a single voice. The annual growth rate of the networks private members is 17% and the stakeholders plan to push forward with international expansion within the next 5 years.¹⁰⁴

Cluster	Quick Facts	Background
Ottawa Security Cluster, Canada	<p>Leading Members</p> <ul style="list-style-type: none"> Invest Ottawa Lockheed Martin General Dynamics Thales Raytheon <p>Total: 300+</p> <p>Turnover & employment</p> <ul style="list-style-type: none"> >1 Billion US\$ (2012) 17,000 employees (2013) <p>Expertise</p> <ul style="list-style-type: none"> Aerospace Defense and Security Technology and Services <p>Website http://investottawa.ca/industries/aerospace-defence-security/ http://investottawa.ca/a-billion-dollars-in-annual-</p> <p>Fact Sheet http://investottawa.ca/wp-content/uploads/2013/09/ADSFactSheet.pdf</p>	<ul style="list-style-type: none"> The Ottawa Security Cluster is founded and maintained by Invest Ottawa. The cluster is home to over 300 companies, providing employment to over 17,000 people. The cluster includes governmental and educational institutions as well as the private sector.¹⁰⁵ Ottawa's aerospace, defence and security companies specialize in technologies and services that span the full range of capabilities - everything from UAVs to anti-hacker communications software, to tank weapons control systems - supported by research institutions and a large concentration of scientists and researchers in the Ottawa area.¹⁰⁶ The cluster is financed by subsidies of public sources such as OCRI and by research institutions as the National Research Council of Canada.¹⁰⁷ Another income stream is the regular organisation of events in the field of defense and security.¹⁰⁸
Security Network San Diego, United States	<p>Leading Members</p> <ul style="list-style-type: none"> Unknown <p>Turnover & employment</p> <ul style="list-style-type: none"> Unknown <p>Expertise</p> <ul style="list-style-type: none"> Security and Defense Technology in the broad sense. <p>Website http://thesecuritynetwork.org</p>	<ul style="list-style-type: none"> The Security Network San Diego (SNSD) was founded in 2005 as an idea borne out of the organisation of the annual 'The Security Summit' in San Diego. The mission of The Security Network is to advance security by 'Fostering Innovation through Collaboration' worldwide. SNSD promotes rapid commercialization of dual/multi-usage, security technologies from around the world and the development of effective regional security, including having San Diego act as a national/international testbed.¹⁰⁹ SNSD hosts forums and technology exhibitions that connect security technology and solutions innovators with public/private sector organisations and defense contractors/systems integrators/distributors looking for innovative security technologies. The focus is on finding innovative COTS (commercial-off-the-shelf) and MOTS (modifiable off-the-shelf) technologies and promoting their rapid adoption by end-users in homeland security, military and first response.¹¹⁰ Due to large variation in the varying number of participants of the events, the precise number of Members of SNSD is unknown. The overall focus lies on the facilitation of the cooperation between national and international companies in the security industry. The main sources of income are private sponsorships and government subsidies.

Cluster	Quick Facts	Background
Aerospace Valley World Competitiveness Cluster Toulouse/Bordeaux, France	<p>Leading Members</p> <ul style="list-style-type: none"> • Airbus, Air France, ATR, Dassault Aviation • CNES, EADS • ACTIA Group, Alstom Transport, Continental, Thales Aeronautics • Ministry of Defence <p>Total: 728+</p> <p>Turnover & Employment</p> <ul style="list-style-type: none"> • > 130.000 employees¹¹¹ <p>Expertise¹¹²</p> <ul style="list-style-type: none"> • Aerospace Technology • Gas turbines for helicopters • Landing gear • Civil and regional aviation • Business aviation • Military aviation • Remote sensing, data collection and localization • Space services <p>Affiliated Clusters & Partners</p> <ul style="list-style-type: none"> • 8 MoU's signed with other clusters • Formal cooperation with 2 other clusters <p>Website</p> <p>http://www.aerospace-valley.com</p> <p>Fact Sheet</p> <p>http://www.aerospace-valley.com/sites/default/files/documents/av-plaq-uk-bd-3005-3-bat.pdf</p>	<ul style="list-style-type: none"> • Aerospace Valley (AV) was created in 2005 to grow the competitiveness of the Midi-Pyrénées & Aquitaine regions' Aeronautics, Space, and Embedded Systems sectors on the national, European and international levels by fostering the development of networks and collaborative initiatives.¹¹³ The network consists of a mix of Small and Medium Sized Enterprises (SMEs), industry leaders, investors, research organisations, and public institutions. • AV has set up an elaborate network of external cooperation. Memoranda of Understanding have been signed with the following other clusters worldwide: <i>Aéro Montréal, Canada; CECOMPI São José dos Campos, Brazil; Skywin Wallonie, Liege Belgium; Farnborough Aerospace Consortium, UK; Aviation Cluster Hamburg, Germany; Hegan, Bilbao Spain; AVSI, Austin, United States; Subsea Valley, Asker Norway.</i> • AV is engaged in more formalized cooperation with two other clusters: Recherche et innovation synergétiques en aérospatiale (CIRAQ), Montréal, Canada; and the Tianjin Free Trade Zone, China. • As a result of the good performance of the cluster, France more than doubled its world export share in aerospace between 2000 and 2010, and became the largest aerospace exporter in the world.¹¹⁴ Between 2005 and 2010 more than 300 R&D projects were funded at a total sum of € 833 million. 57% of this amount was funded from the private sector and 43% came from public sources.¹¹⁵ Annual turnover stood at 10 G€ in 2013 and the budget for running costs was € 1,6 million.¹¹⁶ • The cluster is growing rapidly. Since its founding day it grew from 570 members in 2008, to 620 in 2013 to 720 in 2014.¹¹⁷
Brainport Eindhoven, The Netherlands	<p>Leading Members</p> <ul style="list-style-type: none"> • Philips • ASML • NXP <p>Total 125+</p> <p>Turnover & Employment¹¹⁸</p> <p>€ 13,5 billion worth of industry exports (2012)</p> <p>€ 2,1 billion worth of private R&D spending (2012)</p> <p>60000+ jobs in high-tech, automotive, manufacturing industry and high-tech services</p> <p>28.200 researchers</p> <p>Expertise</p> <ul style="list-style-type: none"> • High-Tech Systems and Materials • Automotive • Design • Food & Technology • Lifetech & Health <p>Website</p> <p>http://www.brainport.nl/en</p> <p>Factsheet 2014</p> <p>http://www.brainport.nl/strategie/feiten-en-cijfers/brainport-monitor-2014-samenvatting-web</p>	<ul style="list-style-type: none"> • Brainport's main focus is on the field of high tech, but constantly seeks cross-sectoral links. The cluster is home to the manufacturing industry, technology and design. It is mainly focused on High-Tech Systems and Materials (HSTM), Food and Technology, Automotives, Lifetec and Design.¹¹⁹ • The cluster is comprised of private parties, research institutes and governmental organisations. Philips, the universities in the region and the provincial governments act as catalysts of the cluster and collaborate intensively. These organisations are united in <i>Brainport-2020</i> and the Stichting <i>Brainport</i>. • Leading institutions within the cluster are committees such as the Brainport 2020 Commission and the Brainport Stichting. The latter is the clusters <i>organisational arm</i> and its projects are equally financed by public money (from local municipalities and the government) and by private money (from its private members). • In 2011 Brainport Eindhoven Region has been elected 'Intelligent Community of the Year 2011' and is the region with the most registered Patents in Europe. Furthermore Eindhoven is, according to FDI Intelligence, Europe's third best region to invest in in 2014.¹²⁰ • The Brainport 2020 Commission, Stichting Brainport and the cluster's executive arm <i>Brainport Development</i> receive both public, as well as private funding. Half of the funds are raised by knowledge institutions and companies that participate in the cluster. The remainder comes from local municipalities, the province and the national government. Revolving funds are one of the ways through which projects are funded. • Internationally, Brainport cooperates with companies from all over the world, including in the US, Canada, Turkey, China, India and Singapore. Within Europe cooperation initiatives exist with companies in Finland, France, Germany, Italy, United Kingdom and Spain. Specific cooperation on top-technology and innovation takes place within the Eindhoven-Leuven-Aken triangle (ELAt).¹²¹

Cluster	Quick Facts	Background
Dutch Institute for Technology Safety & Security (DITSS), The Netherlands	<p>Leading Members</p> <ul style="list-style-type: none"> • Province Noord Brabant • Brainport Development • Midpoint Brabant • Tilburg University • Eindhoven University of Technology • Gemeente Eindhoven & Tilburg • Geodan • Securitas • Axis Communication • ICopp • ST&D <p>Turnover & Employment</p> <ul style="list-style-type: none"> • unknown <p>Expertise</p> <ul style="list-style-type: none"> • Public Security • Terrorism Prevention • Cyber Security • Public Safety • Crisis Management <p>Affiliated Clusters & Partners</p> <p>The Hague Security Delta Twente Safety and Security</p> <p>Website</p> <p>http://ditss.nl</p>	<ul style="list-style-type: none"> • The Dutch Institute for Technology Safety & Security (DITSS) was founded in 2012. DITSS focuses on technological innovations and new forms of collaboration in the security domain.¹²² • DITSS contains both large corporations, as well as SMEs. Ten different partner organisations are active within DITSS. Partner organisations set aside, DITSS has, 20-30 more organisations that are associated with DITSS. Partner organisations are: Stichting Technologie & Veiligheid, Geodan, Regional Platform Criminaliteitsbeheersing Oost-Brabant, Technische Universiteit Eindhoven, Tilburg University, Brainport Development, Midpoint Brabant, gemeente Eindhoven, gemeente Tilburg en provincie Noord-Brabant (BOM). • DITSS is primarily funded through government funds. However, the cluster foresees a shift towards more private funding. Income is generated through projects, the organising of events and research funds coming from national, European and international funds. • Notable achievements include the programs <i>Secure Lane and Safe Truck Stops</i>. The program <i>Secure Lane</i> is aimed at preventing cargo theft in the Netherlands. The program established a corridor from Venlo to Rotterdam where intelligent camera technology monitors a total of 15 different locations. Thanks to <i>Secure Lane</i>, the total number of cargo thefts in The Netherlands decreased from 74 in a single year (2012) to only 4. The program <i>Safe Truck Stops</i> was developed as a follow-on to <i>Secure Lane</i>. Through the use of intelligent cameras it places a virtual fence around truck stops, allowing intruders to be spotted early on. A direct connection with the police allows for an effective and rapid response.
Dutch Polymer Institute (DPI), The Netherlands	<p>Leading Members</p> <ul style="list-style-type: none"> • Ministry of Economic Affairs • Akzo Nobel • Dow Benelux • EXXON • Shell • Philips • Bayer • TU Delft • Eindhoven University <p>Total: 83</p> <p>Budget and Employment</p> <p>33.81 million EUR 200 researchers involved in DPI projects at knowledge institutes throughout the world.</p> <p>Expertise</p> <p>Polymer Materials</p> <p>Website</p> <p>http://www.polymers.nl/</p>	<ul style="list-style-type: none"> • The Dutch Polymer Institute (DPI) is a foundation funded by Dutch industry, universities and the government which was set up to perform exploratory research in the area of polymer materials. DPI operates at the interface of universities and industry, linking the scientific skills of university research groups to the industrial need for innovation.¹²³ • 38 industrial organisations are involved in DPI. In total, 45 knowledge institutes are a member of DPI.¹²⁴ DPI has a large network of foreign companies and knowledge institutes that act as partners of the cluster.¹²⁵ • DPI's budget consists both of public funds, as well as private money. The lion share of the budget is formed by contributions (in-kind and other) by industrial partners (46%) and contributions by the Ministry of Economic Affairs (27%). Other sources are EU FP-7 funding (7%) and various research programs.¹²⁶ Companies that wish to start up projects within the DPI are actively supported by both the DPI, as well as a special subsidiary named the DPI Value Centre, a foundation which helps companies in the area of polymer innovation. Projects can partly be financed by the Innovation Credit of the <i>Innovatiefonds MKB plus</i>.¹²⁷

Cluster	Quick Facts	Background
Silicon Valley (SV), United States	<p>Leading Members</p> <ul style="list-style-type: none"> • Google • Facebook • Cisco Systems • IBM • Intel • Apple • Adobe Systems <p>Turnover and Employment 1.4 million employees</p> <p>Expertise</p> <ul style="list-style-type: none"> • high-tech (all kinds) • Semi conductor industry; • Mobile phone technology; • Social networking; <p>Website http://www.siliconvalley.com/</p>	<ul style="list-style-type: none"> • Silicon Valley (SV) is an evolved network for the high tech industry that is clustered in multiple ways. SV is home to 150 major companies as much as 7000 small and medium sized enterprises and start-ups. SV also hosts numerous prestigious R&D institutes such as the Stanford university and the NASA Ames research center. • SV is home to both organisational networks between companies active in the area, as well as more formalized networks and branch organisations such as Joint Venture Silicon Valley. • SV can build on a combination of a highly skilled labor force, and a high concentration of educational and research institutions such as Stanford and UC Berkeley, together with high access to venture capital. This has allowed the region to become the high-tech center of the US. In 2012, 41% of total venture capital invested in the US went to companies active in SV.¹²⁸
Oost NV, Nederland	<p>Leading Members</p> <ul style="list-style-type: none"> • Ministry of Economics • Municipalities in Gelderland, Overijssel • NFIA • RVO • Kennispark Twente, Enschede <p>Turnover and Employment Total project volume € 30,9 million (2013)</p> <p>Expertise</p> <ul style="list-style-type: none"> • Agrofood • Life Sciences • High Tech <p>Website http://www.oostnv.nl/</p>	<ul style="list-style-type: none"> • Oost NV (the East Netherlands Development Agency) is a regional development company which originated via the merger of three development companies belonging to the provinces of Gelderland, Overijssel and the cities of Arnhem and Nijmegen.¹²⁹ The development company Oost NV is mandated by the Ministry of Economic Affairs and the provinces of Gelderland and Overijssel to carry out its tasks.¹³⁰ • An important subsidiary of the cluster is the so-called <i>Participatiemaatschappij Oost Nederland</i> (PPM Oost). PPM Oost helps start-ups and young companies in getting access to finance for investments for their projects. PPM Oost commands five funds primarily for the purpose of start-up support.¹³¹ • Oost NV is entirely financed by public funds, subsidies and direct investments by the stakeholders. In 2013, Oost NV held a total project volume worth € 30,9 million and an investment volume worth € 156 million. PPM Oost was good for € 28,8 million of investments in new and existing participations.¹³² • Oost NV collaborates with the chambers of commerce, Syntens, Kennispark Twente, Kennispoort Zwolle, Stedendriehoek Innoveert, GreenTechAlliances powered by kiEMT, EVD/NFIA, Regionale Centra voor Technologie, Good Valley and Health Valley.¹³³
Twente Safety & Security	<p>Leading Members</p> <ul style="list-style-type: none"> • Twente Security Region • Thales • Saxion • Twente University • DITSS • HSD • TNO <p>Turnover and Employment • unknown</p> <p>Expertise</p> <ul style="list-style-type: none"> • Safe Community • Smart Intelligence • Smart Safety <p>Website http://www.twentesafetyandsecurity.com/</p>	<ul style="list-style-type: none"> • Twente Safety & Security is a PPP between the government, educational institutions and business. It was created in order to stimulate cooperation in the area of security innovation. • TS&S aims to promote a society that is actively involved with improving its security, whether at home, at work, or in terms of the environment, helping society to deal with unforeseen events. The result is a Twente region that is resilient. • This is achieved by creating innovative solutions and by implementing these, using social and technical innovations, which will be tried out across Twente with the aid of training- and real-life experiences. The solutions we develop are used around the world.¹³⁴

Apart from these clusters, there is a number of others that merit to be mentioned such as the Pirkanmaa Safety and Security Cluster in Tampere; the Bavarian IT Security and Safety Cluster in Regensburg¹³⁵; the European Defense and Economic Network Cluster in Lyon¹³⁶; and the Malvern Cyber Security Cluster in Herefordshire, UK.¹³⁷ Within the Netherlands, Holland Space Cluster should be mentioned, as well as Start-Up Delta.¹³⁸ What these examples show is that HSD is already among the principal security clusters worldwide, and that depending on its strategy, it has ample room to expand its remit of activities both in the Netherlands and abroad.

5.2A Typology of Clusters

Based on the benchmark analysis of the nine clusters in paragraph 3.1, three archetypes of clusters can be discerned (see Table 2 below). The first type (A) consists of clusters which are characterised by homogeneity among their members, and in which the public sector takes the lead and cooperation takes place in a highly formalised manner. The second archetype (B) is characterised by a high degree of heterogeneity among their members and a greater share of private sector initiative, with collaboration taking on a more loosely coordinated form. The third, and final, archetype (C) also has a high degree of heterogeneity among their members (although less pronounced than in the case of type B), and employs a combination of public-private initiatives and semi-formalised cooperation. SIGNUM Berlin, Brainport Eindhoven and Aerospace Toulouse all correspond to Type C, lending support for an institutional setup analogous to Type C.

Table 2 **Typology of Clusters**

Distinguishing factors	Type A	Type B	Type C
Participants	Homogeneity of participants	Heterogeneity of participants	Heterogeneity of participants (less pronounced than in Type B)
Degree of formalisation	Formalised cooperation	Organic cooperation	Semi-formalised cooperation on a case-by-case basis
Role private/public actors	Public sector takes the lead	Private sector takes the lead	Combination of private and public initiatives
Collaboration	Collaboration between cluster partners throughout large part of the process	Collaboration between partners centered on specific parts of the process	Collaboration between partners both on specific and throughout the process

The composition of a cluster in all its diversity is not based on a *pick and mix* of characteristics. Rather, judging from the three archetypes it becomes clear that there is a clear synergy between the role of the public sector, the heterogeneity of the participants and the nature and intensity of collaboration between the partners. In cases where an apparent connection between cluster characteristics (SIGNUM, Aerospace Toulouse and Brainport) existed, these clusters tended to have similar characteristics. All three clusters were rich in both private as well as public initiatives, and intra-cluster collaboration oftentimes had a semi-formalised character.¹³⁹

5.3 Factors for Success

A cluster's relative success can be measured in a number of ways. Factors that qualify as successful achievements could include growing a cluster's turnover; to gain independence from subsidies (if classified as a goal by the cluster in question); the creation of formal and informal modes of collaboration (both internal and external); to contribute to employment growth; to act as a positive spin-off for the region, both in economic and social terms (for example in the form of successful products that contribute to addressing societal challenges); or when the cluster generates innovative products and research, or fosters process innovation.¹⁴⁰

A benchmark analysis of the ten clusters described in paragraph 3.2 based on the above criteria revealed that SIGNUM Berlin, Brainport Eindhoven and Aerospace Toulouse are the best performing clusters. These three clusters outperform others in terms of meeting their organisational goals, the extent to which they successfully grew their turnover, with respect to gaining financial independence, the functionality of their network (i.e., growth, success of collaboration within the network, etc.), their innovative character, the creation of employment, and the extent to which they act as a positive spin-off for the region and society at large.¹⁴¹

Based on these experiences, HSD has been formulating its own factors for success to make it succeed in the long run. These consist of ten criteria¹⁴²:

Table 3 **Success Factors for the Development of Clusters**

Factors	Action
1 Policy	Prioritise the realisation of an integrated approach to security
2 Internationalisation	Internationalise all actions and organise profile-enhancing events
3 Cooperation	Organise a stable basis able to stimulate the security sector
4 Knowledge institutions	Position knowledge institutions as engine for education and research in the security domain
5 Innovation and R&D	Create, facilitate or acquire high profile projects
6 Entrepreneurs	Attract and develop leading companies
7 Capital and investments	Launch a development fund and attract capital investments
8 Quality of living	Help create an attractive living and business environment in the region
9 Human Capital	Attract talent to meet the increasing demand for human capital
10 Infrastructure	Create the necessary infrastructure to support other factors for succes

According to the 2013 Policy Research report, HSD has already met its targets on three factors (infrastructure, human capital and enabling environment), and is making progress on the others. Apart from these factors, the NIAS itself mentions that '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.'¹⁴³ In that regard, the HSD partners that head the different innovation houses play a critical role in determining the success of HSD.

6 – Innovation Projects and Financing Initiatives

The Hague Security Delta is already an organisation that can nurture innovation projects, whether in the Netherlands or abroad. But to achieve critical mass and staying power, HSD and its partners will want to find additional projects to link and contribute to. The NIAS sets out the principal axes for initiatives to be pursued.

6.1 The National Innovation Agenda for Security as Identification Tool

The principal aim of HSD being to bring together triple-helix partners to jointly engage in security innovation projects, the NIAS proposes a framework to channel its ambitions towards creating a procurement agenda grounded in a revenue model (*verdienmodel*) which yields economic and societal returns on investment.

The NIAS is built around six themes, which comprise a number of innovation key focus areas. These are:

Table 4 Themes of the NIAS

Security Themes	Innovation Key Focus Areas
Partnerships in Networks and Systems	1 Management of Demand Articulation: One Government
	2 Learning From Incidents and Drills
	3 Value Creation in Triple-Helix Innovation
Social Innovation for Security in Society	4 Social Innovation and Self-organising Capacity
	5 Awareness: Perception versus Reality
	6 Security by Design in Urban Facilities and at Events
Resilient Critical Infrastructure	7 Identification and Definition of 'Critical'
	8 Cyber Security 'Internet of Things'
	9 Chain Approach to Cyber Security
Action-Oriented Information Provision	10 Networked Information at Interchanges
	11 Identification and Prediction of Deviant Behaviour
	12 Establishing and Guaranteeing —Digital—Identity
Observation with Unmanned Systems	13 Vision and Concept Development for Operations with Unmanned Sensor Platforms
	14 Operational Autonomy of UAVs
Process Information in and between Professional Organisations	15 Integrated Action with Heterogeneous Teams
	16 Linking Current Reality—Virtual Environment

Turning words into action, various HSD members and associated partners have expressed an interest to commit to pulling the cart with respect to various of the innovation key focus areas. In the NIAS, various stakeholders are identified as lead parties for the respective focus areas. A number of these stakeholders reaffirmed their commitments. For instance, the Ministry of Defence indicated its commitment to focus areas 13 and 14; DITSS and Tilburg University to focus areas 4,6 and 11; Twente University to focus areas 4, 5 and 6; KPN to focus areas 7, 8, 9, 10, 11, and 12; and Thales to focus areas 9 and 16. The Ministry of Economic Affairs wishes to link with creative industries with respect to focus areas 2,6, 11 and 16, and wants to be a co-lead partner for area 13. NCTV will contribute to implementing the NIAS through the Ministry of Justice's Security through Innovation Agenda,¹⁴⁴ and intends to be a co-lead partner on focus area 1.

6.2 Implementing the NIAS: From Ideas through Investments to Social Impact

The adoption of the NIAS is not an end in itself, but should lead to meaningful investment into innovations in security and safety which have earnings potential and also make a marked contribution to improving safety and security in our society, and to achieve economic and social value-added in the process.

HSD plans to be involved in all key focus areas of the NIAS. To provide further focus to implementing the NIAS, it has formulated a strategy on how to get innovations from the drawing board to production. This plan relates to HSD's Urgentieprogramma 2015-2018 and is centred around five themes, or programmes:

- 1 Weak signals and the capacity to anticipate: how to deal with an overflow of data in making sense of the world around us? And how can we improve our capacity to act?
- 2 Interconnected security and the internet of things: what consequences for our critical infrastructure, how this is operated and its impact on society.
- 3 Crime and Conflict in Cyberspace: more of the same? How does cybercrime affect our daily lives, and how can it be best combated?
- 4 Forensics Unchained: How can the use of forensics be expanded in the coming years, and how do linkages with IT help to increase its applications?
- 5 Structural Use of Unmanned Systems: How will the range of applications of UAVs expand, and what consequences does this have for commercial operations?

The principal aim of HSD being to bring together triple-helix partners to jointly engage in security innovation projects, the NIAS proposes a framework to channel its ambitions towards creating a procurement agenda grounded in a revenue model (verdienmodel) which yields economic and societal returns on investment.

What these themes have in common is that they are all concerned with the need to improve and ensure access to sufficient and reliable data and information. Today, security hinges more than ever on the ability to access and process reliable information. Hence, ensuring that the right organisations and the right individuals have access to critical information, and that information flows are sufficiently protected, is a major aspect in improving our safety and security.

To move from programmes to projects, an important impetus can be provided by launching customers, who would procure the fruits of such projects once they become available. One key launching customer is the Ministry of Security and Justice. In November 2014, it issued an Innovation Agenda, consisting of seven innovation themes. These include:

- 1 how to deal with changing societal conditions such as demographic and economic change;
- 2 the impact of increased social interaction, mostly through social media and how this changes (perceptions) of security;
- 3 big data;
- 4 the protection of privacy and personal identity;
- 5 security and law enforcement in cyberspace;
- 6 the role of IT in controlling our devices (the internet of things); and
- 7 how to deal with the incessant growth of technological innovations and their myriad applications.¹⁴⁵

The Ministry expresses the ambition that in 2015, 'a tailored set of instruments will be created to help further the capacity for innovation'¹⁴⁶ For now, these themes are not linked to any specific investment or procurement agenda for the ministry.

6.3 Projects in Security Innovation Linking to the NIAS

HSD and its partners engage in a host of ongoing security innovation projects that fall within the ambit of one or more of the themes described in the NIAS. The list below is to provide stakeholders an overview of ongoing or soon-to-be-commenced projects, engaged in by HSD or non-HSD partners, the aims being 1) to provide suggestions on projects where collaborations can be sought or 2) to given the reader an idea of some current directions in security innovation--both at home and abroad.

Table 5 Selected Security Innovation Projects

Theme	Project Description	Initiators/Partners
Partnership in Networks and Systems	<p>COBACORE 'seeks to close the collaboration gaps between stakeholders involved in post-crisis recovery. 2013-2016. The main purpose is to counter collaboration gaps in disaster recovery efforts by developing methods for community-wide collaboration efforts.'¹⁴⁷ COBACORE has developed the COBA-Curriculum educational-portal, in order to facilitate knowledge transfer between communities.</p> <p>http://www.cobacore.eu</p>	TNO University of Ulster German Red Cross Dutch Red Cross Tilburg University
Partnership in Networks and Systems	<p>The Hague Security Delta regularly organises HSD Cafés 'around key security topics relevant for companies, governments and research institutions. From cyber security to critical infrastructure, the Cafés serve to inform partners and those interested and offer a place for building bridges within the triple-helix. They provide an excellent opportunity to meet new business partners, bring along contacts, expanding knowledge and shape the debate on key security issues of the future. The HSD Cafés are an example of the <i>knowledge development</i> mission of HSD and take place at the HSD Campus in The Hague.'¹⁴⁸</p> <p>www.thehaguesecuritydelta.nl</p>	The Hague Security Delta
Partnership in Networks and Systems	<p>The European Space Agency (ESA) and TNO are cooperating on a 'number of research projects for the demonstration of the performance and possibilities of new MMICs in Gallium-Nitride (GaN) technology. ESA is highly interested in this technology because of the robustness and high power capability.'¹⁴⁹</p> <p>https://www.tno.nl</p>	TNO,ESA
Partnership in Networks and Systems	<p>The project DRIVER will 'substantially contribute to strengthening the European Crisis Management arena by means of its innovative demonstration concept the DRIVER enabling dimension, i.e. distributed test-bed. The project will:</p> <ul style="list-style-type: none"> • Address the current (and, after the project's end, future) needs in the Crisis management field developing the DRIVER Portfolio of tools DRIVER help professional responders and society to adaptively cope with crisis by addressing their needs. • Create a more comprehensive view on crisis management & develop a common European Crisis Management culture and understanding by creating and fostering a DRIVER Community • Achieve innovation based on testing and adaptation of existing tools & ideas • Design integrated solutions that build long term societal resilience to help crisis managers to work in, and with communities affected by crisis • Improve and demonstrate the effectiveness of learning solutions aimed at improving the Crisis Management competencies of professionals and communities in the European Union.'¹⁵⁰ <p>www.driver-project.eu</p>	TNO Haaglanden Security Region E-Semble and others
Social innovation for Security in Society Areas	<p>The BESECURE project 'aims to support local policymakers in the creation, enhancement and implementation of security policies in urban zones. The BESECURE project intends to improve our understanding of the urban security landscape (factors and actions that have a bearing on urban security), and to make best practices communicable from one urban area to another.'¹⁵¹</p> <p>http://www.besecure-project.eu</p>	TNO University of Ulster Fraunhofer Universität Freiburg ITTI Ltd.



Theme	Project Description	Initiators/Partners
Social innovation for Security in Society Areas	<p>The House (theme: Event Safety, Crowd management, National/Urban Security): 'Assist the practitioners in charge of planning the security of European major events; it will contribute to the elaboration of a common European major events security planning framework and will facilitate the adoption of a common policing approach at European Union level. Testing of the provision of coordination standards, elaborated in a number of previous UNICRI coordinated projects, during major events in Europe. The final project output will be the publication of User Guidelines for security planners on how to make the best use of the House for planning the security of major events in Europe.'¹⁵²</p> <p>http://www.thehouse-majorevents.org</p>	<p>Ministry of Security and Justice European Commission, DG Enterprise and Industry UNCRI</p>
Social innovation for Security in Society Areas	<p>Integral Area Protection – The Hague International zone: 'The national innovation centre of the Dutch security cluster (HSD Campus), which has been established in 2014, will also accommodate a <i>real-time intelligence field lab</i>. This living lab will primarily be used as an experimental facility for comprehensive protection of the international zone.'¹⁵³</p> <p>https://www.thehaguesecuritydelta.com</p>	<p>TNO Thales Siemens HSD</p>
Social innovation for Security in Society Areas	<p>TNO ACE – Advanced Concept Development & Experimentation: Testing new technologies and concepts for Defence in a realistic environment is a costly operation: many people and resources are involved. This has prompted TNO to develop its Advanced Concept Development & Experimentation Environment, otherwise known as <i>TNO ACE</i>. This is a virtual world in which experiments can be methodically conducted on, say, new weapon systems. This means considerable cost and time savings for Defence.'¹⁵⁴</p> <p>https://www.tno.nl</p>	<p>TNO</p>
Social innovation for Security in Society Areas	<p>Living Lab Stratumseind 2.0 is a project launched by the municipality of Eindhoven to improve the livability and economic viability of one of the city's main streets in its entertainment district.</p> <p>http://ditss.nl/stratumseind-wordt-proeftuin/</p>	<p>DITSS TU Eindhoven Philips ILI Fonteys Eindhoven 365</p>
Resilient critical infrastructure areas	<p>CIPRN – 'Critical Infrastructure Preparedness and Resilience Research Network – Critical infrastructure protection: modeling, simulations and analysis. they have build a virtual centre of shared and integrated knowledge and expertise. Goal: to form the foundation for the European infrastructure simulation and analysis centre.'¹⁵⁵</p> <p>https://www.ciprnet.eu</p>	<p>Fraunhofer IAIS ENEA TNO</p>
Resilient critical infrastructure areas	<p>E-Sponder: 'Real-time data-centric technologies and applications, which will provide actionable information and communication support to first responders that act during abnormal events (crises) occurring in critical infrastructures. This information will enable improved control and management, resulting in real time synchronization between forces on the ground (police, rescue, fire-fighters) and out-of-theatre command and control centres. (...) In the area of critical infrastructure, Rijkswaterstaat, under the auspices of the Ministry of Infrastructure and the Environment (Ministerie van Infrastructuur en Milieu), has an innovation agenda 2015-2020 which includes a host of projects relating to water security for which relevant parties can register to partake in.'¹⁵⁶</p> <p>http://www.e-sponder.eu/</p>	<p>EXUS S.A. (Coordinator), Greece University of Modena and Reggio Emilia, Italy Crisisplan BV, The Netherlands PROSYST Software GmbH, Germany</p>

Theme	Project Description	Initiators/Partners
Resilient critical infrastructure areas	<p>The Shared Research Programme (SRP) Cyber Security is a research programme 'spanning several years, in which TNO, in collaboration with several business partners, develops the knowledge and know-how needed to create concrete products and services that enable our partners to stand up to future cyber threats. The programme includes projects that focus on addressing problems that our partners share with each other but don't want or feel able to resolve on their own.</p> <p>About half of these projects are financed by the government, which thus encourages innovation that fails to take off through other channels. Our current phase involves market research, charting all of our possible partners, their interests and motives for participation in an SRP and their willingness to invest. This primarily occurs in discussions with our clients. TNO's Cyber Security Lab in The Hague is associated with this project.'¹⁵⁷</p> <p>www.tno.nl</p>	TNO
Resilient critical infrastructure areas	<p>SBIR Cyber Security II: 'Innovation being pushed by digitization is an important dimension for economic growth, and for society as a whole. To ensure a safe and open cyber-domain, it is important that opportunities and threats in cyberspace are managed well, and that fundamental rights are protected.'¹⁵⁸</p> <p>http://www.rvo.nl</p>	Ministries of Security and Justice, Interior, Economic Affairs, Finance and Infrastructure Coblue Digital Intelligence Group IC3D Media InnoValor Intrinsic ID ZiuZ Forensics
Resilient critical infrastructure areas	<p>Horizon 2020: Digital Security: Cyber security, Privacy and Trust: The role of ICT in Critical Infrastructure Protection, Information driven Cyber Security Management, Trust e-Services, Value-sensitive technological innovation in Cyber Security. Total budget is € 50,210,000. Deadline for project proposals is 27-08-2015.¹⁵⁹</p> <p>http://ec.europa.eu/programmes/horizon2020/</p>	European Union
Resilient critical infrastructure areas	<p>Horizon 2020: Disaster-Resilience: Safeguarding and Securing Society, including adapting to climate change: Several projects. Total budget € 76,730,000. Deadline for project proposals is 27-8-2015.¹⁶⁰</p> <p>http://ec.europa.eu/programmes/horizon2020/</p>	European Union
Action –Oriented Information Provision	<p>ePoolice: 'Development of an environmental knowledge repository of all relevant information and knowledge, including scanned information and derived, learned or hypothesized knowledge, as well as the metadata needed for credibility and confidence assessment, traceability, and privacy protection management. A key part of this process is semantic filtering for identification of data items that constitutes weak signals of emerging organised crime threats, exploiting fully the concept of crime hubs, crime indicators, and facilitating factors. goal; detection and prediction of organised crime.'¹⁶¹</p> <p>https://www.epoolice.eu/</p>	Thales Europol
Action –Oriented Information Provision	<p>Horizon 2020: Fight Against Crime and Terrorism Several projects. Total budget is € 42,160,000. Deadline for project proposals is 27-8-2015.¹⁶²</p> <p>http://ec.europa.eu/programmes/horizon2020/</p>	European Union

Theme	Project Description	Initiators/Partners
Action –Oriented Information Provision	TEC4SE 'aims to improve the operation decision-making process in the security domain. This is achieved by collecting and connecting as much information as possible so as to connect information streams. The result is an improved view on the regional security situation.' ¹⁶³ http://www.twentesafetyandsecurity.com/	Twente Safety and Security Thales
Observation with Unmanned Systems	As part of its Security through Innovation programme, 'the NCTV launched a Small Business Innovation Research (SBIR) track focused on innovative solutions against mobile unmanned systems, including drones.' ¹⁶⁴ www.rvo.nl	NCTV Fox-IT

Today, security hinges more than ever on the ability to access and process reliable information. Hence, ensuring that the right organisations and the right individuals have access to critical information, and that information flows are sufficiently protected, is a major aspect in improving our safety and security.



To support security innovation initiatives, HSD created, in conjunction with the Hague Municipality and InnovationQuarter, the HSD Development Fund (*Stimuleringsfonds*), which supplies co-financing provided by the Municipality of The Hague. Its goal is to help start-ups traverse the *valley of death*, i.e. to overcome difficulties in the start-up phase. The criteria for awarding financial support include their 'relevance to the security domain, the innovativeness of the ideas, the level of public-private or private-private collaboration, and their potential for creating additional market opportunities.'¹⁶⁵ So far, eleven initiatives have benefited from support from the Fund. (see table 6)

Table 6 **Projects Receiving Support from the HSD Development Fund**

Theme	Project Description	Initiators/Partners
Partnership in Networks and Systems	<p>Blood in the Spotlights: 'The main aim of the project is to develop a spectral camera to support forensic investigators determine the age of blood stains on an objective and non-invasive manner. This will improve the efficacy and efficiency of punitive law.'¹⁶⁶</p> <p>https://thehaguesecuritydelta.com</p>	<ul style="list-style-type: none"> Forensic Technical Solutions (FTS), Netherlands Forensic Institute (NFI), Academic Medical Centre (AMC), Cosine and the Public Prosecution Service (OM).
Social innovation for Security in Society Areas	<p>Eventcloud is creating a 'platform for open and closed event data and security features. The platform's goal is to increase the security at events and at the same time decrease security costs, making events more profitable and assuring the existence of free-of-charge public events.'¹⁶⁷</p> <p>https://thehaguesecuritydelta.com</p>	<ul style="list-style-type: none"> Future Events, Proost BV, Incentro, KPN
Resilient critical infrastructure areas	<p>Foxguard is a detection tool that can be used by organisations to find out whether or not their computers have fallen victim to digital espionage or a cyber attack.'¹⁶⁸</p>	<ul style="list-style-type: none"> Fox-IT, TU Delft, Dreamsolution, Philips, Greenpeace, PWC
Resilient critical infrastructure areas	<p>Threadstone Cyber Security 'delivers a solution to detect and report vulnerable spots in ICT systems. The Threadstone solution consists of advanced scanners and works entirely from the European Cloud- therefore no expensive hardware, software or install costs are applicable. The main customers are Web Developers, Web Designers, Infrastructure specialist, ICT companies.'¹⁶⁹</p> <p>https://www.threadstone.eu/</p>	<ul style="list-style-type: none"> ThreadStone, TNO
Action –Oriented Information Provision	<p>The ultimate objective of Futurebase (HSD Development Fund) is to 'support the conduct of faster and more powerful strategic analyses by automating parts of current research approaches, to process more valuable and diverse data, in a less labor-intensive manner. This will also include more powerful analytical possibilities that contribute to identifying, appreciating and presenting security threats and opportunities in an early phase of development. Thus, the project connects to the overall objectives of the National Security Innovation House of The Hague Security Delta.'¹⁷⁰</p> <p>https://www.thehaguesecuritydelta.com</p>	<ul style="list-style-type: none"> HCSS, Leiden University Campus the Hague, KB, AGT, SurfSara
Action –Oriented Information Provision	<p>Digital Evidence Dashboard is a product that makes it possible for non-technical detectives to determine in an early stage which digital evidence could be of relevance. 'It will provide technology assistance on critical analysis and scenario-based thinking (What type of visualisation is appropriate for large datasets?), with decision support (When to escalate to a digital forensics expert?) and with the modelling and formal description of user, crime and evidence profiles (How can knowledge be modelled?).'¹⁷¹</p> <p>https://www.tracksinspector.com/?p=178</p>	<ul style="list-style-type: none"> In-pact, Tracks Inspector, TNO, SZW, FIOD
Action –Oriented Information Provision	<p>The mission of Tokenizer is to eradicate passwords within 5 years from now and introduce a new standard of security. 'Tokenizer is a new service that makes two-factor authentication available and affordable for any company or organisation around the world. Only using usernames and passwords to protect your private or business data is not enough in 2014. Huge web services, governments and companies are hacked on a daily basis. Tokenizer adds an extra layer of security to all your logins and can be easily deployed by any system administrator or developer. No extra hardware needed. With Tokenizer installed on your mobile, you can safely log in to your account with just one finger's move.'¹⁷²</p> <p>https://www.tokenizer.com</p>	<ul style="list-style-type: none"> Tokenizer, HSD, The Hague Municipality, European Union

Theme	Project Description	Initiators/Partners
Action –Oriented Information Provision	<p>The Crisis Communication Game project focuses specifically on developing a training for the network aspect of crisis communication. 'A team consisting of TNO, T-Xchange, Netherlands Institute of Safety (IFV) and Crisisplan is developing a serious game aimed at training crisis communication consultants. By playing this game, consultants will learn how to quickly map out the relevant network, gather and distribute information and harmonize the message with the other partners. The conceptual game and the training are expected to be available by April 2015.'¹⁷³</p> <p>www.decrisiscommunicatiegame.nl</p>	<p>TNO T-Xchange Netherlands, Institute of Safety, Crisisplan</p>
Action –Oriented Information Provision	<p>Mister eXtra is 'developing a tool for preventing traces being effaced or become unusable during forensic analyses. Detectives will be able to see results directly at the crime scene without having to send the traces to a laboratory first. This increases the chances of criminals being caught.'¹⁷⁴</p>	<p>NFI TU Delft Descin BVDA</p>
Observation with Unmanned Systems	<p>The Sam Outdoor project 'aims to develop an autonomous robot for monitoring purposes in e.g. the port of Rotterdam. Of course this project is executed in cooperation with the Port authority of Rotterdam, but also Trigion security, the Technical University of Delft and the high-tech start-up Robot Security Systems will be working on the ambitious project. For this project, multiple robots will cooperate with each other to guard against intruders, but also a site to check for suspicious circumstances. You can think for example of open containers and suspiciously parked cars.'¹⁷⁵</p> <p>https://www.thehaguesecuritydelta.com/sam-outdoor</p>	<p>Port of Rotterdam TU Delft Trigion Robot Security Systems</p>
Process Information in and between Professional Organisations	<p>Total Blackout is a serious game that helps users from different critical sectors, like energy and telecom, prepare for crises.'¹⁷⁶</p> <p>https://www.thehaguesecuritydelta.com/hsdstimuleringsfonds</p>	<p>Pax Ludens TNO DPI Information House T-Xchange (Thales) Vopak Stedin</p>

Depending on the kind of project envisaged, innovative businesses are likely to seek additional financial support beyond what can be secured through HSD and its partners. In order to help such businesses -SMEs in particular- to find financial support, HSD recently issued a concise but detailed overview of financing initiatives that are available to HSD and its partners, both at home and abroad.¹⁷⁷ This guide is available online and to be updated every three months. In addition, HSD is able to support and facilitate businesses in finding the right financing opportunities at the local, regional or international levels, at all stages of the innovation cycle and linked to the NIAS.

In view of HSD's objectives and evolution, five programme lines are likely to be further developed in 2015:

- 1 **Integrated Area Protection, The Hague International Zone;**
- 2 **Cyber security & vital infrastructure** (e.g. Center for cyber expertise and Testbed project);
- 3 **Event security** (with focus on living labs, event cloud, and lessons learnt from the Nuclear Security Summit);
- 4 **UAVs and downstream activity;** and
- 5 **Secure IT real time intelligence labs** (in cooperation with Police Academy and Security Regions).

These programmes are robust enough in terms of financing available and partner commitments, offer opportunities for HSD partners across all innovation houses, and help to establish 'signature' projects that demonstrate the cluster's innovation ability which can be marketed abroad. In other words, they promise good earnings potential in the long run for the security sector as a whole, and deliver evident security benefits to society.

HSD is able to support and facilitate businesses in finding the right financing opportunities at the local, regional or international levels, at all stages of the innovation cycle and linked to the NIAS.

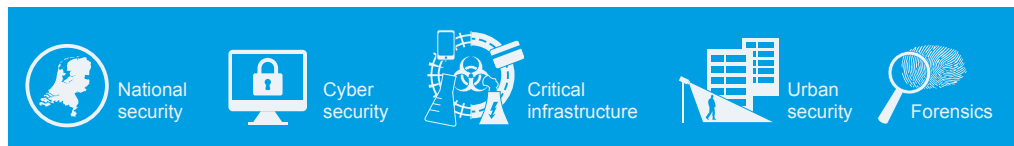
7 – HSD Infographic

The infographic below shows the results achieved by the Hague Security Delta in 2014. It illustrates among other things that HSD itself is about to exit the valley of death in that it has shown modest but solid growth in the past year, even if the after-effects of the recent economic crisis still reverberate. In particular, it highlights the growth of its international network, the increase in outreach and exposure, and the steady development of the HSD campus.

Facts and Figures The Hague Security Delta

January – December 2014

The Hague Security Delta (HSD) is the largest security cluster in Europe. In this Dutch cluster – with important regional hubs in The Hague, Twente, and Brabant – businesses, governments, and knowledge institutions work together on security innovations and knowledge. They share a common goal: more business activity, more jobs, and a secure world.



Partners

Goal: 100 partners (paying)

11 Founding Partners

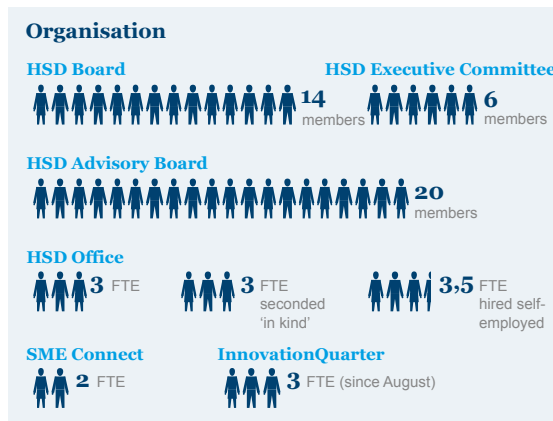
12 Premium Partners

AGT, Bosch, Deloitte, ENAI, InnovationQuarter, KvK, NFI, Rabobank, HCSS, Twynstra Gudde, Van Aetsveld, VHP

73 Network Partners (contract)

+ 31 Potential Partners in the Funnel

+ 26 Platforms and Government Organisations (non-paying)



Initiatives	Master-/Year Plan
HSD Campus	Human Capital
✓ National Innovation Centre	✓ Cyber Security Academy
✓ 5 Innovation hubs	✗ HSD Cyber Security Traineeship
✓ Incubator facilities	✓ Security Talent Portal
✓ Business complex	
✓ Real Time Intelligence Lab	Remaining
✓ Serious Gaming Lab	✓ HSD Development Fund
✗ Cyber Incident Experience Lab	✓ International Acquisition Platform
Living Labs	✓ HSD Board
✓ International Zone	✓ HSD Executive Committee
✓ Secure Societies II	✓ HSD Advisory Board
✓ CSI The Hague II	✓ HSD Office
✓ Event Security	✓ SME Connect
✓ ENCS	✓ InnovationQuarter
✓ Cyber Resilient City	✓ International knowledge bridges
✗ Future Policing	

Figure 13a The Hague Security Delta Facts and Figures (2014) Source: HSD

HSD Products

- National Innovation Agenda for Security (NIAS)
- Finance Guide
- Value Propositions NL: secure digital gateway
- 5 Issue briefs
- Drones report
- HSD strategy and urgency programme
- Trusted Networks Initiative
- Partners in Business/Netherlands-Singapore Cyber Project
- Memorandum of Understanding (MoU)
- Knowledge network and maps per HSD topic area

HSD Events / 'Powered by'

- Opening HSD Campus
- NSS Innovation Room
- Nuclear Knowledge Summit
- TEDx Binnenhof
- TEDx Hague Academy
- Secure Societies
- ASIS Europe Conference & Exhibition
- Bi-weekly HSD Café
- Help the first responder
- 'Cyber Security, een zaak voor de directie'
- 'Ondernemersplein' The Hague
- Information session HSD Development Fund
- Alert Online: Cyber Halloween
- Mobile Unconference
- The Hague Tech Inspiration Event
- Holland Strikes Back
- WTHX

Occupancy HSD Campus

December 2014

90%

Total 19 organisations

Consortia

Facilitated new consortia **14**

Accompaniment consortia HSD Development Fund **11**

- FutureBase
- Tokenizer
- ThreadStone
- Foxguard
- Sam Outdoor
- Total Blackout
- Blood in the Spotlight
- Digital Evidence Dashboard
- Mister eXtra
- Eventcloud
- The Crisis Communication Game

SME Connect (Chamber of Commerce)

Realised **270** connections between

- 138 entrepreneurs ↔ HSD (intake)
- 85 entrepreneurs ↔ HSD partners
- 23 entrepreneurs ↔ Potential customers
- 24 entrepreneurs ↔ Potential financiers
- 8 entrepreneurs ↔ Knowledge institutions
- 13 entrepreneurs ↔ Other experts
- 38 HSD partners ↔ 9 Consortia being developed
- 9 entrepreneurs ↔ Public (speaker/sponsor)
- 16 entrepreneurs ↔ HSD Campus (work space)
- 72 entrepreneurs ↔ Relevant HSD events

International acquisition

Region The Hague

5 businesses and organisations

6 conferences

Communication

Newspapers and magazines

- FD
- Telegraaf
- AD
- De Posthoorn
- Den Haag Centraal
- Security Management
- Beveiliging
- De Ingenieur
- MRDH
- PM
- Technisch Weekblad
- Sunday Times
- Daily Star

News websites

- Washington Post
- Euronews
- NOS
- NU.nl
- Elsevier
- Computable
- Automatiseringsgids
- Management Team
- Den Haag FM
- Security.nl
- Security Bistro
- Emerge

Radio and television

- NOS 8 o'clock news
- RTL News
- RTV West
- BNR Nieuwsradio
- Radio 1
- Radio 2

HSD website

Visitors per month

Opening HSD-Campus and NSS: 3,474

TV show 'De Ondernemersclub': 6,232

Twitter

Goal: 1,000 followers

1,300

619

HSD Newsletter

Number of subscribers

805

1,265

LinkedIn

Goals: group 500 followers; company page 250 followers

Company page: 700

Group: 469

340

200

Financial

Revenue

Budget

Realisation

Costs

Budget

Realisation

Result: +32,835

*Including travel expenses € 36,854

Figure 13b The Hague Security Delta Facts and Figures (2014) Source: HSD

As the annual report announced, 2015 should be the year of implementation. The past year helped to establish HSD firmly in the policy, knowledge and business environment in the Netherlands, but 2015 is to be dedicated to further developing existing initiatives such as the living labs, and to provide innovators and investors with further guidance in securing or committing funding for security innovation projects, not just by way of the Development Fund, but also by pointing interested parties to other financial resources, in the Netherlands and abroad.

Conclusions

The creation of HSD at this juncture could not have been more timely. It responds to a need to enhance our safety and security in a time when doing so has become more complex than ever before. At the same time, it helps to create synergies across a range of key sectors of the economy, giving a boost to economic growth and help improve security in society as well.

The survey of Dutch security in this report shows that while the Netherlands is in many respects a safe country to live and work, security and safety threats continue to evolve, posing challenges in terms of available knowledge and capacity to everyone in the security chain, from government departments to law enforcement, the business sector, and the general public alike.

Hence, security and safety cannot be taken for granted, but require continuous innovation both in the technological and the societal realm. Technological innovations such as CSI tools, living labs, sensory networks, realtime information provision, cyber capacities and other means will make a difference in making security more seamless and affordable. Improved coordination between organisations and individuals across society will also be critical: it can result in more effective dissemination of and timely access to information, and improve the capacity of organisations –in a coordinated effort- to respond to instant calamities or worrying societal trends.

In some respects, threats to our safety and security seem bigger than ever before. But we also have a better perspective on these threats, and continue to refine our tools to assess risks and to decide where extra efforts are needed. Part I of this report showed that among the security themes that could receive more attention are physical security and cyber security. As it is, these are areas that HSD and its partners are well equipped to address, in particular as these areas cut across the innovation houses and thus bring the full gamut of HSD partners' expertise to the table. What is more, these areas are also very suitable for SMEs to be active in, which can then also benefit from the synergy effects that being part of a cluster such as HSD brings.

In developing its portfolio and approach to security, HSD also mirrors developments in security at home and abroad. The thematic approach within HSD is well suited to deal with safety and security issues that cross borders, whether it's cybercrime, the impact of climate change or international jihadism. Neither the government nor society on its own can handle the challenges that we face. This is why cooperation in a triple-helix structure that brings together government agencies, knowledge institutions and business is so important. And this is also why public-private partnerships are the preferred mode of operation for projects relating to security innovation. Furthermore, the international partnerships that HSD has concluded not only help to entrench its position as

Europe's largest security cluster, but also add a critical dimension to responding to global security challenges. In this way, the very way how HSD is organised enables us to start preparing today to better deal with the safety and security threats of tomorrow.

The past year has been important in the development of HSD. The Nuclear Security Summit gave it added momentum, as did the trade missions it undertook, the new international partnerships it concluded, and the successful drones conference that it contributed to. Meanwhile, the National Innovation Agenda for Security points the way in how to spur further innovation in security, helping businesses in the Netherlands to develop a veritable niche market with a worldwide reputation. In fact, the achievements of HSD to date show that the triple-helix structure is already bearing fruit, which is reflected in the growth of HSD itself.

Making the NIAS work, creating new business, and increasing its added value to Dutch society are the key missions for HSD in 2015. The upcoming Global Conference on Cyberspace will be an important landmark event in that regard, not simply in showcasing the technological prowess of Dutch cyber-related companies, but to show that with HSD as the national security cluster, our country has an integrated approach to improving safety and security through innovation and triple-helix participation. In this way, the Hague Security Delta remains at the forefront of nurturing new forms of cooperation in security innovation that bring real economic and societal benefits to the Netherlands and beyond.

Endnotes

- 1 CIA World Factbook, available at <https://www.cia.gov/library/publications/the-world-factbook/geos/nl.html>
- 2 The Netherlands ranks no. 20 out of 162 on the Global Peace Index and no. 4 out of 125 on the Good Country Index. See <http://www.visionofhumanity.org/#page/indexes/global-peace-index/2014/NLD/OVER> and <http://www.goodcountry.org/overall>
- 3 As the Study *Zicht overheden op beschermen burgers en bedrijven* of the Dutch Court of Audit notes: 'Het beschermen van burgers en bedrijven is een samenspel tussen publieke partijen op verschillende bestuurlijke niveaus en private partijen. Het is daarom van belang dat er samenhang is tussen de activiteiten van de verschillende partijen.' See Dutch Court of Audit (Algemene Rekenkamer), *Zicht Overheden op Beschermen Burgers en Bedrijven* (The Hague, November 13, 2014). Available at http://www.rekenkamer.nl/Publicaties/Onderzoeksrapporten/Introducties/2014/11/Zicht_overheden_op_beschermen_burgers_en_bedrijven, p. 6
- 4 HSD Jaarverslag, p. 4
- 5 See NCTV Ipsos *Risico- En Crisisbarometer Basismeting Juni 2014*, p. 3
- 6 Not to be confused with the fire at Chemie-Pack, in the same industrial zone, in 2011
- 7 See e.g. *F5 Networks: Helft van de Bedrijven Was in 2014 Doelwit van Cyberaanval* | Infosecurity Magazine, accessed March 12, 2015, <http://infosecuritymagazine.nl/2014/12/08/f5-networksk-helft-van-de-bedrijven-was-in-2014-doelwit-van-cyberaanval/>; *Opmars Cyber Security, Fd.nl*, accessed March 12, 2015, http://fd.nl/frontpage/Print/Bijlage/FD_Outlook/638767/opmars-cyber-security.
- 8 See Tim Sweijs et al., *Time to Wake Up*, The Hague: HCSS (2014), available at <http://www.hcss.nl/reports/time-to-wake-up/155/>.
- 9 CBS Statline online, *Geregistreeerde criminaliteit; regio (indeling 2013) 2005-2012*. Overall, the number of registered incidents decreased from 1,278,000 to 1,139,000 (about 11%), with some regions seeing significant declines including Utrecht (-20%), Rotterdam (-7%) and The Hague (-9%). Amsterdam figures only fell marginally.
- 10 Compare Centraal Bureau voor de Statistiek, *Veiligheidsmonitor 2008*, p. 49 and *Veiligheidsmonitor 2012*, p. 51
- 11 In Dutch: It is part of the objectives of HSD to help 'Lange termijn visie in functie van maatschappelijke veiligheid Integraal veiligheidsbeleid ontwikkelen en uitvoeren met nadruk op vooruitkijken en anticiperen; dit beleid moet op het juiste niveau verbonden worden met de nationale veiligheidsagenda.' *Security Delta Eindrapport*, Policy Research Corporation, 2013, , p. 13
- 12 See also as defined in ETTIS, *European Trends and Threats in Society*, Seventh Framework Programme European Union, Conceptual Foundations of Security, p. 8
- 13 See also discussed in Lonneke van Noije and Karin Wittebrood, *Sociale Veiligheid Ontleuteld*, Sociaal en Cultureel Planbureau, (The Hague: 2008), and Pinar Bilgin, *Individual and societal dimensions of security*. *International Studies Review*, Vol. 5 (2003), pp. 203–22.
- 14 Marjolein van Asselt et al., *Physical Safety: A Matter of Balancing Responsibilities*. Dutch Scientific Council for Government Policy, (The Hague: 2012), pp. 23-25
- 15 See also Maarten Gehem, Willem Auping, Willem Oosterveld, *Building Cyber Resilient Cities* (The Hague Security Delta, 2014).
- 16 These distinct areas borrow from the divisions between HSD innovation houses, and also reflect distinctions as made for instance in the ETTIS and EvoCS projects. See www.thehaguesecuritydelta.com, www.ettis-project.eu and www.evocs-project.eu
- 17 *A Secure Netherlands in a Secure World – International Security Strategy* (June 21, 2013), p. 8. Available at <http://www.government.nl/documents-and-publications/notes/2013/06/21/international-security-strategy.html>
- 18 Ibid., p. 13
- 19 Ibid., p. 11
- 20 See, for a comprehensive overview of crime and statistics in the Netherlands, CBS et al., *Criminaliteit en Rechtshandhaving 2013*, The Hague, November 5, 2013, available at <http://www.cbs.nl/nl-NL/menu/themas/veiligheid-recht/publicaties/publicaties/archief/2014/2014-criminaliteit-rechtshandhaving-2013-pub.htm>
- 21 *HSD Issue Brief No. 5: Disaster Resilience and Climate Change* (The Hague Security Delta), accessed February 2, 2015, <https://thehaguesecuritydelta.com/news/newsitem/220-hsd-issue-brief-no-5-disaster-resilience-and-climate-change>.
- 22 Ibid., p. 2
- 23 See WRR report, *Vertrouwen in de Buurt* (2005), available at http://www.wrr.nl/fileadmin/nl/publicaties/PDF-Rapporten/Vertrouwen_in_de_buurt.pdf and CBS Bevolkingsonderzoek, *Te veel of te weinig inkomen voor de buurt? Dan een grotere kans om te verhuizen* (2014), available at <http://www.cbs.nl/NR/rdonlyres/FC1A7314-CCF2-4E29-B746-B1CED6A0512E/0/20140104b15art.pdf> and
- 24 *Strategie nationale veiligheid, bevindingenrapportage*, (November 8, 2013), p. 10-11 available at <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/11/08/strategie-nationale-veiligheid-bevindingenrapportage.html>
- 25 Ole Wæver, *Identity, Migration, and the New Security Agenda in Europe* (St. Martin's Press, 1993), p.23
- 26 ETTIS, *European Trends and Threats in Society*, Seventh Framework Programme European Union, Conceptual Foundations of Security, p. 8
- 27 ETTIS, *European Trends and Threats in Society*, Seventh Framework Programme European Union, Conceptual Foundations of Security, p. 10
- 28 Sijbren de Jong, Joshua Polchar, Willem Oosterveld, Stephan de Spiegeleire and Anne-Fleur van Veenstra, *The Fission of Power: Flex and Flux in an Age of Fragmentation* (HCSS, March 2015).
- 29 See e.g. Paul Collier, *Exodus: How Migration is Changing Our World* (New York: Oxford University Press, 2013)
- 30 Sijbren de Jong, Joshua Polchar, Willem Oosterveld, Stephan de Spiegeleire and Anne-Fleur van Veenstra, *The Fission of Power: Flex and Flux in an Age of Fragmentation*.
- 31 See e.g. AIVD report, *The Transformation of Jihadism in the Netherlands: Swarm Dynamics and New Strengths*, available at <https://www.aivd.nl/publicaties/aivd-publicaties/@3114/transformation/> and Steven Erlanger and Katrin Bennhold, *'Dangerous Moment for Europe' as fear and resentment Grow*, *The New York Times*, January 7, 2015.
- 32 See e.g. Monique Kremer et al., *Hoe ongelijk is Nederland? Een verkenning van de ontwikkeling en gevolgen van economische ongelijkheid*, Dutch Scientific Council for Government Policy, (The Hague, June 4, 2014), available at <http://www.wrr.nl/publicaties/publicatie/article/hoe-ongelijk-is-nederland-een-verkenning-van-de-ontwikkeling-en-gevolgen-van-economische-ongelijkhe/>
- 33 *European Commission - PRESS RELEASES - Press Release - Paving the Way for European Energy Security*, accessed January 26, 2015, http://europa.eu/rapid/press-release_IP-14-585_en.htm.
- 34 Ministerie van Veiligheid en Justitie, *Zakelijk omgaan met economische veiligheid Nederland* | *Nationaal Coordinator Terrorismebestrijding en Veiligheid*, nieuwsbericht, (June 10, 2014), pp. 25-27 <https://www.nctv.nl/actueel/nieuws/zakelijk-omgaan-met-economische-veiligheid-nederland.aspx>.
- 35 Analistennetwerk Nationale Veiligheid, *Nationale Risicobeoordeling, 2013*, <https://www.nctv.nl/onderwerpen/nv/strategie-nationale-veiligheid/documenten-snv/index.aspx>, p. 50.
- 36 See *EvoCS Codebook deliverable 3.1*, p. 12, available at www.evocs-project.eu
- 37 *A Secure Netherlands in a Secure World – International Security Strategy* (June 21, 2013). Available at <http://www.government.nl/documents-and-publications/notes/2013/06/21/international->

- security-strategy.html.
But see also Sijbren de Jong, Joshua Polchar, Willem Oosterveld, Stephan de Spiegeleire and Anne-Fleur van Veenstra, *The Fission of Power: Flex and Flux in an Age of Fragmentation*.
- 38 Ministerie van Veiligheid en Justitie, *Nationale Cyber Security Strategie - Rapport - Rijksoverheid.nl*, rapport, (February 28, 2011), <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/02/28/nationale-cyber-security-strategie.html>, page 6
 - 39 *What Will Happen If Countries Carve up the Internet?*, The Guardian, accessed February 2, 2015, <http://www.theguardian.com/media-network/media-network-blog/2013/dec/17/internet-fragmentation-eugene-kaspersky>
 - 40 *Nationale Cyber Security Strategie 2* (October 28, 2013), p. 15, available at <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/10/28/nationale-cyber-security-strategie-2.html>
 - 41 See *Rijksbegroting 2015 ch. VI veiligheid en Justitie* at <http://www.rijksoverheid.nl/onderwerpen/prinsjesdag/miljoenennota-rijksbegroting-en-troonrede/prinsjesdagstukken>
 - 42 *Security Delta Eindrapport*, Policy Research Corporation, 2013, p. ii
 - 43 *A Secure Netherlands in a Secure World – International Security Strategy* (June 21, 2013), pp. 8-9. Available at <http://www.government.nl/documents-and-publications/notes/2013/06/21/international-security-strategy.html>
 - 44 *Rijksbegroting 2015, Ch. X Defensie*, (September 16, 2014), pp. 10-15, available at <http://www.rijksoverheid.nl/documenten-en-publicaties/begrotingen/2014/09/16/x-defensie-rijksbegroting-2015.html>
 - 45 See <https://www.nctv.nl/onderwerpen/nv/strategie-nationale-veiligheid/>
 - 46 See NCTV, *Voortgangsbrief Nationale Veiligheid*, 8 November 2013
 - 47 See *Beleidsbrief Internationale Veiligheid – Turbulente Tijden in een Instabiele Omgeving*, November 14, 2014. Available at <http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/11/14/beleidsbrief-internationale-veiligheid-turbulente-tijden-in-een-instabiele-omgeving.html>
 - 48 See http://www.rijksbegroting.nl/2015/voorbereiding/miljoenennota,kst199382_5.html
 - 49 See http://www.rijksbegroting.nl/2015/voorbereiding/begroting,kst199430_4.html (own translation)
 - 50 See http://www.rijksbegroting.nl/2015/voorbereiding/begroting,kst199430_4.html (own translation).
 - 51 *Ibid.* (own translation).
 - 52 See http://www.rijksbegroting.nl/2015/voorbereiding/begroting,kst199407_5.html (own translation)
 - 53 See http://www.rijksbegroting.nl/2015/voorbereiding/begroting,kst199410_5.html
 - 54 See Dutch Scientific Council for Government Policy, *Consistent maatwerk – handreikingen voor dossieroverstijgend risico- en veiligheidsbeleid*, (The Hague, 26 June 2014), available at http://www.wrr.nl/fileadmin/nl/publicaties/PDF-Rapporten/Consistent_Maatwerk.pdf, and specifically pp. 13-14.
 - 55 Dutch Court of Audit (Algemene Rekenkamer), *Zicht Overheden op Beschermen Burgers en Bedrijven* (The Hague, November 13, 2014). Available at http://www.rekenkamer.nl/Publicaties/Onderzoeksrapporten/Introducties/2014/11/Zicht_overheden_op_beschermen_burgers_en_bedrijven (own translation).
 - 56 *Ibid.*, p. 19
 - 57 *Ibid.*, p. 35
 - 58 Ministry of the Interior and Kingdom Relations, *Rijksbrede Trendverkenning: Strategiebeoordeling Rijksbreed*, p. 34. Available at <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/06/17/rijksbrede-trendverkenning.html>
 - 59 *Rijksbrede Trendverkenning*, p. 35
 - 60 Another report on wifi security highlights the difference between cable and wireless technology, saying that wireless poses significant security hazards in comparison to traditional cable technology. Among the chief threats and risks that the paper identifies are: 1) wardriving, or roaming for unprotected networks to break into; 2) creating rogue (i.e. fake) access points for accessing internet services, 3) MAC-spoofing, which entails taking the identity of an existing hardware address of a device that is linked to protected networks, 4) contamination of devices, 5) unauthorized access to networks, 6) DDoS attacks, which render devices or websites inaccessible to their users, 7) message modification, whereby access is obtained to a real existing network through a rogue access point.
 - 61 See *AIVD Annual Report* (The Hague, April 23, 2014), p. 11, available at <https://www.aivd.nl/publicaties/aivd-publicaties/@3096/annual-report-2013/>
 - 62 See <https://www.aivd.nl/publicaties/aivd-publicaties/@3112/transformatie/>
 - 63 See <https://www.aivd.nl/publicaties/aivd-publicaties/@3114/transformation/>
 - 64 NCTV *Ipsos Risico- En Crisisbarometer Basismetting October 2014*, p. 3
 - 65 NCTV *Ipsos Risico- En Crisisbarometer Basismetting October 2014*, p. 3
 - 66 NCTV *Ipsos Risico- En Crisisbarometer Basismetting October 2014*, p. 16
 - 67 Dutch Court of Audit (Algemene Rekenkamer), *Zicht Overheden op Beschermen Burgers en Bedrijven* (The Hague, November 13, 2014), p. 22 Available at http://www.rekenkamer.nl/Publicaties/Onderzoeksrapporten/Introducties/2014/11/Zicht_overheden_op_beschermen_burgers_en_bedrijven
 - 68 See reiterated in the most recent update of the International Security Strategy, *Beleidsbrief Internationale Veiligheid – Turbulente Tijden in een Instabiele Omgeving*, p. 5ff
 - 69 EvoCS is a project funded through the 7th Framework Programme (FP7), involving nine partners from across the EU, including HCSS.
 - 70 This is done by way of evaluating and coding of representative publications that reflect the views of different constituencies. These are Government, Civil Society, the Private Sector, the Media, Academia and NGOs. The project differentiates between six core values. these are 1) physical safety and security, 2) territorial integrity and security, 3) environmental and ecological security, 4) social stability and security, 5) cultural identity and security, 6) political stability and security, 7) economic prosperity and security. The concepts of security that the project examines are made up of different dimensions, being a mixture of the kinds of security threats and the way they are assessed, the actors involved, the levels at which they take place and the ethical issues that are concerned.
 - 71 For Parliament a selection was made of 100 Parliamentary debates. For newspapers, some 200 articles each has been coded from *De Volkskrant* and *De Telegraaf*. The data represents items issued between 31 Oct 2013-1 November 2014.
 - 72 See *HSD Strategie En Urgentieprogramma 2015-2020*, p. 3
 - 73 See *oplegnotitie, 8-10-14*, p. 2.
 - 74 *HSD Strategie En Urgentieprogramma 2015-2020*, p. 3
 - 75 See *Convenant Nationale Samenwerking Veiligheid En Innovatie*, https://www.thehagusecuritydelta.com/images/Convenant_DITSS_TSS_HSD.pdf.
 - 76 See <https://thehagusecuritydelta.com/news/newsitem/278-hsd-named-as-one-of-10-leading-innovation-hubs>
 - 77 The HSD Foundation 'acts as driving force, responsible for the implementation of the strategic direction and the international promotion of the security cluster, through trade missions, communication and acquisition of companies, institutions and conferences' See <https://thehagusecuritydelta.com/about-hsd>
 - 78 Policy Research Corporation, *Security Delta Eindrapport*, n.d.
 - 79 Scientific Council for Government Policy *Towards a Learning Economy*, synopsis (The Hague, November 4, 2013), p. 21.

- 80 See *HSD Jaarverslag 2014*, p. 5; *Strategie- en Urgentieprogramma 2015-2020* p. 14, and <http://www.hcatopsectoren.nl/human-capital-agenda-s.html>
- 81 See for more information <https://www.csacademy.nl>
- 82 See <https://www.thehaguesecuritydelta.com/securitytalent>
- 83 This approach was further developed by Nick Bostrom at the Humanity Institute at Oxford. See e.g. Nick Bostrom, *Existential Risk Prevention as Global Priority*, *Global Policy* 4, no. 1 (February 2013): 15–31
- 84 See NCTV, *Nationale Risicobeoordeling* 6, p. 69, available at <https://www.nctv.nl/onderwerpen/nv/>. For a detailed explanation of how risk assessments are put together, see Ministry of Security and Justice, *Werken met scenario's, risicobeoordeling en capaciteiten in de Strategie Nationale Veiligheid*, The Hague, March 2013, available at <https://www.nctv.nl/onderwerpen/nv/strategie-nationale-veiligheid/>
- 85 See *National Risk Assessment* 6, available at https://english.nctv.nl/themes_en/national-security/index.aspx
- 86 See also laid out in detail in *De Veiligheid van Nederland in Kaart*, Ministry of Infrastructure and the Environment (The Hague, January 16, 2015), available at <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2015/01/16/eindrapportage-vnk-de-veiligheid-van-nederland-in-kaart.html>
- 87 See *National Innovation Agenda for Security 2015*, p. 37
- 88 See *Strategie- and Urgentieprogramma 2015-2020*, p.15
- 89 See *Oplegnotitie, 8-10-14*, p. 3
- 90 See <http://www.innovationquarter.nl/>
- 91 See *Strategie- and Urgentieprogramma 2015-2020*, p. 8
- 92 See HSD, *Strategie- en Urgentieprogramma 2015-2020*, p. 8
- 93 See European Commission report, at http://ec.europa.eu/enterprise/policies/security/documents/index_en.htm
- 94 See, for more detail, <https://thehaguesecuritydelta.com/projects/project/62-hsd-international-a-secure-gateway-to-europe>
- 95 *HSD Annual Report 2014*, p. 5
- 96 See <https://www.thehaguesecuritydelta.com/about-hsd>
- 97 *Security Delta Eindrapport*, Policy Research Corporation, 2013, p. 12
- 98 In Dutch, 'de vier o's van overheid, onderzoek, opleiden en ondernemen.' See Foreword by Rob de Wijk, NIAS report (Dutch version), p. 3.
- 99 NIAS, p. 33
- 100 *Security Delta Eindrapport*, Policy Research Corporation, 2013, p. 2
- 101 Based on *HSD Jaarverslag*, p. 6 and HSD, *Strategie- en Urgentieprogramma 2015-2020* (2014), pp. 29-30. Available at https://thehaguesecuritydelta.com/images/Strategie_en_urgentieprogramma_2015-2020.pdf
- 102 Total Turnover of the region in the security sector, including members and non members of the cluster.
- 103 *Masterplan Security and Research- Berlin Brandenburg*. Available at http://www.sicherheit.berlin-brandenburg.de/de_sbb_strategie.phtml.
- 104 Ibid.
- 105 Industry Overview : <http://investottawa.ca/industries/aerospace-defence-security>.
- 106 Elyea, Jeff. *A Billion Dollars in Annual Sales and 10,000 Employees Makes Ottawa's Defence and Security Industry One of Ottawa's Major Knowledge-Based Sectors*. Invest Ottawa. Accessed September 15, 2014; <http://investottawa.ca/a-billion-dollars-in-annual-sales-and-10000-employees-makes-ottawas-defence-and-security-industry-one-of-ottawas-major-knowledge-based-sectors/>. Aerospace, *Defence and Security, Ottawa - Canada's Aerospace, Defence and Security Capital*. Invest Ottawa, 2013.
- 107 *Fact Sheet Ottawa Aerospace and Security*; <http://investottawa.ca/wp-content/uploads/2013/09/ADSFactSheet.pdf>
- 108 Ibid.
- 109 *The Security Network – Background*, 2014. <http://thesecuritynetwork.org/about-us/background/>.
- 110 Ibid.
- 111 *Aerospace Valley*. Aerospace Valley Cluster, 2014. <http://www.aerospace-valley.com/en>.
- 112 *Aerospace Valley Midi-Pyrenees & Aquitaine World Competitiveness Cluster*. Aerospace Valley, n.d. <http://www.aerospace-valley.com/sites/default/files/documents/av-plaq-uk-bd-3005-3-bat.pdf>.
- 113 *About Us. Aerospace Valley*, 2014. <http://www.aerospace-valley.com/en/page/about-us>.
- 114 Porter, M., E. (2010). *International Cluster Competitiveness Project*, Institute for Strategy and Competitiveness. Harvard Business School; Richard Bryden, Project Director.
- 115 Aerospace Valley. *Aerospace Valley – the Leading Aerospace Cluster in France Contribution to the Workshop on EU GNSS Programs (GALILEO & EGNOS)*. Brussels, June 4, 2013.
- 116 *Aerospace Valley – the Leading Aerospace Cluster in France Contribution to the Workshop on EU GNSS Programs (GALILEO & EGNOS)*. Brussels, June 4, 2013.
- 117 EACP, *Aerospace Valley*, 2008. <http://www.eacp-aero.eu/index.php?id=26>; *Aerospace Valley – the Leading Aerospace Cluster in France Contribution to the Workshop on EU GNSS Programs (GALILEO & EGNOS)*. Brussels, June 4, 2013; *Aerospace Valley Midi-Pyrenees & Aquitaine World Competitiveness Cluster*. Aerospace Valley, 2014. <http://www.aerospace-valley.com/sites/default/files/documents/av-plaq-uk-bd-3005-3-bat.pdf>.
- 118 *Brainport Eindhoven Pocket Flyer*, October 2013. www.brainport.nl/over-brainport/downloads/10-13-bp-pocketflyer-nl-v5. *Corporate Brochure Brainport Region Eindhoven*. Brainport Development NV, 2012.
- 119 *About Brainport*. Accessed September 19, 2014. <http://www.brainport.nl/en/about-brainport>.
- 120 *Trophy Cabinet - About Brainport - Brainport Region Eindhoven*, 2014. <http://www.brainport.nl/en/about-brainport/trophy-cabinet>. *Brainport Monitor 2012 - Summary. Power of the Smartest*. Brainport Region Eindhoven, 2012.
- 121 *Corporate Brochure Brainport Region Eindhoven*. Brainport Development NV, 2012.
- 122 *Dutch Institute for Technology Safety & Security Officieel Gelanceerd « Brainport Development*. Accessed September 22, 2014. <http://www.brainportdevelopment.nl/dutch-institute-for-technology-safety-security-officieel-gelanceerd>.
- 123 *DPI - Dutch Polymer Institute - About*. Accessed September 22, 2014. <http://www.polymers.nl/About?session=8ri7vrf3lovtk7o2ietgaqrnf4>.
- 124 *Charting a New Course. DPI Annual Report 2013*. Dutch Polymer Institute (DPI), 2013, p. 17.
- 125 *DPI - Dutch Polymer Institute - Partners*. Dutch Polymer Institute. Accessed September 25, 2014. <http://www.polymers.nl/About/Partners>.
- 126 Ibid, p. 7.
- 127 See *Innovatiekrediet | RVO.nl. Rijksdienst Voor Ondernemend Nederland*. Accessed September 25, 2014. <http://www.rvo.nl/subsidies-regelingen/innovatiekrediet>.
- 128 *'High-Tech Cluster' on the West Coast*, 2013. <http://www.gaccwest.com/en/industries/information-technology-it/high-tech-cluster/>.
- 129 *Corporate Story Oost NV*. Accessed September 26, 2014. <http://www.oostnv.nl/page/corporate-story-oost-nv>.
- 130 *Organisatie. Oost NV*. Accessed September 29, 2014. <http://www.oostnv.nl/page/organisatie>.
- 131 *Oost NV*, 2014. <http://www.oostnv.nl/>.
- 132 *Prestaties En Kerncijfers*. Accessed September 26, 2014. <http://www.oostnv.nl/page/prestaties-en-kerncijfers>.
- 133 *Partners*. Accessed September 26, 2014. <http://www.oostnv.nl/page/partners>.
- 134 <http://www.twentesafetyandsecurity.com/> (own translation)
- 135 See <http://www.it-sicherheit-bayern.de/itsecurity/>
- 136 See <http://www.edencluster.com/>
- 137 See <http://www.malvern-cybersecurity.com/>

- 138 See <http://www.hollandspacecluster.nl/> and <http://www.startupdelta.org/>
- 139 Ibid.
- 140 Sophie Roborgh and Anika, Snel, *Internationale Clusters in Vergelijkend Perspectief – Best Practices Voor de Opzet van The Hague Security Delta*, (The Hague: The Hague Centre for Strategic Studies (HCSS), December 2012), 6.
- 141 Ibid.
- 142 According to the *Security Delta Eindrapport*, Policy Research Corporation, 2013, pp. 14-15
- 143 NIAS (English version), p. 27
- 144 See <https://www.nctv.nl/onderwerpen/prioriteiten2014/innovatie/> (in Dutch)
- 145 See <http://www.rijksoverheid.nl/documenten-en-publicaties/publicaties/2014/11/27/innovatie-agenda-veiligheid-en-justitie.html> (in Dutch only)
- 146 Ibid.
- 147 *COBACORE Partners*, Mapbox, accessed February 23, 2015, <http://a.tiles.mapbox.com/v3/jaymes88.h281jmel/page.html>.
- 148 *New at The Hague Security Delta: HSD Café*, *The Hague Security Delta*, accessed February 23, 2015, <https://thehaguesecuritydelta.com/news/newsitem/158-new-at-the-hague-security-delta-hsd-cafe>.
- 149 *Gallium-Nitride MMIC Development for ESA*, TNO, accessed February 23, 2015, <https://www.tno.nl/en/focus-area/defence-safety-security/information-superiority/gallium-nitride-mmic-development-for-esa/>
- 150 *IMPACT | Driver Project*, accessed February 23, 2015, <http://driver-project.eu/content/impact>
- 151 *BESECURE - Home*, accessed February 23, 2015, <http://www.besecure-project.eu/>.
- 152 *The House*, accessed February 23, 2015, http://www.unicri.it/topics/major_events_security/the_house/
- 153 *Integral Area Protection - The Hague International Zone*, *The Hague Security Delta*, accessed February 23, 2015, <https://www.thehaguesecuritydelta.com/projects/project/37-integral-area-protection-the-hague-international-zone>.
- 154 *TNO ACE: Advanced CD&E Environment*, TNO, accessed February 23, 2015, <https://www.tno.nl/en/focus-area/defence-safety-security/missions-operations/tno-ace-advanced-cd-e-environment/>.
- 155 *CIPRNet: Summary*, accessed February 23, 2015, <https://www.ciprnet.eu/summary.html>.
- 156 *Lopende Innovatieprojecten Waterveiligheid*, accessed February 23, 2015, http://www.rijkswaterstaat.nl/zakelijk/innovatie/innovatie_voor_waterveiligheid/lopende_projecten/.
- 157 *Shared Research Programma: SRP-AM*, TNO, accessed February 23, 2015, <https://www.tno.nl/nl/aandachtsgebieden/industrie/flexible-free-form-products/additive-manufacturing/shared-research-programma-srp-am/>.
- 158 *Shared Research Programma: SRP-AM*, TNO, accessed February 23, 2015, <https://www.tno.nl/nl/aandachtsgebieden/industrie/flexible-free-form-products/additive-manufacturing/shared-research-programma-srp-am/>.
- 159 *H2020-DS-2015-1*, accessed February 23, 2015, <http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-ds-2015-1.html#tab2>.
- 160 *H2020-DRS-2015*, accessed February 23, 2015, <http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-drs-2015.html>
- 161 *E-POOLICE | Cultural, Communication and Computing Research Institute | Sheffield Hallam University*, accessed February 23, 2015, <http://www.shu.ac.uk/research/c3ri/projects/e-poolice>.
- 162 *H2020-FCT-2015*, accessed February 23, 2015, <http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-fct-2015.html>.
- 163 *Twente Safety & Security*, accessed February 23, 2015, <http://www.twentesafetyandsecurity.com>
- 164 *Aanbesteden van Innovaties (SBIR) | RVO.nl*, accessed February 23, 2015, <http://www.rvo.nl/subsidies-regelingen/aanbesteden-van-innovaties-sbir>.
- 165 See <https://www.thehaguesecuritydelta.com/projects/project/56-hsd-development-fund-second-edition>
- 166 *Blood in the Spotlights - Project HSD Development Fund*, *The Hague Security Delta*, accessed February 23, 2015, <https://thehaguesecuritydelta.com/projects/project/54-blood-in-the-spotlights-project-hsd-development-fund>.
- 167 *HSD Development Fund (Second Edition)*, *The Hague Security Delta*, accessed February 23, 2015, <https://thehaguesecuritydelta.com/projects/project/56>.
- 168 *HSD Development Fund (Second Edition)*, *The Hague Security Delta*, accessed February 23, 2015, <https://thehaguesecuritydelta.com/projects/project/56>.
- 169 *HSD Development Fund (Second Edition)*, *The Hague Security Delta*, accessed February 23, 2015, <https://www.thehaguesecuritydelta.com/projects/project/56-hsd-development-fund-second-edition>.
- 170 *The Hague Security Delta*, accessed February 23, 2015, <http://www.thehaguesecuritydelta.com/>
- 171 Hans Henseler, *The Digital Evidence Dashboard Project*, *Tracks Inspector*, accessed March 13, 2015, <https://www.tracksinspector.com/?p=178>.
- 172 *Tokenizer: Features*, accessed February 23, 2015, <https://tokenizer.com/features.html>.
- 173 *DeCrisisCommunicatieGame.nl* |, accessed February 23, 2015, <http://www.decrisiscommunicatiegame.nl>
- 174 *The Hague Security Delta*, accessed February 23, 2015, <http://www.thehaguesecuritydelta.com/>. See also http://www.nederlandsforensischinstituut.nl/over_het_nfi/nieuws/2014/tu-delft-en-nfi-ontvangen-subsidie-voor-ontwikkeling-sporenindicator.aspx?cp=34&cs=578
- 175 *The Hague Security Delta*, accessed February 23, 2015, <http://www.thehaguesecuritydelta.com/>
- 176 *HSD Development Fund (Second Edition)*, *The Hague Security Delta*, accessed February 23, 2015, <https://thehaguesecuritydelta.com/projects/project/56>.
- 177 See the Financing guide, available at <https://www.thehaguesecuritydelta.com/projects/project/58-hsd-financeguide-dutch>. This guide is made possible by: The Municipality of The Hague, InnovationQuarter, Chamber of Commerce, Netherlands Enterprise Agency, Rabobank, Twente Safety and Security and the Dutch Institute for Technology Safety and Security.

Publication information

Innovation, Investment and Impact: HSD and the State of Dutch Security 2015 – Clustering Knowledge and Innovation for Security and Prosperity

© 2015, The Hague Security Delta

A publication of

The Hague Security Delta
Wilhelmina van Pruisenweg 104
2595 AN Den Haag
T +31(0)70 2045180
info@thehaguesecuritydelta.com
www.thehaguesecuritydelta.com
 @HSD_NL

Contributors

Willem Th. Oosterveld, Tim Sweijs,
Sijbren de Jong and Joshua Polchar

Editorial support

Ida Haisma, Joris den Bruinen and
Chantal de Niet

Assistance

Vesela Miladinova, Laurin Nabuko Hainy,
Juncal Garayzábal-Fernandez Gonzalez,
Pim ten Haaf and Jacques Mukena

Design

Studio Koelewijn Brüggewirth

Printing

ANDO Graphics

Photography

Hilbert Krane (cover photo, p. 17, p. 52),
Aerialtronics (p. 16), National Police (p. 20),
Robert Huijberts (p. 35), Joris Fisselier
(Infographic, pp. 57-58)

The contributors would like to acknowledge the kind support provided by partners of HSD in putting together this report. The views expressed here are those of the contributors only, and not attributable to HSD or any other party.

