NATIONAL SAFETY AND SECURITY STRATEGY

FINDINGS REPORT

Contents

1. Introduction ............................................................................................................................
   1.1 Background ....................................................................................................................... 
   1.2 Building blocks of the National Safety and Security Strategy ...........................................
   1.3 Results of the National Safety and Security Strategy ...........................................................
   1.4 Summary of contents ........................................................................................................ 

2. Overview of the National Risk Assessment 2012 ................................................................. 
   2.1 Introduction ....................................................................................................................... 
   2.2 Preparation of the National Risk Assessment 2012 .............................................................
   2.3 The position of the new scenarios in the risk diagram ....................................................... 
   2.4 Main outcomes of the new scenarios ................................................................................ 

3. Recommendations concerning capabilities ............................................................................
   3.1 Introduction ....................................................................................................................... 
   3.2 Recommendations arising from the NRA 2012 .................................................................
   3.2.1 Cooperation in the field of crisis management ............................................................... 
   3.2.2 Information gathering ................................................................................................... 
   3.2.3 Awareness and education .............................................................................................. 
   3.2.4 Crisis communications ................................................................................................. 
   3.2.5 International capabilities ..............................................................................................
1. **Introduction**

1.1 **Background**

Risks and uncertainties can never be ruled out: there is no such thing as 100% security. The Netherlands faces countless threats, including natural disasters, disruptions resulting from technical failures or human error, and incidents involving people or groups that deliberately wish to inflict damage or harm or that harbour other criminal intentions. Threats to national security can occur on Dutch territory or impact on Dutch interests abroad.

National security is at stake when the vital interests of the Netherlands and/or the Dutch state are under threat. The five vital interests of the Netherlands are: territorial security, physical security, economic security, ecological security, and social and political stability. The purpose of the National Safety and Security Strategy is to prevent, to the greatest possible extent, any infringement of these vital interests, which could potentially lead to social disruption.

1.2 **Building blocks of the National Safety and Security Strategy**

The National Safety and Security method makes it possible to identify and compare a wide range of potential risks and thus make well-founded decisions about what measures to take.

The risk diagram developed in the framework of the National Safety and Security Strategy helps to visualise the relatively severity and probability of the various risks (see chapter 2). Comparing risks can also be helpful when evaluating and selecting measures designed to improve national security. Which measures should be adopted straight away, which can be adopted later and which should not be adopted at all? These are political questions which the National Safety and Security Strategy must reconsider every year.

The strategy consists of three core components:

1. the National Risk Assessment (NRA)
2. the capability analysis
3. the National Safety and Security Findings Report (the present document).
1. National Risk Assessment

The first component of the National Safety and Security Strategy is the National Risk Assessment (NRA). Every year, the NRA analyses a limited number of risks that could affect the Netherlands and potentially have a disruptive effect on society. These are either risks that have not been analysed before or previously examined risks about which new facts or insights have come to light. The risks are worked up into scenarios, which are then assessed by experts from two angles. First, the assessment teams examine the scenarios on the basis of ten impact criteria that reflect the Netherlands’ five vital interests. Second, they consider the likelihood that the scenarios will actually occur. The method used to analyse and assess scenarios (scoring) also makes it possible to rate uncertain risks (i.e. risks for which there is only limited theoretical and/or empirical scientific data concerning likelihood and impact).

In 2011, the NRA was carried out for the first time by experts from the specially appointed Network of Analysts for National Security (ANV). The establishment of the network is a key step in the enhancement of the National Safety and Security Strategy. Its purpose is to provide efficient access to the expertise of the intelligence services and several renowned knowledge institutions, for the purpose of carrying out scenario analyses. The network is also meant to make a clearer distinction between scenario analysis by experts and its translation into policy by the relevant ministries.

2. Capability analysis

The second component of the National Safety and Security Strategy is the capability analysis, which is conducted on the basis of the results of the NRA. It reveals the extent to which society is equipped to prevent – or limit and manage the impact of – potential incidents as described in the scenarios.

---

1 The text of the NRA can be downloaded from the website of the National Coordinator for Security and Counterterrorism at http://english.nctv.nl.
2 The scenarios are thought experiments that consider how certain risks might develop into actual incidents or disasters, resulting in social disruption. They should in no sense be seen as predictions.
3 The ANV is a consortium consisting of the following six knowledge institutions: the National Institute for Public Health and the Environment (RIVM); the General Intelligence and Security Service (AIVD); the Research and Documentation Centre of the Ministry of Security and Justice (WODC); the Netherlands Organisation for Applied Scientific Research (TNO); the Netherlands Institute of International Relations ‘Clingendael’; and the International Institute of Social Studies (ISS) of Erasmus University Rotterdam. For the purpose of these analyses, the consortium calls in additional expertise from various sectors: the government, academia and the business community. The consortium’s core task is to perform scenario analyses connected to national security, particularly the NRA.
Based on the results of the analysis, a specially appointed working group considers which capabilities need to be enhanced in order to reduce the risks in question and better manage uncertainty. These capabilities are either specific (focused on a single risk) or broadly applicable (designed to combat several risks). Like the NRA, the capability analysis is conducted on the basis of a predetermined system.

3. Findings report
The final component of the Strategy is the preparation of the findings report. On the basis of the capability analysis, the responsible ministries jointly select certain capabilities that the experts have flagged as priorities. The selection focuses on such factors as efficiency and added value as compared with previously selected capabilities. The National Steering Committee for National Safety and Security (SNV) then presents the selected capabilities to the government for consideration. The government ultimately decides on the basis of the findings report which recommendations will be implemented.

1.3 Results of the National Safety and Security Strategy
The government has been using the National Safety and Security Strategy since 2008. Since then, 42 scenarios have been developed, five of which have subsequently been updated. On the basis of these scenarios, experts have conducted capability analyses and the government has identified capabilities that needed to be reinforced. The purpose of reinforcing certain capabilities is always to increase the Netherlands’ resistance to potential risks or to reduce the impact of those risks if a certain scenario were to actually occur. Most of these capabilities have now been addressed and enhanced; several have become ongoing processes, such as ‘performing integrated cyber threat and risk analysis’ and ‘holding strategic talks with Germany, France and the United Kingdom’. The following table provides an overview of all capabilities that have been identified as requiring reinforcement since 2008:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formulate national strategies to prepare for the distribution of scarce resources</td>
<td>In progress</td>
</tr>
</tbody>
</table>

4 A capability is defined as the ability of (central) government, private partners and the public to perform tasks whose aims include safeguarding national security. These tasks involve specific combinations of resources (e.g. material or information systems), people (e.g. civilians, members of the armed forces) and methods (e.g. procedures, plans, training exercises and public-private partnerships). Capabilities can help to reduce the likelihood and/or impact of one or more threats. They cover the entire spectrum of prevention, preparation, response, control and recovery.
<table>
<thead>
<tr>
<th>Task</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transpose EU oil crisis directive into Dutch law</td>
<td>Completed</td>
</tr>
<tr>
<td>Draft a national energy crisis plan</td>
<td>In progress</td>
</tr>
<tr>
<td>Draft a national evacuation plan</td>
<td>Completed</td>
</tr>
<tr>
<td>Examine scope for establishing national operational staff for national crises</td>
<td>Completed</td>
</tr>
<tr>
<td>Examine compliance of the Security and Justice Inspectorate with the Civil-Military Cooperation Intensification Project (ICMS)</td>
<td>Completed / Ongoing process</td>
</tr>
<tr>
<td>Develop national system for standardised communication between all levels and all administrative and operational sectors (Netcentric)</td>
<td>Ongoing process</td>
</tr>
<tr>
<td>Test robustness of communications systems</td>
<td>Completed</td>
</tr>
<tr>
<td>Boost self-reliance and civic engagement</td>
<td>Completed</td>
</tr>
<tr>
<td>Draft national flu epidemic crisis plan</td>
<td>Completed</td>
</tr>
<tr>
<td>Examine continuity of critical infrastructure</td>
<td>Completed</td>
</tr>
<tr>
<td>Analyse the impact of international shortages</td>
<td>Completed</td>
</tr>
<tr>
<td>Evaluate oil crisis mechanisms</td>
<td>Completed</td>
</tr>
<tr>
<td>Put the NRA on the European agenda</td>
<td>Completed</td>
</tr>
<tr>
<td>Draft a national crisis plan</td>
<td>Cancelled because the National Manual on Decision-Making in Crisis Situations provides adequate coverage</td>
</tr>
<tr>
<td>Strategic talks with Germany, France and the United Kingdom</td>
<td>Completed / Ongoing process</td>
</tr>
<tr>
<td>Bolster resistance of critical sectors to power cuts and ICT disruptions</td>
<td>In progress</td>
</tr>
<tr>
<td>Hold series of meetings on firm leadership in crises</td>
<td>Completed</td>
</tr>
<tr>
<td>Develop assessment framework for national crisis organisations</td>
<td>Completed</td>
</tr>
<tr>
<td>Verify current system for preventing and managing nuclear accidents</td>
<td>In progress</td>
</tr>
<tr>
<td>Reorganise crisis communications at regional level</td>
<td>Ongoing process</td>
</tr>
<tr>
<td>Establish a national information point</td>
<td>Completed</td>
</tr>
<tr>
<td>Task</td>
<td>Status</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Link NRA and regional risk profiles to capability planning at national and regional level</td>
<td>Completed</td>
</tr>
<tr>
<td>Measures to tackle criminal subversion of legitimate businesses</td>
<td>Ongoing process</td>
</tr>
<tr>
<td>Prepare national ICT crisis plan</td>
<td>Completed</td>
</tr>
<tr>
<td>Integrity guidelines (mayors, councillors and members of the municipal executive)</td>
<td>Completed</td>
</tr>
<tr>
<td>NL-Alert messaging system</td>
<td>Completed</td>
</tr>
<tr>
<td>Strengthen the judiciary</td>
<td>Completed / Ongoing process</td>
</tr>
<tr>
<td>Improve planning and information exchange/knowledge sharing between Dutch Safety Regions Council and Ministry of Security and Justice</td>
<td>Completed</td>
</tr>
<tr>
<td>Establish ICT response board</td>
<td>Completed</td>
</tr>
<tr>
<td>Establish pool of experts</td>
<td>In progress</td>
</tr>
<tr>
<td>Establish police knowledge centre</td>
<td>In progress</td>
</tr>
<tr>
<td>Strengthen the police</td>
<td>Completed / Ongoing process</td>
</tr>
<tr>
<td>Draft continuity plans for power cuts and ICT disruptions</td>
<td>In progress</td>
</tr>
<tr>
<td>Support regions in cultivating self-reliance</td>
<td>Completed</td>
</tr>
<tr>
<td>Hold high-level strategic talks with the Confederation of Netherlands Industry and Employers (VNO-NCW)</td>
<td>Completed / Ongoing process</td>
</tr>
<tr>
<td>Integrate cyber threat and risk analysis</td>
<td>Completed / Ongoing process</td>
</tr>
<tr>
<td>Identify European energy and transport infrastructures of vital importance to the Netherlands</td>
<td>In progress</td>
</tr>
<tr>
<td>Implement government response to report analysing the Netherlands’ vulnerability to espionage</td>
<td>Completed / Ongoing process</td>
</tr>
<tr>
<td>Strengthen the role of senior civil servants in crisis communications</td>
<td>In progress</td>
</tr>
<tr>
<td>Draft government proposal to strengthen the managerial role of central government</td>
<td>Completed</td>
</tr>
<tr>
<td>Increase resistance of critical infrastructure to ICT threats and cyber attacks</td>
<td>Completed</td>
</tr>
<tr>
<td>Draw up an inventory of key natural resources of vital importance to the economy and for which the</td>
<td>Completed</td>
</tr>
</tbody>
</table>
Netherlands is largely dependent on other countries
Hold training exercise for ministers and state secretaries | Completed / Ongoing process
---|---
Establish a Cyber Security Council | Completed
Draft a National Cyber Security Strategy and plan of action | Completed
Improve national-regional crisis communications | In progress
Improve crisis communications at national level | Completed
Dealing with violent loners | Ongoing process
Increase resistance to the consequences of satellite disruption due to solar storms | In progress
Voluntary agreements for safety regions and critical sectors | Ongoing process
Improve detection of attacks on networks and information systems | Ongoing process
Enhance ability to prevent and manage social catastrophes in an effective manner | In progress

**1.4 Summary of contents**

Chapter 2 briefly describes the main results of the NRA 2012. Chapter 3 presents a number of both general and specific recommendations for enhancing capabilities, based on the results of the capability analysis.

**2. Overview of the National Risk Assessment 2012**

**2.1 Introduction**

As stated in the introduction to this report, the National Safety and Security Strategy takes its cue from the annual National Risk Assessment (NRA). This chapter examines the NRA for 2012.

**2.2 Preparation of the National Risk Assessment 2012**

The present scenarios were developed independently by the Network of Analysts for National Security (ANV). Since 2011, this authoritative body has devised the annual NRA at the behest of the Ministry of Security and Justice and the National Steering Committee for
National Safety and Security (SNV). The SNV selected four types of threat for the NRA 2012, which the ANV developed into the following four scenarios:

- Digital security: Hacktivism
- Terrorism: Violent loner
- International issues: Collapse of arms control in failing state
- Social unrest: Large-scale disturbances

The following sections briefly describe the main insights of the NRA 2012.²

### 2.3 Position of the new scenarios in the risk diagram

*How to read the risk diagram*

The results of the experts’ risk assessment of each scenario are displayed in the risk diagram (see figure 1.1). The experts assessed the scenarios on the basis of ten impact criteria and estimated the likelihood that they might actually occur.

In this diagram, every scenario has a position based on the experts' assessment of its likelihood (horizontal axis) and impact (vertical axis). These two factors determine each scenario's relative risk position. The scenarios that were developed in 2012 appear in red and are underlined, while the scenarios from previous NRAs appear in black.

It is important to note that each score relates to a specific scenario and not to the broader phenomenon of which it is a part.

**Figure 1.1: Risk diagram**

- **Horizontal axis:** Highly Unlikely; Unlikely; Moderately likely; Likely; Highly likely.
- **Vertical axis:** Limited; Substantial; Serious; Very serious; Catastrophic.
- **Scenarios:** Animal rights activism; Animal rights extremism; Black ice; Chemical incident; Collapse of arms control in failing state; Confrontation between ethnic minorities and extreme right; Criminal subversion of vital businesses; Crisis outside the EU; Cyber conflict; Cyber espionage; Dyke Ring 14 flood; Extreme heat and drought; Food shortages – soya beans; Geopolitical oil supply crisis; Hacktivism; Internet exchange failure; IP network failure (ICT);

---

² The text of the NRA can be downloaded from the website of the National Coordinator for Security and Counterterrorism at http://english.nctv.nl.
Large-scale disturbances; Left-wing extremism; Malicious gas supply failure; Malicious ICT disruption in critical sector; Malicious power supply failure; Malicious prolonged electricity failure; Manipulation of public administration; Manipulation of stock market; Mass polarisation; Mild influenza pandemic; Mineral shortages; Muslim extremism; National power failure; Nuclear incident; Rail crash; Response to exogenic jihadist threat; Rhine-IJssel flood; Right-wing extremism; Satellite disruption due to solar storm; Severe influenza pandemic; Severe snowstorm; Shipping accident; Unrest in problem neighbourhoods; Unrest regarding Salafism; Very severe storm; Violent loner; Wildfire; Worst-credible coastal flood.

Considerations relating to the NRA and the risk diagram

Of all the scenarios that could be developed on the basis a particular risk, the NRA usually works up only one or two. It is possible to imagine a more – or less – serious version of a scenario, or a version with different attributes, a different narrative or different circumstances. In practice, however, the NRA develops the scenarios that provide an insight into the capabilities needed to withstand the risks in question.

Moreover, most of the risks examined in the context of the National Safety and Security Strategy are characterised by a certain degree of uncertainty. This is because they concern unusual events (for which there is little empirical data) and complex scenarios (involving multiple elements whose underlying relationships are not always clear). The experts’ individual risk assessments may accordingly vary within certain limits. The risk diagram always reflects the median score assigned by the experts.

2.4 Main outcomes of the new scenarios

This section briefly discusses the outcomes of each new scenario and the position of each scenario in the risk diagram.

Hacktivism

This scenario is set in a world where international hacktivist groups like ‘Ahackgroup’ regularly carry out cyber protests. In Europe, economic decline and high unemployment (particularly among young people) have given rise to political tension. Driven by economic motives, companies increasingly outsource their ICT needs at the lowest possible cost, making use of cloud solutions. At the end of 201X, several thousand highly-skilled ICT managers and system programmers are ‘in between jobs’. Calling themselves ‘the Malcontents’, a number of them organise a monthly distributed denial of service (DDoS) protest. The National Cyber Security Centre (NCSC) is informed by the General Intelligence
and Security Service (AIVD) that hard core members of the Malcontents are trying to link up with Ahackgroup, an internationally known hacktivist group.

In March 201X, the US federal government is once again taken unawares by a deluge of leaked government data. The whistle-blowing website Kickbacks, which has links to Ahackgroup, posts leaked documents and secretly recorded videos of senators and high-ranking officials in the United States accepting bribes from lobbyists from both Western and non-Western countries. Before the documents are posted on Kickbacks, their authenticity and security implications are vetted by an international group of associated internet journalists and former hackers. This is necessary because some of the bribery documents relate to confidential defence programmes involving the United States and the other Five Eyes countries. By taking these steps, Kickbacks hopes to avoid leaking state secrets. The international vetting group includes three well-known and highly experienced Dutch hackers. In mid October 201X, the Ministry of Security and Justice receives an extradition request for these three hackers.

They are suspected of misappropriating and publishing US state secrets and other sensitive information. The Ministry of Security and Justice examines the request and reviews potential national and international legal obstacles.

During the same period, payroll service company XSP announces that it is closing its Dutch computer centres with immediate effect. These centres send out over 1.7 million salary slips per month on behalf of thousands of Dutch companies. As a result, a few hundred ICT workers lose their jobs.

Several developments then occur in rapid succession. On Monday, 18 December, with temperatures dropping well below freezing and the Elfstedentocht skating marathon approaching, the three hackers are picked up by the police. After the Public Prosecution Service explains the reasons for their arrest, the news media rush to report the story. At the same time, activist groups begin to take retaliatory action, calling on the public to defend internet freedom by carrying out cyber attacks against the Dutch government and right-wing media outlets. Instructions are posted on various underground sites. Hacking groups carry out uncoordinated attacks on various websites.

In a break from the past, they also target industrial control systems. For example, they hack into the printer files of a packaging company and add the message ‘Release them!’ to the company’s milk cartons. They also attack the relocated payroll service company XSP,
simultaneously sabotaging the air-conditioning systems in several of its foreign branches. As a result, the company’s computers and servers break down. In the absence of a continuity plan, salary payments are delayed by three to five days.

Ahackgroup announces that the Netherlands will be punished for arresting the three hackers and demands their immediate release. It claims that the Netherlands has been dealt an initial blow and that more attacks will follow. As questions start to be asked in parliament, the national crisis decision-making system swings into action. At the suggestion of the National Coordinator for Security and Counterterrorism, the Ministerial Crisis Management Committee (MCCb) is convened following consultations at ministerial level. The ICT Response Board (IRB) is also activated.

While temperatures outside remain below freezing, the situation becomes increasingly dire. Digital thermostats are hacked. A steam pipe in Rotterdam’s Korte Hoogstraat bursts as a result of interference with industrial automation and control systems (IACS), resulting in dozens of victims with serious burns. Ahackgroup claims responsibility. Fire extinguishing systems and air-conditioning systems in various psychiatric institutions and care homes for the elderly in the Netherlands also begin to malfunction. The combination of icy conditions and lack of capacity leads to a prolonged period of recovery.

The IRB concludes that the country’s critical infrastructure has not yet been harmed, nor is it at risk. The cyber disruptions are still manageable local incidents or are occurring outside the Netherlands. As a precaution, however, the NCSC starts operating around the clock, while businesses also scale up their security measures.

The NCSC notes that international media attention has led to an increase in automated cyber attacks (DDoS attacks and port scanning) as well as more sophisticated attempts to hack into government and critical infrastructure systems. The DDoS attacks appear to originate in Southern Europe. The NCSC’s website and telephone lines are also hit by DoS attacks.

Both critical and non-critical businesses come under fire from hacking groups. While the attacks on well-secured critical businesses are failing, non-critical companies are hit hard. A small chemical plant explodes, necessitating the full evacuation of two residential neighbourhoods for several days. The hackers threaten more cyber attacks on the Netherlands if the three hackers are not released immediately. A ‘high threat’ alert for IACS-controlled processes is issued in connection with three multinational companies named in the US bribery scandal. The IRB recommends increased vigilance regarding critical
infrastructures. It issues a similar recommendation for non-critical systems, even though they officially fall outside its remit.

The delay of salary payments at the height of the holiday season leads to unrest in the streets (riots and looting), forcing the riot police to intervene. In the meantime, various groups continue their disruptive activities. The hacking of dynamic traffic signs above motorways causes widespread gridlock. Hackers also sabotage metro and light rail systems throughout the Randstad conurbation. The unrest in the streets becomes so intense that the mayors of the four major cities (Amsterdam, The Hague, Rotterdam and Utrecht) issue an emergency ordinance that will remain in force until 28 December in order to prevent further looting. As a further result of the unrest, the Elfstedentocht, which was announced with much fanfare, is called off at the last moment because the police cannot guarantee sufficient manpower.

The Netherlands is clearly under heavy attack from the experienced international hackers of Ahackgroup. Other less sophisticated groups and individuals join the attack but tend to lose interest after a few days and return to their daily activities.

Following this chain of events, a large number of parties start taking measures to repair the damage and restore normal service. Furthermore, by means of several motions, the House of Representatives subsequently urges the Ministry of Foreign Affairs and the Ministry of Security and Justice to ensure without delay that international regulations and treaties are in place to tackle any future cyber attack on the Netherlands. Members also insist that the Ministry of Foreign Affairs pressure the countries where the attacks originated to take action. However, these countries protest that they are unable to take any direct action, since it is far from certain that the attackers were ever even present in their territory. It is possible that foreign hackers merely used infected computers in those countries to launch the attacks. Moreover, not all countries have an equally effective national Computer Emergency Response Team (CERT).

The prolonged unrest and insecurity prompted by this period of heavy hacktivism ensure that any reports of new hacking cases – whether true or not – quickly give rise to panic and fresh social unrest among the public and small business community.

*Impact and likelihood*

*Due to the interplay of different events and their ties to a specific period and specific weather conditions, the experts consider this scenario to be fairly unlikely. In contrast, the individual incidents are almost all regarded as realistic. Although none of the Netherlands’ vital*
interests are harmed, they are disrupted, as are several near-critical organisations and functions. The experts assess the impact of the scenario as substantial to serious, based on the consequences of the largely uncoordinated actions of hacktivists that disrupt the operation of public utilities, industrial processes, payment systems and information systems. Because the incidents all take place during the Christmas period, which includes a prolonged spell of sub-zero temperatures, the combination of certain disruptions causes some situations to get out of hand. Several parts of the country experience rioting and looting; traffic and public transport are severely disrupted; there are many accidents (both large and small) and the Elfstedentocht, which was announced with much fanfare, is called off at the last moment. All this gives rise to a great deal of unrest, anger and a certain amount of civil disobedience among the population. There is a substantial amount of material damage, as well as economic damage to the private sector. The Netherlands’ international position is damaged as a result of the actions of foreign hacktivists, the boycott of Dutch goods and a drop in tourism. For one or two days, daily life is severely disrupted, while the increased pressure on the emergency services might lead to several unnecessary deaths and dozens of serious injuries.

**Violent loner**

In recent years, society has been confronted with violent loners on several occasions. These individuals sometimes belong to an ideological or political network, and this can serve as a starting point for preventing violence, given that many terrorist networks are monitored as a matter of course by the authorities. The present scenario focuses on a lone individual who is neither part of a network nor a disturbed psychiatric patient. He carries out several solo attacks that leave no immediate clues as to the identity of the perpetrator. The scenario is set in a near future of economic uncertainty (high unemployment, higher interest rates and an ongoing euro and banking crisis) and increased distrust: the media routinely portray senior public servants, company directors and politicians as greedy fat cats who are out to cheat the honest public.

A 42-year-old process engineer loses his job at a large electronics group. He had previously met with the company psychologist, who noted that his inflexible behaviour made it hard for him to cope with changes within the organisation. However, he always performed well at his job, and his behaviour was not regarded as a problem. Following his redundancy, he becomes increasingly isolated from his family.

He does not find a new job, and his debts begin to mount. Mortgage interest rates have risen sharply, and people in the Netherlands who are forced to sell their homes are left with a
substantial residual debt. The engineer's own house also becomes harder to sell. He feels increasingly hard-pressed by events that are beyond his control. He spends much of his time in the attic, reading articles about the financial crisis and the excesses of bankers, civil servants and politicians on the internet. He tells his wife that he is busy applying for jobs.

Over the course of several months, three fatal attacks are carried out. First, the manager of a large bank is shot dead next to his car. A few months later, a senior official at the Employee Insurance Agency suffers the same fate. Both murders are carefully planned and committed in cold blood without leaving any evidence. The next victim, a university professor, is an ex-politician and former European Commissioner with outspoken ideas on the beneficial effects of the free market, the pursuit of self-interest and the importance of discipline. He writes columns for newspapers and magazines and regularly appears on television talk shows. His murder is connected to the earlier killings, and the police step up their investigation.

The attacks receive a lot of media attention. Fear spreads because nobody claims responsibility for the attacks, and nobody knows who is behind them. Some people, especially senior public servants, politicians and captains of industry, feel increasingly ill at ease and avoid public appearances. At the same time, certain groups in society regard the attacks as a logical consequence of the capitalist excesses of recent years and use the opportunity to criticise EU policy. This elicits a wide range of reactions from other countries.

A few months later, the police finally make some real progress in their investigation. They decide to make a compilation video using images captured by security cameras. Before showing the images on television, the police contact the company psychologist from the aforementioned electronics group, which had already arisen earlier in the investigation. The psychologist states that he wishes to discuss this, in his view, far-reaching request with his professional association before viewing the images. The police decide not to wait. That same evening, the blurry images are broadcast on a television crime programme. The process engineer's wife recognises her husband and calls the police, after which he goes on the run. The police search his house. In the attic, they find a list of potential targets that suggest the next victim might be a politician. The tension and anxiety increase with every hour that he remains at large, especially within political circles. Parliament is adjourned, and politicians go into hiding. A few days later, he is finally arrested.

Impact and likelihood
There are a number of social factors that make this a plausible scenario. The economic situation could cause people to become frustrated. It is possible to get hold of a firearm in the
Netherlands. Persons with a profile like the one described in this scenario do exist in society, although the vast majority would never resort to such actions. Moreover, the crimes of the ‘invisible loner’ described in this scenario are difficult to prevent, because such people are not on the radar of the relevant authorities. The experts therefore deem this scenario ‘likely’.

The impact of the actions of the violent loner is not regarded as very substantial or serious, primarily because his victims are members of a specific target group. On the other hand, the three fatal attacks attract considerable media attention and give rise to increased fear and tension in society. This is chiefly due to the fact that the last victim is a famous ex-politician with outspoken opinions, which in turn reveals that the perpetrator, who is still at large, is targeting people such as senior public servants, politicians, bankers and captains of industry. The attacks spark heated debates about freedom of expression and the role of ‘big money’. For a limited time, these debates have a substantial impact on the rule of law, resulting in social unrest and public anger, and damage the international position of the Netherlands. The remaining impact criteria are given low scores, and critical sectors and services are not affected.

**Large-scale disturbances**

In the year 201X, social relations in the Netherlands are heavily influenced by a strong sense of discontent within a key section of the population (especially young people) towards ‘the establishment’, including political leaders, public authorities, the judiciary, the education system and the health authorities. Although this ‘great dissatisfaction’ has not yet resulted in active rebellion against these institutions, something is definitely brewing.

In the summer of 201X, a large number of ‘flash robs’ suddenly occur in Amsterdam. Groups of young people who usually do not know each other personally arrange via social media to meet at a certain time and place in order to raid a shop or mug people in the street. The media coverage of these flash robs causes increasing anxiety among the people of Amsterdam, who are scared to go out on the street. The hype generated by the flash robs quickly spreads to other cities in the Randstad conurbation. Shopkeepers’ associations in these cities hire a large number of private security companies to protect their shops from these young delinquents, who are increasingly resorting to violence, destroying property and looting shops. Other groups, such as anarcho-extremists, latch onto the flash robs in order to promote their own ideologies. The police are meanwhile finding it very difficult to muster enough manpower to tackle the violence in the cities. As all this is going on, the relevant government ministries also become deeply concerned about the unrest in the Randstad.
The situation escalates when a violent flash rob results in a fatality. Via social media, the public is encouraged to protest against the failure of the police and the authorities to do something about the violence. As a result, hundreds of people in Amsterdam, Rotterdam and The Hague take to the streets to demand that the authorities intervene. At the same time, shopkeepers and members of the public organise patrols to protect their neighbourhoods from young delinquents. Various politicians get involved and request an emergency debate in the House of Representatives. When a second fatality occurs, the situation escalates even further. A young man of Moroccan heritage who is wrongly suspected of looting dies after getting into a fight with a neighbourhood watch patrol. In response to his death, a large group of young people mobilised via social media storms a police station and large-scale riots break out.

The next day, the violence and looting continue in several major cities despite the introduction of strict security measures. Calls to demonstrate against the looting circulate via social media after each incident. The riot police repeatedly charge the crowds to separate the demonstrators and counter-demonstrators. Inflammatory messages appear on social media sites, and speculation is rife about who is behind the violence and what it means. The situation in the cities becomes increasingly chaotic, and riots break out in several locations around the country. Neither the police nor the emergency services have sufficient manpower to deal with the situation.

Central government tries to take control of efforts to tackle the disturbances around the country. It attempts to improve communication, using social media to keep the public adequately informed without spreading anxiety. However, it is difficult to come to grips with all the local initiatives to communicate with the press and public. The coordination of local and national efforts to tackle the disturbances is also far from smooth in other areas. A proposal by the Minister of Security and Justice to order police units from around the country to assist the police in the four largest cities leads to a major clash between national and local authorities.

The disturbances have meanwhile spread from the streets to the internet. Various government websites are targeted by cyber attacks. Anarchists hack the NCSC’s Twitter account and use it to spread disinformation.

In subsequent days, the disturbances swiftly spread throughout the country. The situation in the cities descends into total chaos, with mass riots, widespread looting and arson attacks. Major city centres resemble war zones. Looted shops are closed and boarded up. Parents
keep their children at home because of the unrest on the streets. Trams and buses stop running, and it is impossible to reach city centres by car. Businesses and shops in the town centres close their doors, protected only by private security companies. Fire and medical services in the major cities find it increasingly difficult to do their work. In several neighbourhoods, emergency workers can only operate under escort of the riot police. In every police region, the police have their hands full trying to control the situation, meaning that they cannot respond to requests for assistance from other regions. The police are running out of manpower. The Royal Military and Border Police (Koninklijke Marechaussee) are deployed to support the police, but this additional capacity also threatens to run out quickly. The government considers deploying other military units and issues a call for foreign assistance. As a result, police in the Netherlands’ border regions are assisted by fellow officers from Belgium and Germany.

Authorities at local level are encouraged to mobilise community leaders to restore calm in their own neighbourhoods. Attempts are made to organise a ‘peaceful countermovement’ via social and traditional media. Spontaneous public initiatives pop up in various locations around the country. Examples include people sweeping the streets after lootings and volunteers bringing food to people who are scared to leave their homes. When the large-scale disturbances have finally subsided, the authorities make a strong effort to track down the looters, who are immediately tried and convicted through summary proceedings. Peace and quiet finally returns to the Netherlands, but the after-effects of the chaos are felt for years afterwards.

Impact and likelihood
The events described in this scenario lead to a substantial amount of social unrest, serious infringement of the rule of law and the core values of society, and a significant disruption to daily life. The resulting material and economic damage is huge, as are the costs of dealing with the disturbances. From an international perspective, the Netherlands’ image has been tarnished, and tourists will avoid the country for some time. There are several fatalities and a large number of injuries. Taking all this together, the experts rank the total impact of this scenario as ‘very serious’. They assess the chance that such an extreme scenario could occur in the Netherlands within the next few years as ‘moderately likely’, in part because of the adequate levels of resistance and resilience that currently exist in government and society. Regarding the vulnerability of Dutch society to the events described in this scenario, the experts point out that the ‘thermometer system’ used by local authorities to monitor specific population groups is still functioning properly. It is worth noting that the government
is still behind the curve in terms of social media, but several initiatives aimed at remedying this situation are currently being developed.

**Collapse of arms control in failing state**

This scenario is set in a fictitious non-European country with a democratic central government but a history of political instability. The army and the political system are both built on secular foundations but are increasingly dominated by political Islam. The country is home to several different ethnic and religious groups, although the vast majority of the population is Muslim. The region in which the country is located is characterised by frequent border conflicts and geopolitical tensions. Domestically, instability is on the rise due to the deteriorating economy and growing dissatisfaction with the country’s weak and corrupt government and the failure of critical services, including justice, education and health care. At the same time, Islamic radicalism, which began making its voice heard a few years earlier, is gaining a greater foothold in society. The country is degenerating into a ‘failing state’. In the 201X elections, no party achieves a clear majority. After months of political infighting, the army decides to intervene. At the end of 201X, it announces the formation of an interim military government. However, the divisions between the country’s various population groups gradually continue to increase.

In May 201X+2, intelligence agencies reveal that an unknown number of nuclear warheads and an unknown amount of enriched plutonium have gone missing, possibly as the result of an inside job. The next day, in a video message aired on national television and available on YouTube, three generals announce that they have taken control of a number of nuclear weapons in the interests of their country and their religion. They threaten to use the weapons if necessary.

Experts on Dutch television and in the international media immediately qualify the threat. It seems very unlikely that whoever has the nuclear warheads would actually possess the means to detonate them. At any rate, they do not have a missile system capable of reaching Europe or the United States. As a result of these reassuring statements, the public remains calm in spite of the aforementioned events.

Tensions begin to rise between countries in the region where the failing state is located. NATO and the UN Security Council both discuss the possibility of increasing their military presence in the area. The discussions are complicated by disagreements concerning the status of the government of the failing state.
In July 201X+2, a group of men are arrested in the Dutch town of Almere on suspicion of plotting terrorist acts. A current affairs programme portrays them as a gang of nuclear terrorists. In the meantime, the diplomatic tug-of-war over the situation in the failing state continues. The total number of missing nuclear warheads is still not known, but intelligence agencies assume that they are looking for five 12-kiloton warheads.

Soon after, one of the warheads is discovered in a large port in a non-Western country. A week later, the radicals release a new video in which they threaten to start a nuclear conflict if Western countries do not withdraw from the region.

On 16 October 201X+2, in the port of Rotterdam, a nuclear cargo that proves to be one of the missing warheads is discovered in a container originating from a non-European port.

Immediately following this discovery, a section of the port is quietly closed off and all relevant crisis mechanisms are activated. The Dutch government and the governments of several surrounding countries take various measures, including tighter controls at major seaports and airports. A few hours after the discovery in Rotterdam, the media get wind of the story. They create the impression of a large-scale terrorist attack – a nuclear 9/11. Although the official spokespersons convey a unified message, various experts issue contradictory statements in the media. The public does not know whom to trust and assumes the worst. After all, the so-called ‘experts’ claimed only a few days earlier that the missing warheads would never be a threat to Europe, but now one of them has turned up in Rotterdam! In the ensuing panic, anxious mayors order the closure of several other Dutch ports.

In the course of the day (16 October), it emerges that it is technically impossible to detonate the warheads and that they therefore do not constitute an immediate threat. After one or two days, the various Dutch ports that were closed are reopened. In spite of this, the media coverage remains tense. Moreover, the public is not familiar with this type of threat, which reinforces the prevailing mood of uncertainty, fear and unease.

The aforementioned events also rekindle the debate on Muslims and integration. Tolerance towards the Muslim population in the Netherlands declines, while the media in Islamic countries are highly critical of the West’s hegemonic attitude. The failing state becomes a safe haven for global jihadism. Fatwas issued against the West and ‘unworthy governments’ in the region find increasing support among young people. Individuals from Western countries, including the Netherlands, set off to join the global struggle. The threat of nuclear terrorism and the possibility of a costly intervention in the region of the failing state lead to
uncertainty and pessimism on the international markets. Consumer and business confidence in the Netherlands fall sharply. The global economy, which had appeared to be recovering, suffers another heavy blow.

**Impact and likelihood**

The experts consider this scenario as a whole to be ‘unlikely’ to ‘moderately likely’. The destabilisation of the failing state and the theft of nuclear weapons through an ‘inside job’ are not inconceivable as portrayed, but the discovery of one of the warheads in the Netherlands is pure coincidence. The anxiety resulting from the nuclear threat and the increasing polarisation of society are certainly plausible.

The experts consider the impact of the events to be ‘very serious’. The damage to the Netherlands’ international position and the infringement of the rule of law and democratic values are key factors in this regard. The public anxiety resulting from the nuclear threat also has a high social and psychological impact.
3. Recommendations concerning capabilities

3.1 Introduction

The previous chapter focused on the NRA 2012, whose results serve as the basis for the capability analysis. In the framework of this analysis, which takes account of existing capabilities, a large number of experts identified the capabilities that we (the government, the private sector and the public) need to reinforce in order to be better prepared to deal with the risks and threats described in the NRA. For a summary of the outcomes of the individual capability analyses, see annexe 1.

Following a consultation, the responsible ministries have made a selection of the capabilities the experts recommended enhancing. In doing so, they focused in particular on the efficiency and added value of those capabilities in comparison with those previously identified. In addition, they took account of current developments and initiatives wherever possible and specifically sought out capabilities with broad applicability, so that every investment has maximum impact. Finally, the selected capabilities were summarised in an advisory report. The scenarios in the NRA 2012 partly validate several existing initiatives. In those cases, reinforcing capabilities implies strengthening these particular initiatives.

On the basis of the findings report, the government decides which recommendations to implement. This chapter discusses the selected capabilities and recommendations contained in the advisory report.

3.2 Recommendations arising from the NRA 2012

The capabilities requiring reinforcement, as identified in the individual capability analyses, have been divided into five categories:

1. cooperation in the field of crisis management
2. information gathering
3. awareness and education
4. crisis communications
5. international capabilities

Within each category, the government is advised to focus on a number of specific capabilities, which are discussed in detail in the following sections.
3.2.1 Cooperation in the field of crisis management

Introduction

A well-coordinated and well-integrated crisis mechanism is a prerequisite for a timely and effective response. Previous findings reports have already included recommendations to this effect, focused chiefly on general processes such as establishing the National Operational Staff (LOS) and improving the decision-making process in crisis situations. The assessment of the scenarios relating to hacktivism, large-scale disturbances and international issues indicates that several specific aspects of crisis-management cooperation in these areas still require improvement.

National and international cooperation in cyber crises

The idea that ICT disruptions can lead to crises at national or even international level is a fairly new concept in the field of crisis management. A number of measures have already been taken to deal with such crises, but there is still room for improvement. Given that these crises often have an international dimension, ongoing investment should be made in strengthening international cooperation. It is also necessary to continue developing the capabilities of national partners, especially those in the security field, as they relate to other public authorities and private partners. The aim is to turn ICT crisis management into a fully fledged component of the Netherlands’ national crisis mechanism, in which all the relevant parties have clear roles and responsibilities. The National Cyber Security Centre (NCSC) plays a coordinating role in this regard.

With this in mind, the government is advised to take the following concrete steps:

- Draft cooperation agreements for measures such as information exchanges with the NCSC, local authorities and key private partners during crises. Products: a revised version of the National ICT Crisis Plan (completion date: first half of 2014) and cooperation agreements with partners (ongoing, given the large number of public and private partners).
- Prepare for cyber incidents and crises by improving cooperation between system partners at national level. Product: national training exercises (ongoing: next exercise scheduled for second half of 2014).
- Enhance international cooperation by drawing up an inventory of different approaches to cyber security and of response capabilities. Product: international benchmarks (completion date: mid 2014).
- Ratify and implement existing international agreements and methods of cooperation (e.g. International Watch and Warning Network (IWWN) and EU standard operating procedures (SOPs)). Products: up-to-date SOPs and international training exercises (ongoing: international training exercises take place every two years).

Responsible party: *Minister of Security and Justice*, as the coordinating minister for cyber security.

**Cooperation in providing assistance**

As part of its preparations for responding to large-scale disturbances, the authorities are already developing a National Riots Crisis Plan that lays down the interministerial crisis mechanism for such situations. In addition to this, they are advised to develop options for working with other partners. In the extreme and exceptional scenario of disturbances that require a 24/7 response, the police force's standard capacity to maintain order is limited and likely to be exhausted within a few days if not augmented by additional deployments or assistance. For this reason, the options and basic conditions for cooperative undertakings (e.g. the deployment of military units and public-private partnerships) should be fleshed out and enshrined in agreements. In this context, it is important to create a real-time quantitative and qualitative overview of the available assistance capability (and the related costs).

Pursuant to the Police Act 2012 and in the framework of civil-military cooperation, it is already possible to request assistance from the Ministry of Defence for the purpose of maintaining law and order. The capability analysis prioritises capabilities aimed at maintaining continuity in the event of the exhaustion of police capacity. An example of this would be transferring responsibility for back-office police tasks to the Ministry of Defence in order to keep the front lines 'blue'.

Responsible party: *Minister of Security and Justice*.

**Synchronisation of plans for dealing with nuclear threats**

It is unclear how international, national and regional (including local) plans are supposed to link up in the event of an international nuclear threat. This issue needs to be examined in greater depth. It should be clear which organisations and mechanisms should be engaged in such circumstances and what their role is. Questions that need to answered include: Are there any gaps in the system? How do the mechanisms and processes fit together? What is the link between the general crisis mechanism, the National Nuclear Accident Prevention and Management Plan (NPK), the Counterterrorism Alert System (ATb), NATO and existing
procedures? Such an examination should clarify the division of responsibilities at national
and international level and provide an adequate basis for drawing up an inventory of
agreements on the deployment of international response units in the framework of NATO and
the European Union. In addition, it can aid in streamlining the relevant plans.

Responsible parties: Minister of Security and Justice, Minister of Economic Affairs and
Minister of Foreign Affairs.

3.2.2 Information gathering

Introduction

The assessment of the scenarios relating to hacktivism, large-scale disturbances and
international issues indicates that improved government information gathering is a key
capability for reducing the likelihood that such incidents will occur.

Detection and analysis capability

ICT attacks and disruptions cannot always be detected immediately. For instance, malware
may be active long before an actual disruption or failure occurs. In order to reduce the
likelihood of such incidents, it is important to detect malware as early as possible. Efforts
aimed at mapping and tracking digital threats are essential for developing situational
awareness, observing trends and providing a quick and accurate diagnosis during incidents
and crisis situations. Cyber detection and analysis capability, which requires dedicated
systems and staff, is also useful for finding links between apparently isolated incidents and
developments. Because the field of ICT keeps expanding and the world of cyber security is
subject to rapid change, it is vital that this capability keeps developing operationally and that
resources for early detection of malware and attacks keep improving. A first requirement in
this regard is to expand both the technological infrastructure and the quality and quantity of
personnel.

Detection is a key initial step, but the information that is gathered in the process needs to be
quickly and thoroughly analysed with a view to diagnosing problems and identifying potential
courses of action. Other sources of information (such as social media) should also be
monitored in order to track and interpret current developments. Information from long-term
detection activities helps identify future risks. This requires a different type of analysis and
interpretation than the kind used in the context of short-term-response activities. Good
analysis can help uncover flaws in detection capabilities and lead to new insights that help to
improve detection. The government is accordingly advised to expand its analysis capability
so it is better positioned to identify and diagnose incidents in real time and better equipped to understand new threats and developments through social media analysis, malware analysis and the mapping and tracking of rogue networks (e.g. botnets).

In this context, it is also important that the authorities are equipped to identify long-term risks. Finally, in the case of malicious ICT disruptions, they should also have sufficient capacity to track down and prosecute the perpetrators.

Responsible parties: Minister of Security and Justice, Minister of the Interior and Kingdom Relations and Minister of Defence.

Information gathering in connection with large-scale disturbances

In order to gain a better insight into breeding grounds for unrest and people who disturb public order, the government needs to expand its information gathering and investigative resources. In addition, it needs to reinforce its analysis capability in order to interpret complex information from various sources.

Moreover, increased attention should be devoted to monitoring and analysing social media (e.g. Twitter and Facebook). This entails developing and/or reinforcing certain relevant knowledge, skills and resources, as also recommended in relation to cyber security. Such reinforcement involves not only purchasing and developing software, but also – and especially – developing staff competences. This is consistent with the recommendation of the committee investigating the Facebook-related rioting in the Dutch town of Haren\(^6\) to monitor social media as an established part of everyday life, with a focus on finding unusual patterns that may require action.

During large-scale disturbances, the government needs to have a full picture of what is going on in society. At present, it overlooks certain trends because of the fragmentation of information across various reports. To solve this problem, an analytical tool should be developed (closed box principle) that links information on short and long-term risks to trends from existing reports.

Responsible parties: Minister of Security and Justice, Minister of the Interior and Kingdom Relations, the police and the Public Prosecution Service.

---

International information gathering by the intelligence services

In order to identify international threats at an early stage and avert them before they reach the Netherlands, it is vital that the Dutch intelligence and security services maintain their independent capability to gather information and verify sources. To this end, the authorities are advised to use these services’ resources and capabilities as efficiently and effectively as possible. The Netherlands’ foreign missions can play a key role in this regard, while the information from the intelligence and security services may be regarded as complementary. Improved information gathering will increase the chances of identifying and averting international threats. Early identification outside the Netherlands also enhances potential responses, such as the ability to intercept such threats.

Responsible parties: Minister of the Interior and Kingdom Relations, Minister of Defence and Minister of Foreign Affairs (foreign missions).

3.2.3 Awareness and education

Introduction

In order to reduce the likelihood of certain incidents and bolster the Netherlands’ resilience, it is important to increase awareness and knowledge among the public as well as among professionals. This applies both to the issue of cyber security and to the identification of potentially violent loners.

Increasing awareness by providing information on digital vulnerabilities

The dissemination of specific information on various digital vulnerabilities can help bolster the resilience of users. Both the government and the private sector regularly devote attention to this issue in the various media. Past and present examples of this include campaigns on safe internet use (Surf op Safe), internet banking (3 keer kloppen), phishing and passwords, as well as the first Alert Online campaign in 2012. Such information campaigns are most effective when they focus on current issues and suggest potential actions for specific target groups. A good example of this is the ‘Protect Your Business’ website, which was developed by the Digibewust (Digi-Aware) programme and the Dutch ICT trade association Nederland ICT. At the end of 2012, the site was reorganised to allow small and medium-sized enterprises (SMEs) and freelancers to test their cyber security policies. Effective cooperation between the government and the private sector is vital in this regard. Another example of an effective campaign is the Taskforce on Administration and Data Security of Service Providers, which was launched by the Minister of the Interior and Kingdom Relations at the beginning of 2013. Its aims are to increase awareness of data security within government in
cooperation with the umbrella organisations in this field and to develop tools to enable administrators and senior managers at all levels of government to work on improving data security. The aim is to introduce mandatory self-regulation for each level of government after two years.

The Alert Online campaign, which was renewed in 2013, has adopted a more structured approach to providing information and raising awareness. It links up with several European cyber security campaigns that take place every year in the month of October.

Responsible parties: Minister of Security and Justice (as initiator), in cooperation with all ministries, private parties, trade associations and interest groups.

Training and education to increase knowledge and expertise in the field of cyber security
This capability, which is identified as an action item in the National Cyber Security Strategy (NCSS), focuses on improving the professional standards of those working the field of cyber security. The aim is to stimulate and support the formulation and implementation of a comprehensive training programme that brings together various ideas and initiatives. Initial efforts will focus on drawing up an inventory of existing programmes, campaigns and needs (completion date: first half of 2014).

Responsible parties: Minister of Security and Justice, as coordinating minister for cyber security; responsible for drawing up the inventory.

Expertise related to potentially violent loners
In order to minimise the risk posed by violent loners, the government must boost the level of knowledge and scope for action of front-line professionals and increase opportunities for sharing knowledge and expertise.

To this end, three priorities have been identified:

1. Establishing an operational advice and expertise centre at national or regional level which would focus on the sharing of case-level knowledge and expertise by and for use by care workers, welfare officers and mental health professionals, the police, the probation service, the Public Prosecution Service, etc. It goes without saying that all relevant privacy regulations would be respected. The centre is meant to serve as a platform where front-line professionals can find practical knowledge, advice and referrals if they have case-specific questions concerning an actual or potential violent loner. It is in
no sense a reporting centre. The attending professional remains responsible for the case/client in question.

2. Establishing a central knowledge centre, which would focus on compiling and publishing existing knowledge and collecting new knowledge relating to research, policy, legislation and international developments. Despite their different objectives, it is important that a strong link is established between the two information centres discussed in priorities 1 and 2. The centres will support each other, exchange information and establish clear connections between national and regional needs.

3. Promoting specific skills among professionals. A number of basic training courses for professionals will have to be improved and expanded so that the professionals concerned gain a better understanding of the issue, thus facilitating the early detection of violent loners. Some professional groups already have access to such courses. It is important to examine whether they should be made available to all care professionals, police officers and members of the judiciary.

In the interests of efficiency, the aim is to incorporate the two centres into existing networks and structures. This will spare the deployment of additional people and resources. Where necessary, outside experts will be brought in on a temporary basis.

The Ministry of Security and Justice, the Ministry of the Interior and Kingdom Relations and the Ministry of Health, Welfare and Sport are jointly responsible for achieving these three priorities. This is because security policy, intelligence work and mental health care all play a role in limiting the risk posed by violent loners. In such cases, these areas influence and reinforce each other.

*Crisis management training for Dutch diplomats at foreign missions*

Crisis management is increasingly well organised at the Ministry of Foreign Affairs, but Dutch missions abroad know too little about how to respond in crises. The Ministry is currently developing a training module for this purpose. It will initially be rolled out at high-risk missions and will subsequently be expanded to others.

Responsible parties: Minister of Foreign Affairs.
3.2.4 Crisis communications

Alongside administrative and operational efforts, communications is one of the three pillars of effective crisis management. In recent years, much has been done to raise the standards of crisis communications, which has become a discipline in its own right. The assessment of the scenarios relating to hacktivism, large-scale disturbances and nuclear weapons indicates that specific knowledge adds value in communications concerning such crises.

The government is therefore advised to devote specific attention to the following two issues in existing national communications plans and existing crisis management plans that deal with communications:

- ICT crises/hacktivism
- malicious international nuclear threats.

With regard to large-scale disturbances, the government is further advised to simplify the national crisis communications framework so the authorities are able to communicate clearly with the public, while allowing scope for local customisation. Clear and effective crisis communications is one of the key instruments for de-escalating social unrest.

At a time that is seeing a significant increase in the use of social media as a means of communication, the government is advised to not only continue monitoring social media, but also to make greater use of it as an instrument of active crisis communication.

Non-government experts also play a key role in communications during actual or impending crises. On the basis of the nuclear threat scenario, the government is advised to identify a network of experts who are popular with the public and strengthen its relationship with them, especially during ‘quiet periods’. During these times, it should proactively inform these experts about government measures of a substantive or organisational nature (e.g. regarding the structure of the national crisis management system) as well as the considerations on which those measures are based. This will help to increase public understanding of government action during crises and prevent contradictory messages.

Finally, during crises with an international dimension, the government should take account of the impact of its measures and communications on the international community.

Responsible party: Minister of Security and Justice.
3.2.5 International capabilities

Introduction

There are two capabilities whose nature and scope are such that they cannot be addressed by the Netherlands alone. They require international support and a concerted effort to put them on the international agenda. Because of this, more time will be required to reinforce these particular capabilities.

Basic security guidelines for the development of hardware and software

Society's ability to defend itself against the various vulnerabilities that exist in many ICT applications remains insufficient.

For instance, peripheral devices such as printers, scanners, cameras and network drives are often equipped with web servers that make it possible to access them remotely via the internet. A significant number of devices come unsecured as standard, which means that they can be accessed by anyone, anywhere. The goal of drawing up a basic set of guidelines is to formulate requirements and obligations for the development of new hardware and software products and thus ensure a minimum level of security during the production of hardware and software components. This reduces the vulnerability of systems assembled from these components and makes it harder to exploit vulnerabilities in fully assembled systems.

In this way, it is possible to achieve a certain minimum level of security on a large scale without being dependent on the installation of security measures by users.

Responsible party: Minister of Economic Affairs, in cooperation with various interest groups.
A time frame is not available at this time.

International focus on the optimum protection of nuclear facilities

The Netherlands works closely with other countries and organisations to prevent nuclear terrorism. To this end, it does its utmost at international and bilateral level to ensure optimum protection of nuclear facilities and material and radioactive sources. By eliminating the origin of the threat, it is possible to prevent incidents and reduce the likelihood of their emergence, development or spread.
The Nuclear Security Summit (NSS), which is being hosted by the Netherlands in 2014, plays a leading role in this area. The stated goal of the NSS is to improve the security of nuclear material and facilities, in cooperation with 53 participating countries and four international organisations. Together, these countries account for more than 95% of global nuclear material.

In consultation with its member states, the International Atomic Energy Agency (IAEA) has issued a recommendation on the protection of nuclear facilities, the protection of nuclear material during transport and the location and recovery of missing or stolen nuclear material (INFCIRC/225/Revision 5). The IAEA also offers an International Physical Protection Advisory Service (IPPAS) from which countries can request advice to assist them in improving the security of their facilities. It is important that the Netherlands draw attention to these efforts. Transparency, international trust and actual improvement in international protection are all reasons for reinforcing this capability.

The social benefits of improving international protection include increased national and international security, international trust and better international coordination and cooperation.

Responsible parties: Minister of Foreign Affairs and Minister of Economic Affairs.