Letter of 9 April 2015 from the Minister of Security and Justice to the House of Representatives on the state of the National Safety and Security Strategy

A focus on security is the basis of a free and safe society for all citizens. The government has various strategies at its disposal to safeguard security, in collaboration with its crisis partners, both public and private. These include the National Safety and Security Strategy (SNV), the Counterterrorism Strategy and the Cyber Security Strategy. The common thread running through all three strategies is the need to protect critical infrastructure.

I am writing to inform you about developments regarding the SNV, specifically the following interrelated matters:
1. revision of the SNV;
2. review of critical infrastructure;
3. enhancement of crisis management.

A great deal has already been accomplished in the realm of national security. Further measures have been planned in the above areas to protect national security even more effectively. These improvements will be described in greater detail below.

In my letter of 16 December 2014[1] I informed you about the objectives jointly formulated by the Safety Regions Council and myself in line with the recommendations of the Hoekstra Evaluation Committee. These common objectives lie in the areas of water safety and evacuation, enhanced risk and crisis management in nuclear incidents, and social continuity. These objectives are part of the Strategic Agenda of the Safety Regions Council. This summer you will be sent a progress report on the aims and follow-up of the other improvement measures being taken in response to the recommendations of the Evaluation Committee.

1. Revision of the National Safety and Security Strategy

The SNV facilitates a government-wide approach protecting national security interests[2] from potential social disruption. The strategy rests on three pillars: analysing threats and risks,

1 Parliamentary Papers, House of Representatives, 2014-2015 session, 29517, no. 90.
2 The interests that must be protected are territorial security, physical security, economic security, ecological security, and social and political stability.

focusing on capabilities that need to be strengthened[3] and ensuring the continuity of critical infrastructure.

When it was devised in 2007, the SNV was seen internationally as one of the first documents of its kind. Since that time a great deal of work has gone into realising the goals of the strategy. For example, numerous threat scenarios have been developed and evaluated, and experts have conducted capability analyses that have led to various enhancement measures.

Over the past year the parties involved have taken stock of all their experiences and concluded that when it comes to national security, oversight and leadership are as necessary as ever. To maintain the strategy's effectiveness, the government has decided to develop it further. In what follows I would like to inform you about the proposed improvements. The key theme is increased flexibility.

National Security Profile

The current annual National Risk Assessment will be replaced by a National Security Profile, which will be released every four years. This National Security Profile will be a comprehensive analysis of the most salient risks and threats to national security (the 'all-hazard approach'), plus an overview of relevant technological and social developments. On the basis of the National Security Profile, it should be possible to conduct a separate capacity analysis to determine whether (and to what extent) the Netherlands is adequately prepared for various threats to national security. Identifying and assessing risks is an ongoing process which can be reported on periodically by means of various types of communication products. An overview of this process will be provided by the four-yearly National Security Profile.

The National Security Profile and the regional risk profiles will complement each other wherever relevant. The safety regions and crisis partners will be instrumental in the creation of the National Security Profile. The profile's findings may prompt the safety regions to update or tighten up their own regional risk profile.

The first National Security Profile will be released in 2016.

[3] A 'capability' is defined as the ability to do something, whether on the part of government, businesses or private individuals. Capacities can relate to reducing the threat, limiting its impact or improving the response.

Focusing on capabilities that need to be enhanced

The aim of the SNV remains the identification of capabilities that should be developed or enhanced to make the Netherlands better equipped to deal with disasters, crises and other incidents, and thereby to minimise social disruption to the greatest possible extent. A capability programme will be established to set priorities and make decisions about these needs. This programme will complement the National Risk Profile. The input for capability enhancement within the programme will be broad: capability analyses, evaluations of crises exercises and lessons learned from actual incidents, both in the Netherlands and abroad. Technological studies will also provide input for the capability programme if they offer scope to carry out certain tasks more effectively or more cheaply. The programme will also involve the capabilities of the safety regions and the crisis partners. The Steering Committee for National Safety and Security will monitor the progress of the programme and provide recommendations where necessary.

The House will be informed about the most important findings in this area in the periodic progress report on national security.

2. Review of policy on critical infrastructure

In the previous national security progress report of 8 November 2013[4] I undertook to review government policy on protecting critical infrastructure. The purpose of this review is to maintain a high level of protection and to take account of the evolving threat situation and society's increased dependence on this critical infrastructure. In short, we are aiming for an updated, more rigorous approach to protecting critical infrastructure. The review of what constitutes critical infrastructure in the Netherlands is now effectively complete, and I will inform you of the results below.

A clear definition and identification of critical infrastructure for the Netherlands in 2015 and a resulting policy on maintaining or heightening resilience are vital for our national security. With this in mind, the importance of a given piece of infrastructure was determined on the basis of uniform criteria and limit values for social disruption that apply to all public, private and semi-private partners. This determination was made by scoring the effects of a potential breakdown of critical processes on the basis of its economic, physical and social impact. For this purpose, critical processes were identified for each sector and then assigned to one of two categories. These categories were introduced to take account of the different types of

[4] Parliamentary Papers, House of Representatives 2013-2014, 30821, no. 19.

critical infrastructure, to help establish priorities for when incidents occur and to enable us to customise any resilience-boosting measures that must be taken.

Thanks to the joint efforts of the relevant public and private partners, the reassessment resulted in a clear, up-to-date overview of what is critical for our society, with an emphasis on social impact: a single, integrated list of critical infrastructure. As stated above, this infrastructure was then subdivided into two categories, A and B.

Category A

This includes infrastructure whose disruption, damage or failure will have the type of impact described in at least one of four impact criteria below.

- Economic impact > approx. €50 billion in damage or an approx. 5.0% drop in real income
- Physical impact: more than 10,000 dead, seriously injured or chronically ill
- Social impact: more than 1 million people afflicted by emotional problems or serious problems with basic survival.
- Domino effect: failure results in the breakdown of at least two other sectors.

Category B

This category includes infrastructure whose disruption, damage or failure will have the type of impact described at least one of four impact criteria below.

- Economic impact: > approx. €5 billion in damage or an approx. 1.0 % drop in real income
- Physical impact: more than 1,000 dead, seriously injured or chronically ill
- Social impact: more than 100,000 people afflicted by emotional problems or serious problems with basic survival.

The table on the following page contains the new list of critical infrastructure.

Revised list of critical infrastructure

Processes	Cat.	Product, service or location	Sector	Min.
National transportation/distribution of electricity	A	Electricity	Energy	Econ. Aff.
Regional distribution of electricity	B			
Gas production National transportation/distribution of gas	A	Natural gas		
Regional distribution of gas	B			
Oil supply	A	Oil		
Internet access and data traffic	TBD[5]		IT / Tel	Econ. Aff.
Speech-communication services (mobiles and landlines)				
Satellite				
Time and location services (satellite)				
Drinking water supply	A	Drinking water	Drinking water	Infrastr./ Env.
Flood defences and water management	A	- primary flood defences - regional flood defences[6]	Water	Infrastr./ Env.
Air traffic control	B	Schiphol Airport	Transport	Infrastr./ Env.
Vessel traffic service	B	Port of Rotterdam		
Large-sale production, processing and/or storage of (petro-) chemicals	B	(Petro-)chemical industry	Chemical	Infrastr./ Env.
Storage, production and processing of nuclear material	A	Nuclear industry	Nuclear	Infrastr./ Env.
Retail transactions	B	Financial transactions	Finance	FIN
Consumer financial transactions	B			
High-value transactions between banks	B			
Securities trading	B			
Communication with and between	B	Maintaining public order and	Public	Security

[5] The review of the telecom sector will take place after talks with the sector in spring 2015

[6] The government and the water authorities are currently looking at what regional water defence should qualify as critical, in accordance with the 2014 assessment methodology.

emergency services through 112 and C2000		safety	order and safety[7]	and Justice
Police deployment	B			
Availability of reliable personal and corporate data about individuals and organisations, the ability to share such data, and the availability of data systems which multiple government agencies require in order to function.	B	Digital government[8]	Public administration[9]	BZK

Resilient critical infrastructure

If a piece of infrastructure is designated as critical, this means that its failure could have far-reaching consequences for national security and that a high degree of resilience is vital. By reviewing what infrastructure is critical to the Netherlands and dividing it into two categories, the authorities will be able to adopt a more customised approach in the use of resilience-boosting instruments. Critical infrastructure will be incorporated into the existing crisis structures, given special attention within the National Academy for Crisis Management and included in the products and services catalogue of the National Cyber Security Centre. It will also be addressed in the project plan for social continuity of the Strategic Agenda (see below). The fact that a particular type of infrastructure has been designated 'critical' also has bearing on the classification of certain jobs as confidential positions.[10] This also applies to the Counterterrorism Alert System (ATb), which, it should be noted, remains in effect for the sectors that are currently connected to it. Finally, the classification 'critical' can also be used as a policy category in certain instances. This is already the case, for example, in the forthcoming Network and Information Security Directive and the Cyber Security (Data Processing and Mandatory Reporting) Act.

7 The Ministry of Defence will assess the level of importance of this sector later in 2015.

8 The competent ministries and implementing agencies are currently examining what processes and systems of digital government should be deemed vital, on the basis of the 2014 assessment methodology. After an evaluation is made of the financial impact, the processes and systems will be identified on the advice of the National Board on Digital Government.

9 The assessment of the importance of diplomatic communication will be conducted later in 2015.

10 Under the Security Screening Act jobs that have the potential to jeopardise national security can be designated confidential positions. The guidelines on confidential positions set out policy frameworks for determining which positions warrant a security screening and how thorough it should be. The policy on designating confidential positions complements the government-wide SNV.

The review also revealed that there is a need for intersectoral information-sharing and knowledge retention as regards the interdependence of different types of critical infrastructure. In my capacity as coordinating authority for national security matters, I will facilitate intersectoral consultations, working closely with the relevant organisations. The government will stay alert to possible new critical infrastructure or changes to existing critical infrastructure, in order to ensure that there is at all times a clear, up-to-date overview of what sectors should be regarded as critical for the Netherlands.

The government attaches great importance to the above-mentioned systematic, joint approach, and as Minister of Security and Justice, I am hereby expressly affirming my coordinating role. In this capacity I will keep the House informed about the state of security for our critical infrastructure by means of regular progress reports.

Common goals for safety regions

Over the past few years it has become clear that there is room for improvement in the way the government and critical organisations work together. The recent large-scale power cut underscored the importance of good teamwork. The Safety Regions Council's project Critical Partnerships (now completed) helped to show that safety regions need not only clarity regarding their role in relation to critical infrastructure but also more knowledge on the subject. With that in mind the Safety Regions Council and I have selected the theme 'social continuity' as a common goal. It is our shared ambition to work together effectively to prevent or minimise large-scale infrastructure failures or disruptions to social continuity. This summer you will be sent a progress report on the other improvement measures being taken in response to the recommendations of the Evaluation Committee.

3. Improving crisis management

The ever-changing national security context demands the most flexible possible crisis organisation whose administrative and operational functions can operate swiftly and decisively in all situations. A rapid response requires clearly delineated responsibilities and powers and a flat organisational structure. To ensure effectiveness it is important that parties that have a role to play or specific expertise to contribute are adequately involved in the preparations for and response to crises and incidents. This means that there is room for improvement in the current crisis management system. To that end I have taken the following initiatives.

Making the crisis management organisation simpler and more flexible

In consultation with the parties involved I will make the crisis organisation simpler and more flexible in order to keep step with developments. The guiding principle will be to reduce the distance between (strategic) decision-making processes and day-to-day operations. Over the course of the year, the agreements made about these changes will be incorporated into the National Handbook on Decision-Making in Crisis Situations and, if necessary, in the Ministerial Order Establishing the Ministerial Crisis Management Committee 2013. With the help of the relevant partners, the organisation and methodology of the national crisis network for situations that warrant the highest level of the Coordinated Regional Crisis Management Procedure (GRIP Rijk) will be incorporated into simple and uniform national crisis plans.

Improving nationwide operational coordination

To improve nation wide operational coordination, I have launched a project to enhance the effectiveness and efficiency of the deployment of operational crisis management capabilities (both people and other resources). This project will run until the end of this year.

Harmonising the knowledge and advisory network structure

In connection with the evaluation of the fire at Chemie-Pack Moerdijk, an undertaking was given to the House to more clearly define the structure of the knowledge and advisory networks underlying decision-making in crisis situations. The principles governing this undertaking are set down in the report ‘Unity in Diversity’ (February 2013), which introduced the roles of the ‘enquiry coordinator’ and the head of the Crisis Expert Team (CET).

In January of this year the guidelines for the knowledge and advisory structure were approved. They are intended to be used in a crisis situation to formulate appropriate, independent and integrated recommendations on decision-making. Among other things, they lay down a procedure for appointing an enquiry coordinator in the case of a national crisis and explain how this coordinator should work with his or her counterparts at regional level and the head of a CET.

We are now entering the second phase of the project to harmonise the knowledge and advisory network structure, which deals with the implementation of the models described in the guidelines. This second phase is expected to be completed in the autumn, after which point it will be possible to conduct exercises in the new structure.

Enhancing civil-military cooperation

Good civil-military cooperation is essential for effective crisis management. Working closely with my counterpart from the Ministry of Defence, I am committed to ensuring that this

partnership is as effective as possible. The safety regions and crisis partners will be even more focused on this issue in the months ahead.

At the start of this year a new catalogue was presented detailing military capabilities that can be deployed by civilian authorities. This catalogue is available in a digital, interactive format, with a view to fostering greater familiarity with the various possibilities in the field of civil-military cooperation, whether administrative, operational or media-related.

In mid-2014 the Ministry of Defence officially made available the Wildfires Support Module. The systematic deployment of heavy equipment and logistical support in this context will substantially increase the capabilities and endurance of the fire brigade in combating wildfires. Alongside these efforts the use of fire-fighting helicopters has also been enhanced and formalised.[11]

2014 also saw the opening of the National CBRN Training Centre, a shared-service centre with a multidisciplinary approach that enables ongoing cooperation among all relevant partners. The opening of the Centre represents the completion of a project that began several years ago in the context of a broader programme to deepen civil-military cooperation (ICMS).

Investing in professionalism

The government has designated a number of key instruments for maintaining, and where necessary, enhancing the quality of the national crisis organisation: education, training, exercises, testing, evaluation and lessons learned. In this context, conducting exercises is no longer an end in itself but rather a link in a larger chain, connecting prior education and training to subsequent testing, evaluating and learning, thus bringing the system full circle. At my ministry it is the National Academy for Crisis Management (NAC) that deals with the individual links in this chain.

Initially, the NAC focused on the interministerial crisis management organisation. Now the NAC is enlarging its target group; the safety regions, our partners in critical infrastructure and international partners are all important in managing a crisis. In a safe learning environment these partners can be brought into in the activities of the NAC with the aim of fostering a qualitatively better crisis management organisation.

[11] Voluntary agreement on the implementation of fire bucket operations (*Government Gazette* 2014, 23255). On 4 March a Memorandum of Understanding was signed with Belgium which makes possible the deployment of Dutch military and civilian personnel and equipment in that country for the purpose of fire-fighting.

The NAC is organising individual training courses to strengthen crisis professionals in their specific roles. These courses will be taken by around 500 crisis management professionals from all relevant public and private sectors and will focus on the advisory function, decision-making, communication and operations within the national crisis management organisation. These courses vary from introductory sessions on crisis management to master classes on current affairs. Courses will also be given on skills related to the advisory function in crisis situations and the devising of scenarios. To ensure an appropriate response following international threats and incidents, additional crisis training courses that go beyond the basic curriculum have also been given to diplomats at the missions around the world.

In addition to developing their individual talents, members of teams and organisations in the national crisis management organisation will have a chance to take part in educational programmes, organised by theme, to develop their proficiency in processes and methods. A recent theme was critical infrastructure, with an emphasis on the repercussions of a large-scale failure in the gas sector. In 2015 the theme of cyber security is on the agenda. This will be followed by themes like water and nuclear issues.

Crisis management from an international perspective

It goes without saying that security in the Netherlands does not begin and end at our national borders. Security is not just a domestic issue. It is also a matter to be addressed with other countries, international organisations, civil society groups and the business community. The government works to ensure national security mainly through its partnerships within the EU and NATO, as well as via the UN.

In the EU, legislation on the Union Civil Protection Mechanism entered into force on 1 January 2014. This mechanism promotes cooperation between the EU member states on disaster reduction and crisis management. The aim is to enhance the efficiency, effectiveness and coherence of the EU's disaster response network, with due regard for cost effectiveness.

The Netherlands' efforts in regard to national security are already aligned with the UN's global framework for action, the 'Hyogo Framework for Action (2005-2015): Building the Resilience of Nations and Communities to Disasters'. The purpose of the framework is to use risk assessments to make countries resilient to disasters.

A follow-up document has since been drafted. The Dutch government advised the UN to include six specific themes.[12] The new document, the 'Sendai Framework for Disaster Risk Reduction, 2015-2030' was adopted by 186 other countries on 18 March 2015. The all-hazard approach proposed in this framework incorporates those six themes and the elements of the crisis management cycle. It also aligns with the domains the Netherlands has designated as five critical interests in the National Safety and Security Strategy. From the Netherlands' perspective the new UN framework for action is thus generally in line with current Dutch and EU policy.

Conclusion

With these proposed improvements and modifications across the national security spectrum, some of which are already under way, we are boosting our capacity to make the Netherlands more secure and keep it that way. The further enhancement of the crisis management organisation will ensure that we are better equipped to tackle disasters and crises, today and in a rapidly changing future.

[12] Parliamentary Papers, House of Representatives 2013-2014, 22112, no. 1851.