kst-30821-12
ISSN 0921 - 7371
The Hague 2011

Dutch House of Representatives (Tweede Kamer der Staten-Generaal)

Parliamentary Year 2010–2011

30 821 National Security

No. 12 LETTER FROM THE MINISTER OF SECURITY AND JUSTICE

To the President of the House of Representatives

The Hague, 22 February 2011

Ensuring a free and secure society is the most important duty of the government. The Cabinet sees preventing societal upheaval as one of the important tasks in realising its duty to provide security. The government cannot guarantee 100% security, but the Cabinet can and must make choices and priorities in the use of people and resources, especially in times of cut-backs. The goal of this Cabinet is to deal with risks in a sober manner, while simultaneously being able to tighten the reins when action needs to be taken. The Cabinet wants to signal, prioritise and where necessary handle (international) developments and threats that the Netherlands face and that could potentially pose a risk to the Dutch national security at an early stage. Everyone must take his responsibility in this respect: government, citizens and the business community.

I am hereby present you with the report of findings of the National Risk Assessment 2010 (NRA)[1] and I am informing you on behalf of the Cabinet as to the most important new emphases which the Cabinet, in accordance with the coalition agreement, wants to place on the area of National Security[2]. Via the appendix to this letter I am also informing you as to the progress in the topics that were set out in the third progress letter on National Security of 22 February 2010[3] and as promised in the Parliamentary Committee Meeting of 9 December last (Parliamentary Document 29 517, no. 45).

A safe and secure Netherlands in a changing society

The Netherlands is among the wealthiest and safest countries in the world. Prosperity in the Netherlands can be attributed to our open and safe society, international orientation and a geographic position at a key junction in a global network of water, land, air and, in modern times, through digital routes. We owe our security to a solid legal system and rule of law, a long tradition of working together on security and prosperity which find their roots in mastering the water and active international cooperation in, inter alia, the EU, NATO and the UN. The Netherlands has built a powerful international political and economic position on these foundations. A position which we wish to protect and reinforce.

[1] Made available for inspection at the Central Information Point of the Netherlands House of Representatives.

[2] Other recommendations of the NRA 2010 are used by related ministries for the tightening of existing policy frameworks and activities.

[3] TK 2009–2010, 30 821, no. 10.

The threats which we are facing now and which we will increasingly be confronted with in the future are threats which inherently ensue from a modern, open, international society, such as the risk of a cyber attack, the risk of a geopolitically caused energy or commodity scarcity or the risk of a terrorist attack.

The National Security Strategy

In the past few years the National Security Strategy, with as important component the National Risk Assessment (NRA), played an important role in the identification of risks and dealing with crises. For example, in 2008 a possible flu pandemic was identified as one of the biggest risks to the Netherlands. These insights led to the vital sectors and government institutions preparing for a flu pandemic, inter alia in the form of continuity plans in this area. Insights acquired in the risk assessment in the area of, e.g., floods, polarisation and radicalisation and extreme weather, have further reinforced the policies relating to these topics. Internationally, the Dutch approach, which combines risk assessment and crisis management, is seen as an example for careful handling of national security issues. Together with the United Kingdom the Netherlands is leading the way in Europe in this respect. Within the European Union, a lot of work is currently being put into developing guidelines for risk assessments, whereby the experience gained in the Netherlands is used. The working method is also being addressed within NATO.

This Cabinet wants to continue the working method, as established by the last Cabinet. The working method is used to keep a sharp focus on potential risks and to prepare for possible risks so as to prevent social disruption. The current Cabinet favours an approach which combines common sense and reserve with assertiveness.

Topics for the future

The following risk diagram provides insight into the outcome of the National Risk Assessment 2010 whereby impact and likelihood of threats are charted using scenarios. Six scenarios were added this year. These relate to a cyber conflict scenario, two scarcity scenarios (food scarcity and mineral-related geopolitics), two accident scenarios (railway accident and maritime accident) and the loss of an internet exchange. In the coming years and based upon the NRA 2010 the Cabinet wants to focus on the topics of cyber security and international threats of national security, including shifting (economic) power relationships and geopolitical influence on energy, commodity and food security within the framework of national security.

[risk diagram]

Cyber security

The development of ICT offers hitherto unknown possibilities. Digital systems (ICT) are fundamental for our society and economy and a catalyst for (further) sustainable economic growth. Society is becoming increasingly dependent on the use of ICT. Failure of systems, misuse of ICT by malevolent individuals and data becoming unreliable can have serious consequences. For example, damages caused by cybercrime are globally estimated to be around one trillion dollars annually. During interstate conflicts coordinated cyber attacks by governments or actors affiliated with governments have been observed. Examples are the cyber attacks on Estonia (April – May 2007), Georgia (August 2008) and Kyrgyzstan (February 2009) and Iran (summer 2010). The concomitant dependence and entwinement leaves us increasingly exposed to espionage, as was also noted in the Espionage Vulnerability Analysis. In a separate response to this report, the Cabinet will outline the ambitions relating to the topic «resilience against espionage».

The National Risk Assessment 2010 highlighted that a large-scale cyber conflict will lead to major social breakdown. It is a feasible scenario with a high degree of vulnerability. Experts believe it likely that the defence against such an attack will fail, as at present it is virtually impossible to rapidly determine where an attack comes from and who is behind it. Where possible efforts must be geared towards the prevention of cyber attacks. Should such an attack nevertheless occur, the Netherlands must be able to respond adequately. All of this makes it of crucial importance that the Cabinet prioritises (just as many other countries, including the UK and US) the reinforcement of cyber security (civil and military, public and private, national and international). In this regard, the Cabinet will, by March 2011 latest, present a National Cyber Security Strategy (NCSS) and a concrete plan of action setting out how prevention, detection and response are to be reinforced, while retaining the open structure of the internet.

With the strategy and concrete plan of action the Cabinet fulfils its ambition voiced in the coalition agreement, to achieve an integral approach to cyber crime, expanded to cyber security and consequently fits in with the earlier promise to the Netherlands House of Representatives to establish a nationwide cyber security strategy on the basis of the Knops motion[4]. The central point in the strategy is an approach with more direct management of government tasks, reinforcing public-private cooperation and safeguarding an open and free digital society which contributes to economic development, prosperity and well-being. The main points of the cyber security strategy have been worked out in a number of actions. The main points are:

- Cyber security will be tackled in a more integral fashion by public and private parties.
- The monitoring and identification of threats will be strengthened through integral threat and risk analyses.
- The resilience of critical infrastructure against ICT threats and cyber attacks will be increased;
- Response capacity to be able to operate effectively in the digital domain will be reinforced, inter alia at the Ministry of Defence;
- The chain of investigation and prosecution will be reinforced. In the coming years capacity will be freed up for the investigating and prosecution of cyber crime;

[4] TK 2009–2010, 32 123 X, no. 66.

– Existing public and if possible scientific and private research programmes and budgets will be aligned.

The Minister of Security and Justice, in conjunction with the Minister of Economic Affairs, Agriculture & Innovation and the Minister of Defence, will take the lead in the development and elaboration of this strategy and the related plan of action.

Risks and threat in the overlap area of international and national security

National and international (security) policy are two sides of the same coin. The Cabinet is of the opinion that Dutch foreign policy, bilateral and in the framework of the EU, NATO and the UN contribute to a considerable extent to the security of the Netherlands. Developments abroad can – directly or indirectly – influence security in the Netherlands, for example economic security. For our energy and commodity security, international (economic) stability and security are of eminent importance. To an increasing extent (economically) our society is dependent on products and services from abroad. A part of, inter alia, the commodities for our industry and power supply come from unstable regions in the world, so that interdependency has economic disadvantages as well as advantages.

The Minister of Foreign Affairs and the Minister of Security and Justice will take the lead in further reinforcing the relationship between the international and national security policy. Inter alia by being alert to essential interests (for the Netherlands) abroad and the development of policies to safeguard these interests (relationship between defence policy, economic security in foreign policy). The recently published «Explorations in Defence[5]» form an important starting point in this respect. The Ministry of Economic Affairs, Agriculture & Innovation has already started identifying vital commodities which the Netherlands acquires to a significant extent from foreign countries and which are of crucial importance for the Dutch economy.

In relation to the European programme for critical infrastructure protection (EPCIP), the Ministry of Economic Affairs, Agriculture & Innovation and the Ministry of Infrastructure & the Environment, in cooperation with the Ministry of Security and Justice, is identifying which critical infrastructures within the energy and transport sector in other European countries are of vital importance for the Netherlands. In 2011 the Netherlands House of Representatives will be informed as to the outcomes and the consequences for Dutch policy on critical infrastructure protection.

Continuing attention

In addition to the above-mentioned threats, threats noted in previous versions of the National Risk Assessment[6] require continuing attention. This applies in particular with regard to natural hazards and terrorist threats.

Natural hazards

The flu pandemic which had the world in its grip in 2009 emphasised the importance of keeping an eye on more traditional hazards and threats in the face of our rapidly developing

[5] TK 2009–2010, 31 243, no. 16.

[6] TK 2007–2008, 30 821, no. 6 and TK 2008–2009, 30 821, no. 8.

society. In the past few years potential floods and pandemic scenarios have been developed and capabilities have been strengthened or developed to increase societal resilience to these types of risks. Flu pandemic and floods remain issues with a potentially high risk factor, as the current NRA (2010) shows. The additional efforts being called for result from, inter alia, the currently ongoing evaluation of government efforts to counter the pandemic flu (New influenza A (H1N1)), that hit our country in 2009. The Minister of Health, Welfare and Sport will provide more information on this matter later. In 2011 the pandemic flu scenarios in the NRA will be updated based on the outcomes of the evaluation.

Terrorist threat

Since the attacks of 11 September 2001 in the United States, terrorism has been on the agenda all over the world. This threat has been given full attention in the Netherlands as well. In the past few years, under the coordination of the National Coordinator for Counterterrorism a large number of developments have taken place to ensure that the Netherlands is better able to deal with possible terrorist threats. Dutch society has achieved and learned a lot in this area. As a terrorist threat can lead to damage to one or more vital interests and social breakdown, this type of threat also forms an important issue in the context of national security. Progress made in the fight against terrorism is reported via the Counterterrorism Progress Reports. The insights into the national and international terrorist threat against the Netherlands and its interests abroad we refer you to the Terrorist Threat Assessment of the Netherlands published by the National Coordinator for Counterterrorism and the Counterterrorism Alert System. With regards to generic capabilities extensive cooperation takes place between all involved partners to increase overall resilience in the area of national security.

A future-proof approach

In the past few years the national crisis structure has been reinforced, the Safety Regions Act was recently passed and implemented and the scope for joint and effective actions has been broadened for the emergency services and the ministry of Defenc. The NRA shows that new types of threats and crisis require a supra-sector and supra-regional or national approach. An adequate set of tools is needed whereby the options of direct management align with the questions raised by these developments. Before the summer of 2011 this Cabinet will come up with a proposal to reinforce the managerial role of the central government where needed in the event of (potential) crises. In any event, this will be explored for crisiscommunication, national operational services and up scaling. The proposal will of course take account the lessons learned from the evaluation of government handling of the outbreaks of Q fever and pandemic flu (New influenza A (H1N1)). In a later stage, this will have to be aligned with the outcomes of the evaluation of the Moerdijk disaster, that is being carried out by the Dutch Safety Board.

Lately, the cooperation between the public and private sector (and in particular the vital infrastructure) has been greatly enhanced in relation to the increase of continuity and concomitantly the prevention of social disruption. For example, agreement are being prepared or have already been agreed between safety regions and critical infrastructure sectors (drinking water, gas, electricity and telecom) regarding more intensive cooperation in the area of crisis management. The Cabinet will enhance the cooperation with businesses that are of critical importance to our society by organising strategic consultations at top level with VNO-NCW on the topics relating to national security. During times of crisis it must be clear to

whom critical infrastructure partners can turn. The government must speak and act with one voice, so that public and private sectors are able and willing to find each other, before, during and after a crisis.

This Cabinet stands for a participating safety and security policy. This means that the Cabinet wants to make citizens and businesses self-reliant and resilient, inter alia in the area of possible crisis. Nevertheless, this does not mean that citizens and businesses will be left to fend for themselves. There is an explicit role for the government to facilitate self-reliance and resilience. The Cabinet will therefore, on the basis of the NRA, develop concrete action perspectives in 2011 for citizens, public and private sector, at local, regional and national level. In addition, crisis communication plays an important role. Crisis communication during a potential or actual crisis is not only intended to provide general information, but is in fact also an important instrument for mitigating the effects of a (potential) crisis. In times of crisis citizens and businesses must be able to trust interpretations of a (potential) crisis made by leaders, are in need of fast, clear and uniform information from the government regarding what is happening and what actions they could take themselves to limit damage. In this manner the (potential) effects of a threat or crisis can be influenced. This means that crisis communication must be strongly rooted in the crisis and up scaling structure, with a clear mandate and management. Social media are playing an increasingly important role in this respect. The role which crisis communication can play and the way in which this takes place will be further enhanced in the coming time period, based partly on the experience gained when dealing with, inter alia, the Q fever and New Influenza A (H1N1). The information derived from the research into the recent disaster in Moerdijk will also be integrated. In accordance with the Dijkstra motion it will be shared with all safety regions[7].

This Cabinet wants to be able to quickly assess current developments inside and outside the Netherlands in relation to national security and to make choices. This partly in the light of the current financial and economic situation, which in the coming years will force us to make sober and clear choices on how we spend our money. The NRA supports this decision making process.

At the end of 2011 you will be informed regarding the results which will be reached in the coming period. In Appendix 1 you will find a brief state of affairs relating to the topics from the «agenda for 2010», as set out in the National Security third progress letter of 22 February 2010[8].

Finally, this Cabinet believes it is important that the Cabinet itself is properly equipped for its role in times of crisis. Not only locally, regionally or interdepartmentally must drills and practice be the motto, the Cabinet too has its role to play. It has therefore been decided to organise an extra Cabinet drill for the summer.

The Minister of Security and Justice,
I. W. Opstelten

[7] TK 2010–2011, 26 956, no. 81.
[8] TK 2009–2010, 30 821, no. 10.

APPENDIX 1

State of affairs with regard to the ambitions set out in the third National Security progress letter of 22 February 2010

Following is a brief review of results, which in addition to the National Risk Assessment and capacities analysis 2010, were achieved in the past year in the area of National Security:

1. In order to enhance the resilience and the response to large-scale disruptions of ICT and electricity, measures have been identified, with intensive involvement from the telecommunications and electricity sectors, that can increase the resilience in critical infrastructure sectors. By doing this jointly the awareness of critical infrastructure sectors has been increased and the insights into the consequences of large-scale disruption of ICT and electricity have been enhanced. The consequences of large-scale disruption of ICT and electricity can be substantial if critical infrastructure sectors are insufficiently prepared and the continuity of critical infrastructure processes is at risk. It has therefore been decided to prepare continuity plans for disruptions in ICT and electricity in the sectors of public order and safety and of public administration. The lessons learned from the development of continuity plans for pandemic flu will of course be used.
2. An ICT Response Board (IRB) is being set up for the response to ICT incidents. The ICT Response Board is a public-private joint venture. Its goal is to directly advise the government in the event of large-scale ICT incidents. The ICT Response Board participated in the recent international exercise Cyber Storm III..
3. A large number of parties, public and private, national and regional, participated in the international Cyber Storm III exercise. This exercise, which was led by the United States, was carried out with the aim of practising a response to a broadly structure cyber attack. The assessment of Cyber storm III will be sent to Parliament in the spring of 2012.
4. In the past year, under the management of the Board of Safety Regions, agreements were developed for cooperation between the critical infrastructure sectors of drinking water, electricity, gas and telecom (not yet completed) and safety regions. The cooperation between the critical infrastructure sectors and safety regions can be reinforced on the basis of these agreements.
5. The National Operational Staff has been shaped at national level. Upon activation by the chairman of the crisis management committee, its task is to provide operational advice regarding the availability of (national) capabilities for crisis management and public order and security within the framework of the national crisis decision making structure.
6. Together with all involved chain partners an important start has been made for the development of a multidisciplinary approach to combat CBRN (Chemical, Biological, Radiological and Nuclear) incidents. In the framework of the intensification of the civil-military cooperation (ICMS), agreements have been made with the Ministry of Defence on multidisciplinary training facilities and on the future deployment in the event of CBRN incidents. The implementation of the European directive for the protection of critical infrastructure was carried out in full as of 11 January 2011.
7. The Dutch method of reviewing risks and threats is increasingly being followed on the international stage. Individual countries, but also the EU and NATO are developing a system of risk analysis and assessment which greatly resembles the Dutch approach.
8. The lessons learnt in the area of the pandemic flu which the Netherlands had to deal with in 2009 will be presented to you in the near future by the Minister of Health, Welfare and Sport.

9. The project *Self-reliance in the event of disasters and crises*[9] has resulted in valuable knowledge and insights, which will be used in the coming period. The most important conclusion is that the tendency toward self-reliance is a given in the event of emergency situations, but the quality and outcome thereof can be influenced and are open to improvement.
   The ambition of this Cabinet is that safety regions and the police organisation will have integrated (self-)reliance of citizens and businesses into their workprocesses to such an extent that in two years active involvement of the central government will no longer be necessary. Regions will contribute to risk awareness of citizens and businesses in a simple manner, and citizens and businesses will in turn realise that they themselves are partly responsible for the preparation for these risks. Emergency services know how to deal with (self-)reliant citizens to best advantage and will not encounter any impediments.
   In order to realise this, the Cabinet wants to provide optimal support for the regions in the coming two years in order to take charge of this role and eliminate barriers as much as possible.
   – Because information provision *during* an emergency situation is essential for self-reliance, this Cabinet is striving, with the help of NL Alert[10], to alert everyone who participates in NL Alert by mobile phone in emergency situations and offer them a concrete course of action. The goal is that in 2011 people will be familiarised with and informed of this new alarm tool by means of a national publicity campaign with a regional element.
   – Emergency services must in turn be enabled to allow room for and make use of (self-) reliance depending on the situation. Self-reliance of citizens must be integrated in actions of the emergency services. In processes for, inter alia, registration, accommodation and care provision, account must be taken of self-reliance. Liability issues should not form an impediment to the use of citizens.

[9] TK 2007–2008, 30 821, no. 6.
[10] TK 2009–2010, 29 668, no. 30.