



**LÊTZ
PREPARE!**
STRATÉGIE NATIONALE DE RÉSILIENCE

PILLAR 6



Cyber resilience

We are increasingly dependent on digital technologies in our daily lives, our economy and our institutions. To ensure the stability of the country and the confidence of its citizens, we must be able not only to prevent cyberattacks, but also to resist them, recover from them and adapt to them. Faced with increasingly sophisticated threats, orchestrated by state and non-state actors, cyber resilience relies on a systemic and coordinated approach:

effective governance, a culture of crisis management and communication, and access to technical resources are essential to protect and defend our networks and information systems.

Objective: To strengthen Luxembourg's cyber resilience capabilities.



Key actions

Several actions are being implemented to achieve this objective, such as:



To strengthen national governance and strategic coordination:

- We review the national cybersecurity strategy in order to strengthen public confidence in the digital world, protect human rights online, consolidate the security and resilience of digital infrastructures, and help to develop a reliable, sustainable and secure digital economy.

To strengthen operational capacities:

- We continue to strengthen the governance and coordination of the national cybersecurity ecosystem in order to optimise the structure and harmonisation of cybersecurity efforts at the national level by involving the public institutions and authorities in charge of cybersecurity and cyber defence, as well as critical entities, companies and citizens.
- We safeguard critical information systems by improving operational capabilities, implementing advanced detection capabilities, developing shared situational awareness, issuing early warnings, and systematically sharing actionable information on threats, attacks and intrusion attempts, and cooperating with relevant national actors to strengthen the level of preparation for managing major incidents and cyber crises.
- We are strengthening civil-military cooperation through integrated crisis management systems, information sharing, the development of interoperable standards, joint risk assessments and the organisation of joint exercises.
- We promote innovation in the field of cybersecurity and accelerate the deployment of Luxembourgish or European tools through funding or aid programmes in the areas of digitalisation, cybersecurity, quantum computing and artificial intelligence.



To develop expertise and awareness:

- We continue to develop national expertise in cyber resilience in collaboration with public research institutions, maintaining a high level of expertise and independent mastery of skills, developing expertise in emerging technologies and autonomous tools for small and medium-sized enterprises, and addressing the skills shortage in the cybersecurity sector.
 - We promote education, training and awareness raising regarding information system security through the creation of specific programmes in school curricula and information and awareness campaigns.
 - We support regulated entities, in particular small and medium-sized enterprises, through the development of recommendations and tools.
-