Protection of Critical Infrastructure

Ministry of the Interior and Kingdom Relations
Contents

1 General

1.1 Reason for and objective of the Dutch CIP project 5
1.2 Scale, scope and ambition level 6
1.3 Relationship between Critical Infrastructure Protection and Crisis Management 7
1.4 Critical Infrastructure Protection in an international context 8
1.5 Practical application 8

2 Initial phase of the CIP Project – Quick Scan 9

3 Follow-up phase of the CIP Project 13

3.1 Follow-up phase of the CIP Project divided into three subphases 13
3.2 Further elaboration of the three subphases 14
3.3 Learning from scenario analyses 15

4 Responsibilities 17

5 Conclusions 19

Appendix A 21
Intermediate steps and explanatory notes

Appendix B 25
Deadlines for intermediate steps
1 General

1.1 Reason for and objective of the Dutch CIP Project

The motion submitted in the spring of 2001 by the members of parliament Wijn et al. (Lower House of the States General (TK), 2000-2001, 26 643, no. 20) requested the government to draw up an intersectoral plan of action for the protection of critical infrastructures. This request sprang from the growing dependence of critical public services on the availability and reliability of other critical public services, including ICT.

The awareness of the complex, comprehensive and interwoven nature of critical infrastructures grew particularly in the period leading up to 2000. The dramatic events in the United States on 11 September 2001 occurred shortly after the Wijn motion was submitted. These attacks once again revealed the interdependence and vulnerability of the infrastructures of the government, business community and national and international society. The events in the United States greatly influenced Dutch crisis management policy.

The attacks on the World Trade Center and the Pentagon led to the formulation of the Action Plan on Security and Combating terrorism\(^1\), Action Point 10 of which addresses the protection of critical infrastructure. The protection of critical infrastructure in the Netherlands also involves protection from other types of disasters, such as natural disasters, organisational and technical failures and human acts (both deliberate and accidental). Recent events, such as the large-scale power failures in the United States and Italy, as well as the terrorist attack in Madrid, underscore the importance of preventing and mitigating factors that may undermine the stability of a country's key interests. Accordingly, attempts are being made to establish structural connections between the critical infrastructure, the so-called ‘soft targets’ and the actual warning system to be implemented.

\(^1\) TK, 2001-2002, 27 925, no. 21
Set up in April 2002, the Dutch CIP project aims to:
1. develop and preserve a cohesive set of measures for the protection of critical infrastructures, including ICT;
2. incorporate these measures into the regular operations of the government and business community.

The development of this cohesive set of protective measures has not yet been completed. This is due in large part to the complexity of the subject matter and the great care that must be taken in the development process. Furthermore, it has become clear that the protection of critical infrastructure must be more than a one-off (project-based) undertaking and should be ongoing. A structural approach to the protection of critical infrastructure is essential in order to be able to respond rapidly to current events. As the co-ordinating project owner of CIP, the Minister of the Interior and Kingdom relations therefore invests heavily in ensuring that a cohesive and comprehensive approach is being followed. Official direction will be in the hands of the National Crisis Management Co-ordinator of the Ministry of the Interior and Kingdom relations. Agreements have been made with everyone involved within the business community and government to proceed activities after June 2004. These agreements can be seen as the results of the CIP project and ensure further development of cohesive protective measures. The Ministry of the Interior will continue to coordinate further progress of critical infrastructure protection.

This is the last report on critical infrastructure protection in its original project form. The organisation has already been incorporated into regular operations, and the project organisation committee has been disbanded. The report describes the efforts the ministries and business sectors involved have undertaken up until now in order to attain the final results referred to above. It provides an overview of the approach used and the results achieved. It also outlines the results that have yet to be achieved and how this has to be done in the near future.

1.2 Scale, scope and ambition level

Dutch CIP policy aims to reduce the vulnerability of critical infrastructures in the Netherlands wherever possible, using feasible and enforceable measures. An infrastructure is qualified as critical if at least one of the following criteria applies:
- the disruption or failure of a critical sector, service or product causes national or international socio-economic disturbance
- the disruption or failure directly or indirectly affects a large number of people
- the disturbance lasts for a long time, recovery requires a great deal of time and, during the recovery, there are few effective alternatives available

As a result, only the top end of the disaster spectrum is being assessed.

The approach on CIP involves a wide range of critical products and services. This broad, non-prioritised approach has resulted in an in-depth understanding of the interdependencies of critical products and services. Given the major consequences of the interwovenness of these products and services, this approach was also used in the project's follow-up phase. In order to keep the selected approach manageable, choices were made as to clearly outline the areas to be addressed. For instance, the project did not focus on the areas of continuity under normal conditions as these are being addressed by supervisory bodies. Small-scale disruptions were likewise not taken into consideration. Nevertheless, the way in which the business community handles crises constitutes a key basis for critical infrastructure protection. A bottom-up approach is essential to prevent the failure and disruption of critical sectors, products and services.

2 See also TK 20-03-2004, 26 643, no. 48
The government cannot guarantee that critical infrastructures will never fail or be disrupted. Society is exposed to too many risks to exclude such a possibility. However, the consequences of failures or disruptions will be reduced using the knowledge gained from and practical measures implemented as a result of CIP policy.

With regard to the protection of critical infrastructures in The Netherlands, the professional and political ambition level aims to ensure that the government and business sector take responsibility and work together so that:

1. widespread failure or disruption of critical infrastructures can be prevented more effectively (proaction and prevention)
2. the government and business community are sufficiently prepared for the effects of a failure or disruption (preparation)
3. effective action can be taken to minimise the damage caused by the failure or disruption (response).

1.3 Relationship between Critical Infrastructure Protection and Crisis Management

The Beleidsplan Crisisbeheersing 2004-2007 (Crisis Management Policy Plan 2004-2007) was recently presented to the Lower House. Crisis Management aims to safeguard society’s critical interests, which are largely promoted by critical sectors and services. As a consequence, the protection of critical sectors, products and services – and hence critical infrastructures – is an essential condition for crisis management. With the knowledge of vulnerabilities, risks and associated protective measures, CIP policy addresses all links in the safety and security chain, from proaction to aftercare. Consequently, it has implications for policymaking outside crisis management. Any current and future knowledge that provides grounds to reinforce and adjust crisis management will be incorporated into crisis management policy.
1.4 Critical Infrastructure Protection in an international context

Dutch CIP policy also aims to exchange knowledge on an international level. Not only among participating consultation channels within the Ministry of the Interior and other ministries, but also those of the EU and NATO. In addition, knowledge is exchanged bilaterally with countries such as the United States and Sweden. International exchange of knowledge has brought to a fore that there are many similarities in the policy issues addressed and the (broad) approach used. Compared with other countries, the Netherlands is making good progress and achieving good results.

1.5 Practical application

Although the development of a cohesive set of protective measures has yet to be completed, existing insights regarding critical infrastructures have already proved useful in a number of current policy issues. For instance, based on the knowledge of interdependencies, a (categorised) list was drawn up of critical objects in the Netherlands eligible for protection and surveillance. Prompted in part by the attack in Madrid, this list is being completed and updated.

Another example of a practical application of CIP policy is the influenza pandemic scenario. Decisions as to which professional groups are eligible for antiviral agents will be based in part on the knowledge regarding critical products and services and the professional groups managing them.

Finally, the problem surrounding the supply of electricity merits attention. The prolonged drought in 2003 is one of the reasons why the insights into interdependencies are now being used in decisions as to which plants should be shut down first in the event of a power shortage.
2 Initial phase of the CIP Project - Quick Scan

The CIP Project distinguishes between two phases: the Quick Scan phase and the follow-up phase. During the Quick Scan phase, an inventory was made of the critical sectors, products and services and their interrelationships. This inventory was performed in collaboration with the Netherlands Organization for Applied Scientific Research TNO. The Quick Scan phase was completed with a presentation of a report to the Lower House.

The primary objective of the Quick Scan was to give an overall view of the elements that comprise the Netherlands’ Critical Infrastructure and to inventory how these elements relate to another and interconnect. Based on inventories conducted in preparation for the year 2000, experts of market parties, trade organisations and authorities helped mapping out critical products and services. This led to the following overview of critical sectors, products and services.

---

3 TK, 2002-2003, 26 643, no. 39
4 In April 2004, ‘chemical and nuclear industry’ was added under the heading of ‘external safety’. As this industry has an entire security regime of its own, it was decided during the Quick Scan not to list external safety as a separate sector. This subject was addressed once more during the follow-up phase. After all, the criteria used to determine whether a sector is critical (see p. 3) also apply to this sector. Due to the nature of the ‘chemical and nuclear’ sector the necessary analyses will differ from those of other critical sectors. These will place less emphasis on vulnerability due to chain effects. The approach will focus particularly on reducing the sector’s vulnerability to deliberate disruption. After all, under the heading of ‘external safety’, protection against natural and other disasters and unintentional human acts is one of this sector’s core duties.
5 The Health sector initially had one critical service. In the current inventory, the sector has been subdivided into four separate products or services.
<table>
<thead>
<tr>
<th>Sector</th>
<th>Product or service</th>
</tr>
</thead>
<tbody>
<tr>
<td>I Energy</td>
<td>1 Electricity</td>
</tr>
<tr>
<td></td>
<td>2 Natural gas</td>
</tr>
<tr>
<td></td>
<td>3 Oil</td>
</tr>
<tr>
<td>II Telecommunications</td>
<td>4 Provision of fixed telecommunications</td>
</tr>
<tr>
<td></td>
<td>5 Provision of mobile telecommunications</td>
</tr>
<tr>
<td></td>
<td>6 Radio communication and navigation</td>
</tr>
<tr>
<td></td>
<td>7 Satellite communication</td>
</tr>
<tr>
<td></td>
<td>8 Broadcasting</td>
</tr>
<tr>
<td></td>
<td>9 Internet access</td>
</tr>
<tr>
<td></td>
<td>10 Postal and courier services</td>
</tr>
<tr>
<td>III Drinking water</td>
<td>11 Provision of drinking water</td>
</tr>
<tr>
<td>IV Food</td>
<td>12 Provision of food and safeguarding food safety and security</td>
</tr>
<tr>
<td>V Health</td>
<td>13 Urgent care and hospital care</td>
</tr>
<tr>
<td></td>
<td>14 Medicines</td>
</tr>
<tr>
<td></td>
<td>15 Serums and vaccines</td>
</tr>
<tr>
<td></td>
<td>16 Nuclear medicine</td>
</tr>
<tr>
<td>VI Financial</td>
<td>17 Payment services / payment structure (private)</td>
</tr>
<tr>
<td>VII Stemming and control of surface water</td>
<td>18 Government financial assignment</td>
</tr>
<tr>
<td></td>
<td>19 Control of water quality</td>
</tr>
<tr>
<td></td>
<td>20 Stemming and control of water quantity</td>
</tr>
<tr>
<td>VIII Public Order and Safety (POS)</td>
<td>21 Maintaining public order</td>
</tr>
<tr>
<td></td>
<td>22 Maintaining public safety and security</td>
</tr>
<tr>
<td>IX Legal order</td>
<td>23 Administration of justice and detention</td>
</tr>
<tr>
<td></td>
<td>24 Maintenance of law and order</td>
</tr>
<tr>
<td>X Civil administration</td>
<td>25 Diplomatic communication</td>
</tr>
<tr>
<td></td>
<td>26 Government dissemination of information</td>
</tr>
<tr>
<td></td>
<td>27 Armed forces</td>
</tr>
<tr>
<td></td>
<td>28 Civil administration</td>
</tr>
<tr>
<td>XI Transport</td>
<td>29 Road transport</td>
</tr>
<tr>
<td></td>
<td>30 Rail transport</td>
</tr>
<tr>
<td></td>
<td>31 Air traffic</td>
</tr>
<tr>
<td></td>
<td>32 Inland shipping</td>
</tr>
<tr>
<td></td>
<td>33 Ocean shipping</td>
</tr>
<tr>
<td></td>
<td>34 Pipeline control</td>
</tr>
<tr>
<td>XII Chemical and nuclear industry</td>
<td>35 Transport, storage and production/processing of chemical and nuclear substances</td>
</tr>
</tbody>
</table>
Additionally, a basic understanding has been gained of the forms of damage that may be caused by the disruption or failure of a critical product or service (damage impact). Finally, the degree to which a critical product or service contributes to the coming about of other products and services has been mapped out.

The Quick Scan confirms the impression that the Dutch critical infrastructure is highly complex and has many interdependencies. It has also been recognised that those responsible for critical products and services have a limited understanding of other critical products and services that depend on them and of the extent of this dependence. Without backup or security measures, a disruption or failure of a critical product or service may produce chain effects with major consequences for Dutch society and that of our neighbouring countries. The Quick Scan has gained support from those involved in the government and the business community. The broad approach has led to an in-depth insight into the interdependencies of critical products and services. This insight clearly represents added value compared to the findings of studies conducted in the past. In addition, increased awareness led to the understanding that protective measures are necessary and that the parties themselves are responsible for them. Additional studies conducted by the COT Institute for Safety, Security and Crisis Management and Berenschot confirm that the public and private stakeholders are convinced of the use and necessity of paying systematic attention to the protection of critical infrastructures.
3 Follow-up phase of the CIP Project

3.1 Follow-up phase of the CIP Project divided into three subphases

The aim of the CIP Project’s follow-up phase is to provide clarity about the vulnerabilities and risks that endanger the availability and continuity of the supply of critical products and services. Based on the insights gained in this follow-up phase, decisions can be made whether any additional measures need to be taken. The follow-up phase has been divided into three subphases. These phases also form the three cornerstones of the permanent policy cycle of critical infrastructure protection.

Subphase I
Identifying critical interests and critical junctions (also in terms of geographic location) between critical sectors, products and services.

Subphase II
Mapping out the vulnerability of sectors and junctions. Providing insight into protective measures already implemented and their effectiveness.

Subphase III
Developing a cohesive set of protective measures, including any additional measures.
3.2 Further elaboration of the three subphases

A step-by-step plan has been adopted to implement the three subphases. The step-by-step plan and explanatory notes are included in Appendix A. The ministries and the sectors that come under them are responsible for carrying out these steps. This step-by-step plan was elaborated using a method that considers interests, threats and resistance in relation to one another. The Dutch General Intelligence and Security Service employs this method in conducting risk analyses with regard to deliberate human acts and assists the ministries in conducting vulnerability analyses in this area. It was decided to use the same method for conducting vulnerability analyses with regard to unintentional human acts, technical and organisation failures and natural disasters.

In order to learn as much as possible from one another and exchange experiences, the Ministry of the Interior organises quarterly peer review meetings. This form of peer-to-peer coaching and review enables the ministries and sectors to help one another without impeding the individual subphases. General and specific learning points are incorporated into the individual subphases.

State of affairs of subphase I

Two parts of subphase I have already been completed by the critical sectors in question. First, the critical interests were identified during the Quick Scan. The description of the subprocesses, i.e. the constituents into which the critical processes can be broken down, is an initial description of the critical interests that the sector is to serve\(^6\). For instance, the Ministry of Justice must be able to safeguard a minimum level of criminal prosecution and settlement of disputes by courts for as long as possible. The Ministry of the Interior and Kingdom relations will also have to maintain public order and safety and administrative decision-making at all levels for as long as possible.

Secondly, the junctions have been identified. A summary of the list of junctions was submitted to the Lower House in March 2004\(^7\). This list should be regarded as a start, forming the preliminary basis for the planned vulnerability analyses. The current list is neither exhaustive nor definitive. Most of the intersectoral junctions (that is, the junctions arising from dependence on other sectors) have yet to be established, partly on the basis of the vulnerability analyses to be conducted. The main points of this subphase will have been completed by April 2005.

State of affairs of subphase II

The steps to be completed in the second subphase are underway. The ministries have committed themselves to strict deadlines. The schedule is presented in Appendix B. These agreements guarantee the timely completion of this subphase. Meanwhile, the ministries have adopted the so-called ‘basic list of initial events’. Each sector will determine which of these initial events have the potential to disrupt or lead to a failure of the sector. The sector will determine the vulnerability to at least these initial events. The Dutch General Intelligence and Security Service actively supports the ministries in conducting the vulnerability analyses in the area of deliberate human acts\(^8\). According to the schedule, this subphase will be completed by December 2004.

---

6 See Table 2.1 on pp. 16, 17 and 18 of TNO’s Quick Scan of January 2003, FEL-03-C002; TK, 2002-2003, 26 643, no. 39
7 TK, 2003-2004, 26 643, no. 48
8 The ministries should take the Dutch General Intelligence and Security Service’s available capacity for this into account.
The results of the first two subphases form the basis for determining the cohesive set of protective measures. The three subphases jointly form the (permanent) policy cycle of CIP. According to the schedule, the results of the first completion of this policy cycle will be presented to the Lower House in the second quarter of 2005. This report will also address how often this policy cycle will be completed in the future.

### 3.3 Learning from scenario analyses

During the second subphase, the vulnerability of critical infrastructures is also mapped out in a different manner. By means of conducting scenario analyses insight can be generated into vulnerabilities, domino effects and the operation of the intended crisis management system. The insights obtained serves as input for the individual subphases. Rather than addressing critical infrastructures separately, the scenario analyses underscore the interrelationships of the sectors.

At the end of May 2004, the Ministry of the Interior and TNO led the first scenario workshop, which involved running through a power failure scenario. This is a particularly relevant case, as virtually all sectors rely heavily on electricity, and a power failure would entail relatively many chain effects. A great many critical factors were identified during the workshop, particularly with regard to the following topics:

- **a)** information provision and drawing a factually accurate picture of a situation for administrative co-ordination and policy teams;
- **b)** unequivocal control of interministerial co-ordination and decision-making;
- **c)** the necessary co-ordination between the government and the sectors in question where the prioritisation of shutting down or engaging facilities is concerned;
- **d)** the attention to be paid to the consequences of privatising critical (sub)sectors, the proper operation of emergency resources, and the preparation of logistical operations to replenish these emergency resources.
During the follow-up phase special attention will be paid to these topics. It is reasonable to conclude that the scenario analysis proves a valuable addition to three subphases of the follow-up phase. Running through a real-life case scenario has proved a useful tool for comprehensively assessing the robustness of critical infrastructures. A comprehensive approach better reveals the dependencies and thus any vulnerabilities between critical sectors. Furthermore, it quickly yields concrete results. The findings and insights from the workshop are used in the sectoral vulnerability analyses. The public and private sector have also worked together to generate insights, thus increasing the support for a joint approach to the protection of critical infrastructures. In the near future, this method will be used to gain more detailed knowledge of vulnerabilities.
4 Responsibilities

General
In many cases, optimum protection of processes, products and services within the critical sectors is primarily the responsibility of the private sector. Therefore, requirements will be laid down for managers and owners in areas such as proficiency and updating of contingency plans. The starting point for this is that such requirements should be functional and not include unnecessary administrative demands. The government will oversee the implementation of the requirements and, if need be, take action in the relevant sector. The government will support the business community on the joint development of detection methods, conducting threat analyses, on the basis of which the business community can develop contingency plans and organise simulations and joint exercises. Critical businesses are entitled to a certain degree of protection whenever the nature or magnitude of the crisis warrants this.

Ministries and business sectors
The CIP Project has been transformed from a temporary project into an ongoing policy process. The ministries and business sectors remain responsible for carrying out the agreed steps and achieving the results in a timely manner. This applies to both mapping out the (inter)sectoral junctions, (inter)sectoral vulnerabilities and risks, and the (inter)sectoral protective measures. Notwithstanding the fact that the vast majority (i.e. 70 to 80%) of critical infrastructures are owned or managed by the business community, one of the ministries can in all cases be held to account for the results, politically and administratively.

Co-ordination, monitoring and review
In addition to being responsible for the critical sectors of public order and safety and of civil administration, the Minister for the Interior continues to bear responsibility for the co-ordination of critical infrastructure protection. The Ministry of the Interior is thus in charge of co-ordination, monitoring and review, and can be held to account for the comprehensive approach and cohesiveness of the total set of protective measures.

Organisation
The continuity of critical infrastructure protection is safeguarded, as private and public parties have embedded their activities permanently in their organisational structure. In the near future, the Ministry of the Interior will consult with all parties involved to assess whether the current organisational forms are effective.

Public-private partnership
As stated above, most of the critical infrastructures are partly, and in some case entirely, managed by the business community and lower tiers of government. As a result, the protection of critical infrastructures requires close co-operation between the national government, the business community and lower tiers of government. The input from the business community is co-ordinated by the Confederation of Netherlands Industry and Employers (VNO-NCW). The lower tiers of government are represented by the Association of Netherlands Municipalities (VNG), the Association of Provincial Authorities (IPO), and the Association of Water Boards. In addition, the ministerial bodies responsible for carrying out the necessary steps maintain direct contact with the relevant trade organisations and business sectors.
Legal research

An important element of critical infrastructure protection is the division of responsibilities and powers in times of crises. Commissioned by the Ministry of the Interior, a study of legal aspects in the areas of crisis management and the protection of critical infrastructures is being completed. This study aims to examine the effectiveness of current legislation, detect possible gaps and put forth any proposals for improvement. A draft version of the report will be available in the autumn of 2004. Subsequently, the Cabinet will decide, together with the business sectors involved, if any measures are necessary.

9 The study is being carried out by Mr. E.T. Brainich von Brainich Felth.
This report presents the results of the CIP Project. A great deal has been achieved in the last two years. A Quick Scan has provided in-depth insight into the critical sectors, products and services. A follow-up approach was agreed upon, consisting of three sub-phases and various intermediate steps. So far, several steps have been put into practice.

In spite of the endeavours made by the ministries and business community, the project’s objectives have not yet been achieved due to the complexity of the subject matter and the great care that must be taken in the development process. Some of the results have yet to be achieved, which is one of the reasons why the CIP Project has been transformed into an ongoing policy process. This guarantees that the protection of critical infrastructure can be reviewed and updated on a regular basis. Co-ordinated by the Ministry of the Interior, further progress will be made in the near future.

As part of the four-yearly crisis management report cycle, the Minister of the Interior will continue to submit detailed updates on the protection of critical infrastructure to the Lower House. In addition, the Lower House will receive interim briefings on relevant sections. Such as the results of the first policy cycle, which are expected in the second quarter of 2005.

The protection of critical infrastructures is an important element of crisis management policy. Neither the business community nor the government can afford to allow their attention for CIP to slacken. Both the business community and the government have invested heavily in consistently safeguarding this complex issue and carrying on resolutely. The Ministry of the Interior has invested internally in the new organisation of Public Order and Safety in order to be able to permanently manage the cohesiveness of and comprehensive approach of critical infrastructure protection. The support generated within the authorities and business sectors offers promising prospects in that regard.
Appendix A

Step-by-step plan of Critical Infrastructure Protection

Step 1  Describe (critical) interests
Describe the interests that need to be secured with regard to your critical products and services.

Step 0  Perfect the analysis of junctions
When the analysis of sectoral junctions is completed: examine if these junctions apply to the aforementioned criteria ((inter)national impact, etc.) and assess their dependencies.

Result: Insight into sectoral junctions and critical interests. Complete: 1 June 2004

Step 1  Describe realistic initial events (threats)
First the entire list of initial events needs to be agreed upon at an interministerial level. Afterwards, identify those events that cause failure or disruption of the critical junctions.

Note: Failure of any critical product or service is also taken up in the list of initial events.

Step 2  Identify protective measures (resistance)
Describe the measures already in place, that protect the sector against any realistic threats and those measures as a result of dependencies.

Note: Vulnerability is determined through steps 1 and 2. It is defined as ‘a system’s sensitivity to an adverse event’.

Step 3  Identify risks
Determine risks associated with critical junctions and sectors. Risks are determined by:

a) the realistic initial events and the chance that they can occur;
b) the effect of such an occurrence (threat).

Step 4  Formulate control model
In a control model the earlier identified risks and protective measures will be balanced against each other.

Result: Insight into (inter)sectoral vulnerability

Step 5  Adopt measures to consolidate or improve the control of vulnerabilities
Describe which (additional) measures must be taken to ensure optimum control of the risks and reduction of vulnerability.

Result: Cohesive set of protective measures. Complete: 1 May 2005

Most of the intersectoral junctions have yet to be identified, partly on the basis of the vulnerability analyses to be performed.
Explanatory notes to the Step-by-step plan

Subphase I
Identify (critical) interests
By identifying the critical interests, the relevant sector designates the target that is achieved by protecting the critical sector or critical junction. Step 1 primarily fulfils a review function.

Perfect the analysis of junctions
When examining the vulnerability of critical infrastructures, the relationships between the various sectors should not be left out. After all, these make critical infrastructures a complex whole. To increase the manageability of the approach, it has been agreed to establish the critical junctions within and between sectors. Critical junctions are defined as parts of networks of business and policy processes where various critical products or services are joined that are highly or completely interdependent. During the analysis of junctions, the criteria referred to earlier (see p. 3) were used as guidelines. The results of the analysis give an overview of those critical infrastructure elements whose vulnerability should be examined.

Subphase II
Describe realistic initial events (threats)
The vulnerability analyses start with the identification and detailing of the initial events (i.e. threats) that are relevant to the critical sector or junction. Using this insight in the following steps, it is possible to determine a) the extent to which the sector is susceptible to these threats; b) the protective measures that are already in place; c) the chance that these events will occur; and d) the effects that these events have.

Identify protective measures
To determine a critical sector's or junction's vulnerability to the initial events identified, insight is needed into the critical sector's or junction's resistance. In other words, after identifying the realistic initial events, the sector will have to make an inventory of those protective measures already taken to control the threats recognised by the sector.

Identify the risks
Gaining insight into the risk that an initial event will occur is also required to determine vulnerability. This risk is determined by the chance of a certain threat and the effect that this event will have, both balanced against the interests to be secured.

Formulate control model
The vulnerability of a critical sector or junction is eventually assessed by means of a control model. The risks of realistic initial events mapped out for each sector and junction (known as the 'risk profile') will be balanced against the resistance, i.e. the protective measures taken. Based on the control model, the Cabinet will decide whether and, if so, what additional protective measures need to be taken. For instance, critical junctions with a high risk profile and a low degree of control will sooner be in need for additional protection than other junctions.
Subphase III
ADOPT MEASURES TO CONSOLIDATE OR IMPROVE THE CONTROL OF VULNERABILITIES

Using the control model, any deficiencies in the current set of protective measures will become apparent. In consultation with the public authorities, social partners and business community involved, the ministries will work out proposals to address these deficiencies. These proposals may serve as input for decision-making by the Cabinet. The division of responsibilities and powers with regard to the protection of critical infrastructures and the financing of the (additional) measures to be taken form an integral part of the ministries’ proposals.
## Appendix B

### Deadlines for intermediate steps

<table>
<thead>
<tr>
<th>Identify critical interests (step -1)</th>
<th>Perfect analysis of junctions (step 0)</th>
<th>Identify and elaborate realistic initial events (step 1)</th>
<th>Identify protective measures (step 2)</th>
<th>Identify risks (step 3)</th>
<th>Formulate control model (step 4)</th>
<th>Adopt measures to consolidate or improve the control of vulnerabilities (step 5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drinking water</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Food</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Health</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stemming and control of surface water</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public order and safety</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telecommunications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal order</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Civil administration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chemical and nuclear industry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*The above dates are deadlines.*

A = 10 May 2004  B = 10 May 2004  C = 1 February 2005  D = 1 April 2005