THE CRITICAL INFRASTRUCTURE PROTECTION IN FRANCE

Objectives and challenges

What is a critical activity in France?

Because they contribute to the production and distribution of goods and services that are essential for the French State to exercise its authority, for the economy to function, for the continued defence of the nation or for the sake of national security, some activities are considered to be “of critical importance”.

The very nature of these activities means that they are difficult to substitute or replace.

How are critical operators designated?

Critical opertors are appointed by the sector’s minister who selects them from among those who operate or use facilities forming the backbone of French society and its way of life. The designation criteria and security objectives are set by the coordinating ministry.

The procedure involves, on the one hand, a consultation with the pre-selected operators and, on the other, cross-government talks enabling equivalent protection between all sectors identified as critical. Critical operators are designated with account taken of any distortion of competition and with every effort taken to avoid undue burdens.

What are critical infrastructures (CI)?

Critical infrastructures are institutions, structures or facilities that provide the essential goods and services forming the backbone of French society and its way of life.

The operators themselves draw up the list of their critical infrastructures, which may be production sites, control centres, network nodes or data centres for example.

What is the policy on the critical infrastructure protection (CIP)?

Developed and coordinated by the General Secretariat for Defence and National Security (SGDSN), the critical infrastructure protection (CIP) policy provides a framework in which public or private critical operators can assist in implementing the national security strategy in terms of protection against malicious acts (terrorism, sabotage) and natural, technological and health risks.

As the linchpins of this system, critical operators must analyse the risks to which they are exposed and apply the protection measures within their remit – particularly the VIGIPIRATE plan.

The 2013 White Paper on Defence and National Security establishes this policy as a means of strengthening the Nation’s resilience.

SGDSN

Twelve sectors of critical importance across four key areas of responsibility

BASIC HUMAN NEED

Food
Water management
Health



SOVEREIGN

Civilian activities
Legal activities
Military activities



ECONOMIC

Energy
Finance
Transport



TECHNOLOGICAL

Communication, technologies and broadcasting
Industry
Space & research



Stakeholders and responsibilities

Prime Minister/SGDSN

By delegation of the Prime Minister, the General Secretariat for Defence and National Security (SGDSN) is responsible for the cross-government coordination and organisation of the system. It determines the scope of the CIP policy, particularly as regards method and doctrine.

It approves the National Security Directive. It also lays down the cybersecurity rules that must be applied by critical operators.

Ministries

Ministries are tasked with drawing up the National Security Directive for each sector (and subsector) by stating which challenges, vulnerabilities and threats must be taken on board and by defining the sector's security objectives.

Ministries are also the operators' main points of contact.

Ministry of the Interior

The Ministry of the Interior oversees the territorial organisation of the system so as to support the action of zone and *département*-level.

Defence and security zone prefect

France is shared in 13 defence and security zone (including over-sea territories).

The zone prefect is the territorial stakeholder in charge of coordinating the CIP system. His responsibilities include organisation, support for préfectures and informational liaison between the central and local levels. He also coordinates inspections of critical infrastructure within his area of jurisdiction.

Département-level prefect

For each critical infrastructure, the *département*-level prefect approves the specific protection plan drawn up by the operator.

He also drafts an external protection plan setting out the intervention and vigilance measures to take if this critical infrastructure should ever find itself under threat or attack.

Critical operators

Once designated, operators must assume several types of responsibility: appointing a security liaison officer (who shall represent the operator to the administrative authority) and drawing up both an operator security plan (OSP), which describes the operator's security policy and organisation, and specific protection plans for each critical infrastructure identified.

Critical operators: stakeholders of the national security strategy

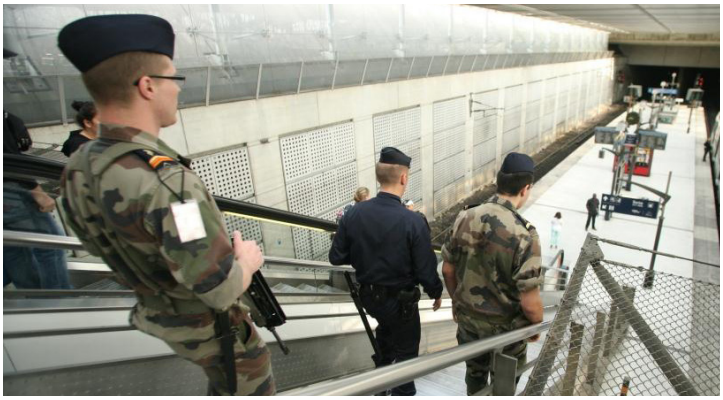
Critical operators act as the mainspring of the CIP system and, as such, they are accorded a specific status:

- appointment of the security liaison officer within the company. In this way the administrative authority has **a point of contact with security clearance** to whom it shall directly communicate information on threat or any changes in stance regarding the VIGIPIRATE plan;
- the so-called **"background checks"** procedure. This enables the critical operators to ask the administrative authority to check that the characteristics of the person wishing to access his critical infrastructure are not at odds with the security of the site;
- the **external protection plan**. Written under the authority of the *département*-level prefect, this rounds off the critical infrastructure protection setup. It describes and plans the State human and physical resources for an intervention at the infrastructure. It also provides for surveillance measures of surrounding areas.

Business continuity planning

In 2013, the SGDSN launched a process for revising the national security directive. One of its objectives is to adopt an all-hazards approach so as to encourage operators to make preparations for every critical eventuality that may affect their staff, premises, networks and production facilities by drawing up a business continuity plan (BCP).

These documents are a requirement on the part of critical infrastructure. The SGDSN has produced a methodological guide to drawing up BCPs, which the general public has been able to access since 2013.



SAIV and VIGIPIRATE

The critical infrastructure protection system has been set up to facilitate application of the VIGIPIRATE plan by involving the operators concerned in all efforts bearing on vigilance, prevention and protection against terrorism.

Critical operators need to incorporate into their plans the measures of the VIGIPIRATE plan that concern them and, as such, they must be able to take action in response to stances adopted by the Government depending on the situation on the threat or vulnerability front.

Cybersecurity

As early as 2008, the White Paper on Defence and National Security identified cyber-attacks as one of the main threats to our defence and security. To tackle those new threats, Article 22 of the 2013 Military Programming Law now requires critical operators to reinforce the security of their information systems.

These requirements apply to critical information systems identified by operators and involve reporting incidents, implementing a core set of security rules and making use of qualified detection service providers and products.

The National Cybersecurity Agency (ANSSI) is in charge of implementing these provisions within the SGDSN and has worked closely with the ministries and operators to define rules that are at once effective, appropriate and sustainable for operators.

Find out more at: www.ssi.gouv.fr

The European dimension

In the EU's single market where companies are becoming increasingly dependent on one another, the impacts of an attack on one operator can extend beyond the borders of a single State. France has therefore supported and strongly contributed to the EU's efforts to develop the European Programme for Critical Infrastructure Protection.

As a key element of this programme, the Council Directive of 8 December 2008 on the designation and protection of European critical infrastructures introduces a mechanism aimed at identifying European critical infrastructures in the energy and transport sectors.

Not only does this directive provide a framework for improving the security of major infrastructure with transnational implications, but it also encourages the development and improvement of national security systems bearing on critical activities in each Member State so as to avoid distortions of competition and contribute towards better protection of economic activities and citizens – i.e. towards Europe-wide resilience.

CIP
FACTS & FIGURES

8
MINISTRIES IN CHARGE

12
SECTORS OF ACTIVITY

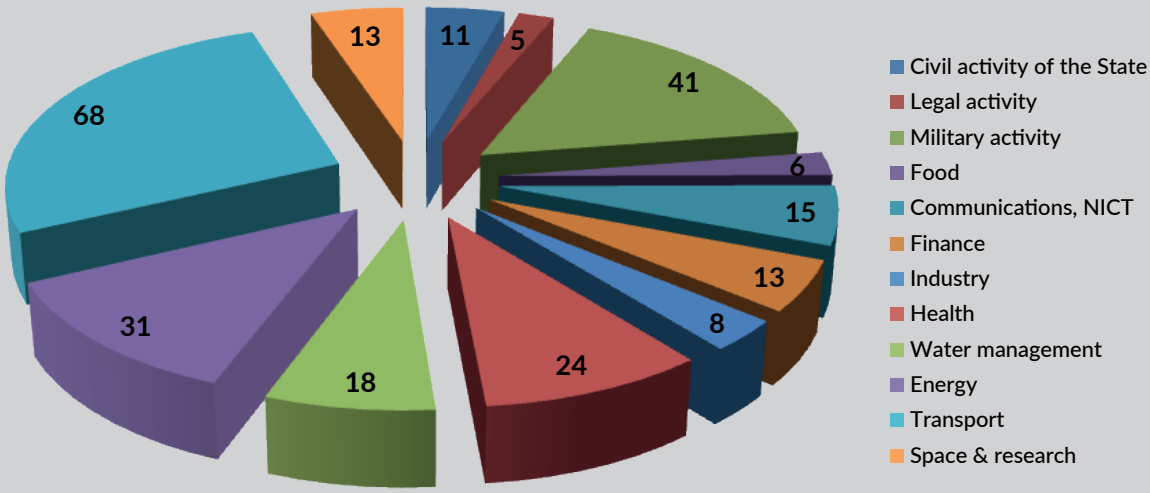
22
NATIONAL SECURITY DIRECTIVES

253
CRITICAL OPERATORS

1,381
CRITICAL INFRASTRUCTURES

300
PUBLIC SECTOR EMPLOYEES WORKING DAILY ON MATTERS TO DO WITH THE CIP

Breakdown of critical operators per sector



About the SGDSN

SReporting to the Prime Minister and working in close liaison with the President of the Republic's office, the General Secretariat for Defence and National Security (SGDSN) assists the Head of Government in fulfilling his/her responsibilities in matters of national defence and security. It is responsible for the cross-government coordination and organisation of Government matters.

Find out more at: www.sgdsn.gouv.fr

Reference texts

- Defence Code – Articles L. 1332-1 to L. 1332-7, L. 2151-1 to L. 2151-5 and R. 1332-1 to R. 1332-42.
- Instruction générale interministérielle n° 6600 relative à la sécurité des activités d'importance vitale du 7 janvier 2014.
- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Update: January 2017