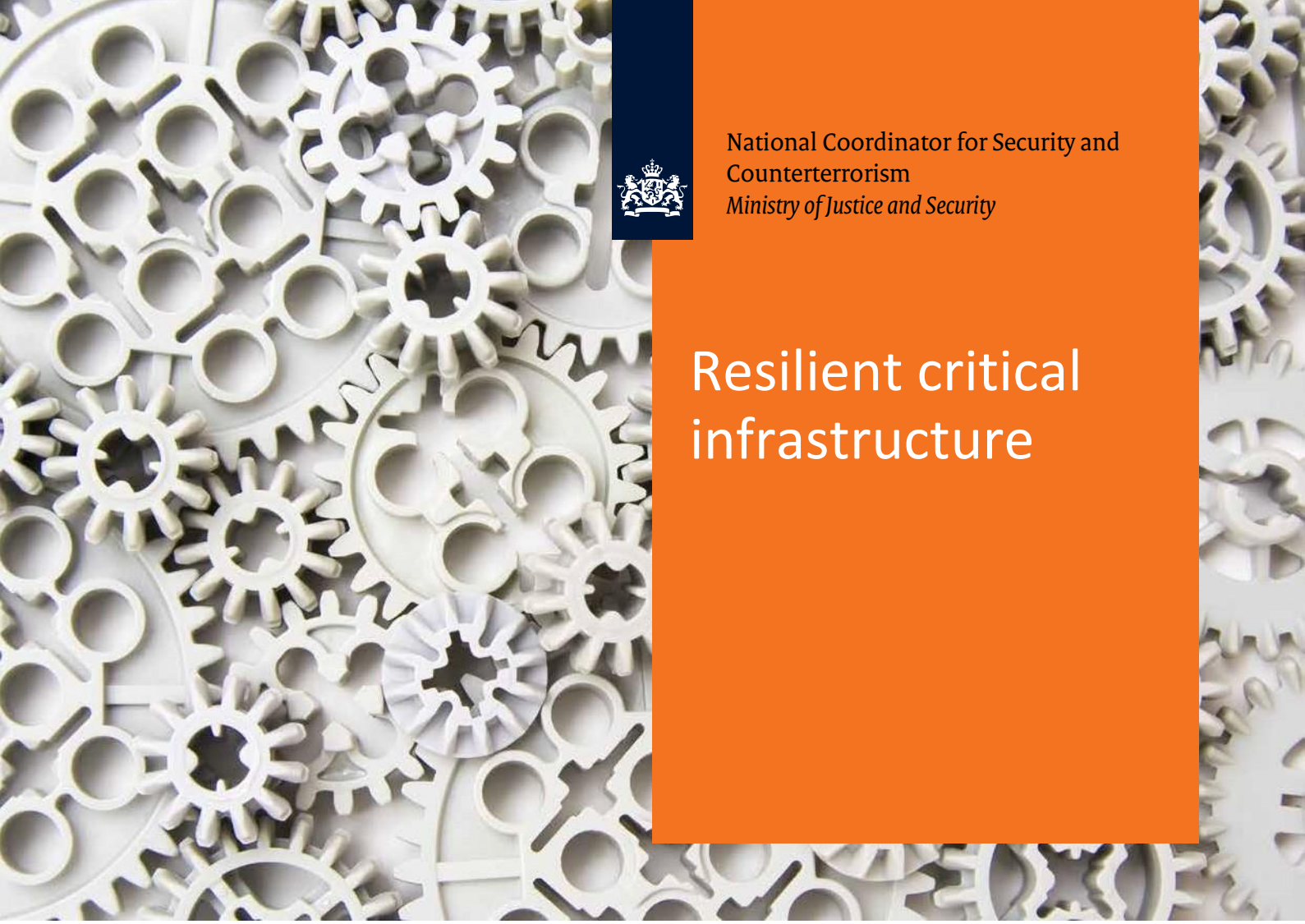

National Coordinator for Security and Counterterrorism
Ministry of Justice and Security

Resilient critical infrastructure

Certain processes are very critical for the Dutch society. The failure or disruption of such processes would result in severe social disruption and poses a threat to national security. These processes together form the critical infrastructure of The Netherlands.

The impact of incidents involving critical infrastructure, the speed of technological developments, the change in threats and cyber threats and the increasing mutual interdependence of critical infrastructure necessitates a permanent focus on increasing and safeguarding its resilience.

Approximately 80% of critical processes are in the hands of private parties. Public private partnership is necessary to achieve supported policy. The critical infrastructure policy is shaped as much as possible in association with the operators of critical processes, knowledge institutes and the government.

Critical processes and operators of critical processes

Critical processes are processes that could result in severe social disruption in the event of their failure or disruption. The term 'critical sectors' was used in the past. Since not all processes in a sector are critical, the current focus is on critical processes instead of critical sectors. Identifying critical processes allows the use of tools and scarce resources in a more efficient and targeted manner.

In these processes one or more organisations such as (private) companies, independent administrative bodies and water authorities are important for the continuity and resilience of the process. These organisations are referred to as critical providers.

Assessment of the level of criticality

The assessment is performed on the basis of established impact criteria, such as economic damage and physical consequences. Societal developments, such as altered threats or risks and incident evaluations, can lead to the assessment of new processes.

The assessment distinguishes between two critical categories, A and B. The failure of A-critical processes have greater potential effects than the failure of B-critical processes. The distinction between A- and B-critical can be helpful in prioritising incidents or the development of capacities that increase resilience. Each ministry is responsible for performing the assessment of the critical processes that fall under its responsibility. The coordinating Ministry of Justice and Security will regularly examine the methodology to ascertain whether it is up-to-date and will identify if there are indications of possible, new critical processes.

Stakeholders critical infrastructure

Many stakeholders are involved in the resilience of critical infrastructure.

- Primary responsibility for the continuity and resilience of critical processes is borne by the actual operators of critical processes. This includes gaining an insight into threats, vulnerabilities and risks, and developing and maintaining capacities that increase and safeguard the resilience of critical processes.
- The responsible ministry establishes general frameworks for the sectors that fall under its responsibility (in policy or in laws and regulations). The ministries, in association with the operators of critical processes, are responsible for safeguarding and inspecting capabilities related to critical infrastructure.
- Safety and Security Regions provide support to operators of critical processes in the event of (imminent) disruption or failure if the capabilities are inadequate and public order and safety are endangered. This takes place in coordination with the operators of critical processes and ministries.
- The fact that there are many, diverse stakeholders necessitates coordination and management. The National Coordinator for Security and Counterterrorism (NCTV) of the Ministry of Justice and Security is responsible for this management and ensures cohesion of resilience-increasing measures with and for all parties.

Critical processes	Category[1]	Sector	Ministry
National transport and distribution of electricity	A	Energy	Economic Affairs and Climate Policy
Regional distribution of electricity	B		
Gas production, national transport and distribution of gas	A		
Regional distribution of gas	B		
Oil supply	A		
Internet and data services	B	ICT/ Tel	Economic Affairs and Climate Policy
Internet access and data traffic	B		
Voice services and text messaging[2]	B		
Geolocation and time information by GPS	B		Infrastructure and Water Management
Drinking water supply	A	Drinking water	Infrastructure and Water Management
Flood defences and water management	A	Water	Infrastructure and Water Management
Air traffic control	B	Transport	Infrastructure and Water Management
Vessel traffic service	B		
Large-scale production/processing and/or storage of chemicals and petrochemicals	B	Chemistry	Infrastructure and Water Management
Storage, production and processing of nuclear materials	A	Nuclear	Infrastructure and Water Management
Retail transactions	B	Financial	Finance
Consumer financial transactions	B		
High-value transactions between banks	B		
Securities trading	B		
Communication with and between emergency services through the 112 emergency number and C2000	B	Public Order and Safety	Security and Justice
Police deployment	B		
Personal and organisational record databases	B	Digital Government	Interior and Kingdom Relations
Interconnectivity between record databases	B		
Electronic messaging and information disclosure to citizens	B		
Identification of citizens and organisations	B		
Military deployment	B	Defence	Defence

1 A decision is made whether the process is A critical or B critical based on the economic, physical, societal and potential cascade consequences in the event of the process failing.

2 All ICT/Telecom processes are managed via fixed as well as mobile connections and infrastructure, with the exception of text messaging, which is managed via mobile connections and infrastructure only.

Publication

National Coordinator for Security and Counterterrorism (NCTV)

PO Box 20301, 2500 EH The Hague | Turfmarkt 147, 2511 DP The Hague

070 751 5050

More information

www.nctv.nl | info@nctv.minvenj.nl | @nctv_nl

January 2018