Cybersecurity in France for civil aviation

Ravo RANDRIA

December 2018

Cybersecurity in France for civil aviation

Cybersecurity in France for civil aviation

1. Cybersecurity in civil aviation at national level
2. Cybersecurity at the operational level in DSNA, the French ANSP

Cybersecurity in civil aviation at national level

Cybersecurity in civil aviation at national level

- National regulation
- Civil aviation, a sensitive domain
- National committee for cybersecurity in Air Transport
- Coordination at international level : EU and ICAO
- Cybersecurity for DGAC

National regulation

- Adoption of Critical Information Infrastructures Protection (CIIP) law in december 2013
- Publication of decree regarding the security of information systems for operators of vital importance (OVI) in march 2015
- Publication of decree for OVI in air transport in october 2016
- State Policy on Security of Information Systems (PSIS) in july 2014

ANSSI - France's cybersecurity agency

- The Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) is France's national cybersecurity agency created in 2009
- ANSSI is also the National Authority for information systems security (2009) and defence (2011).
- An interministerial body, attached to the Prime Minister's services, reporting to the General Secretary for Defence and National Security (SGDSN).
- ANSSI went from 100 staff in 2009 to more than 500 today.

ANSSI – 3 main missions

Prevent

The threats by anticipating modes of attack through scientific expertise, defining protective measures and by certifying trusted IT products and services.

Inform

Target audiences, by raising awareness on the necessary protection of digital environments, promoting best practices for cybersecurity and by issuing technical recommendations.

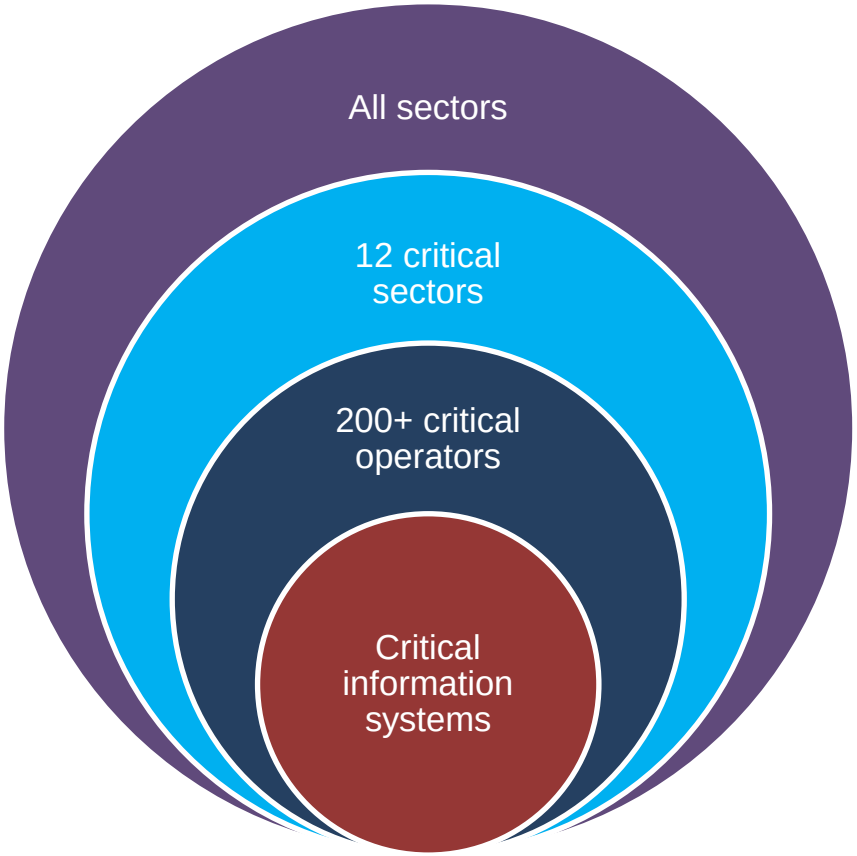
Defend

Information systems by detecting weaknesses and incidents and by reacting as early as possible in case of a cyberattack, including by providing technical assistance and expertise (CERT-FR included) to administrations and operators.

Civil aviation, a sensitive domain

Operator of vital importance (OVI)

« An operator whose unavailability could strongly threaten the economical or military potential, the security or the resilience of the Nation »



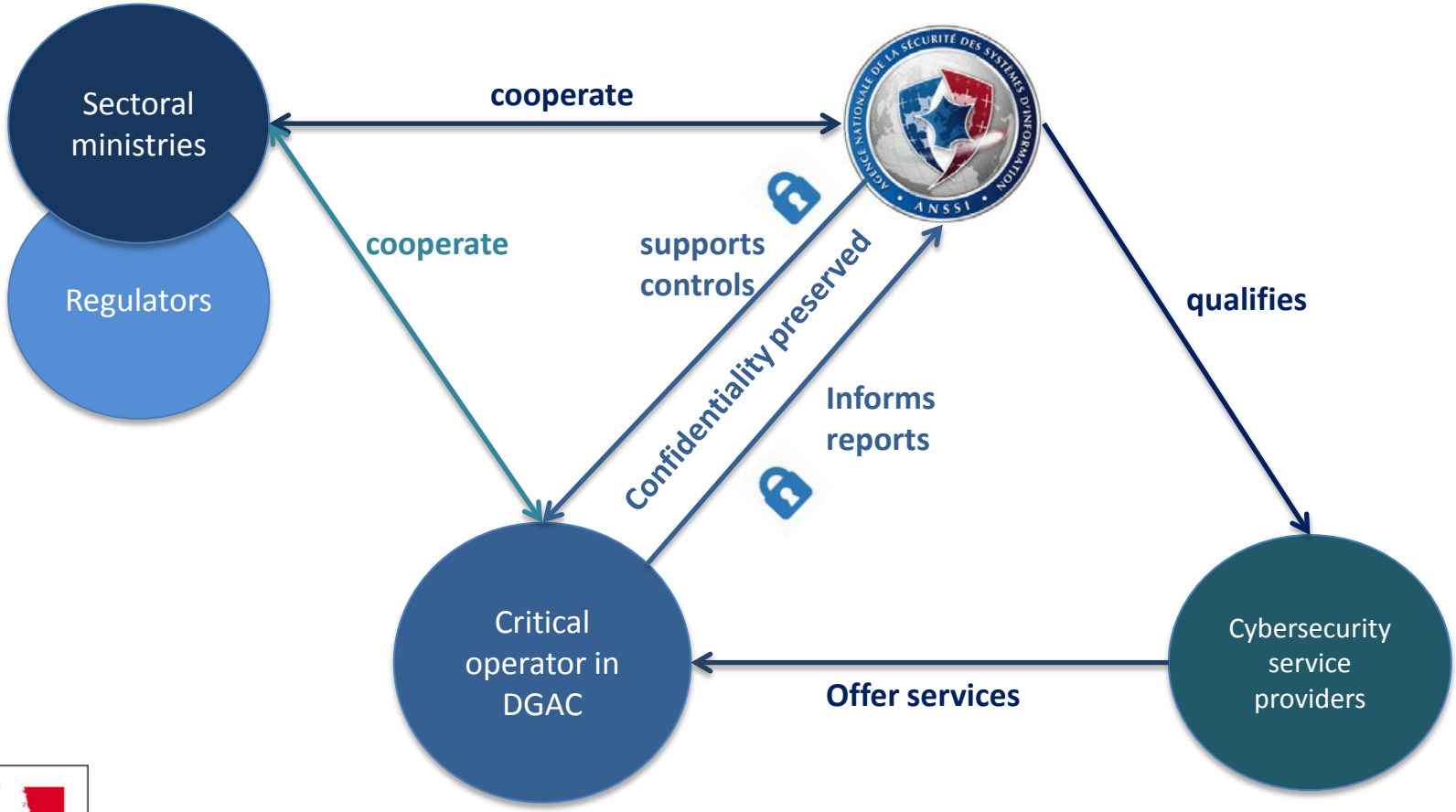
Civil aviation, a sensitive domain

The CIIP law provides with 4 sets of measures

SECURITY REQUIREMENTS ANSSI will impose to the operators a set of technical and organisational rules	**INCIDENTS NOTIFICATION** ANSSI shall be notified directly by operators of incidents occuring on their critical information systems.
INSPECTION ANSSI can trigger security audits led by itself, another State authority or a Trust service provider.	**MAJOR CRISIS** ANSSI can impose cybersecurity measures in case of major crisis, declared by the Prime Minister.

Civil aviation, a sensitive domain

DGAC within the French CIIP model



National committee for cybersecurity in Air transport

- **The national committee for cybersecurity in Air transport** coordinates strategy on cybersecurity for all stakeholders in aviation (aircraft manufacturers, airlines, airports, service providers…) and cybersecurity expertise (ANSSI…)

Emerging threats

To take into account emerging threats and scenarios that could impact activities in air transport

Impact on air transport

To analyse the impact of threats and scenarios on air transport activities, to propose protecting measures

Regulation amendments

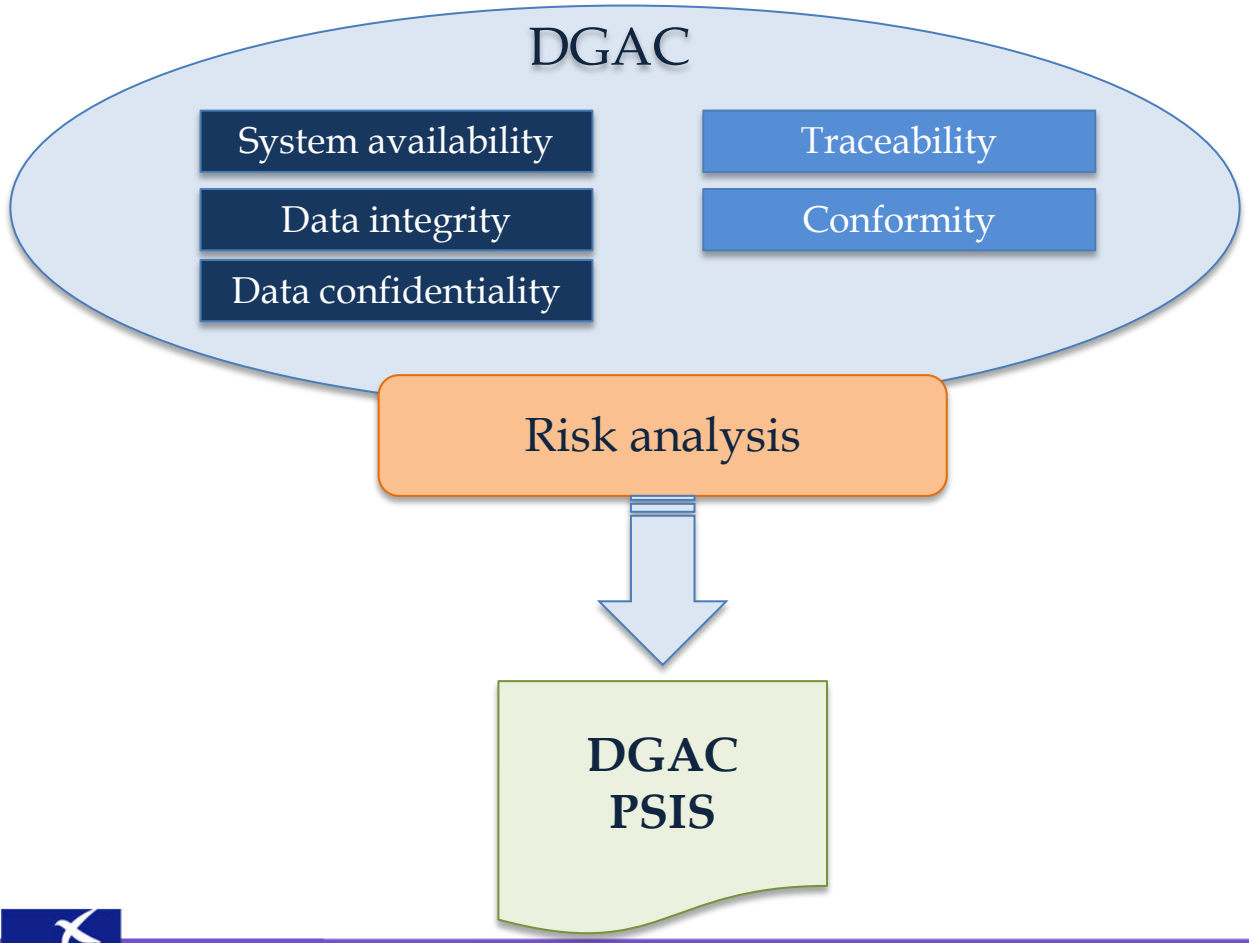
To evaluate the needs to amend the regulation at national and international level

Coordination at international level

- Active participation regarding cybersecurity at ICAO level
- The national committee for cybersecurity in Air transport proposes coordination with the international level in EU or ICAO
- French DGAC can provide pedagogical tools on cybersecurity for its foreign partners

Cybersecurity for DGAC

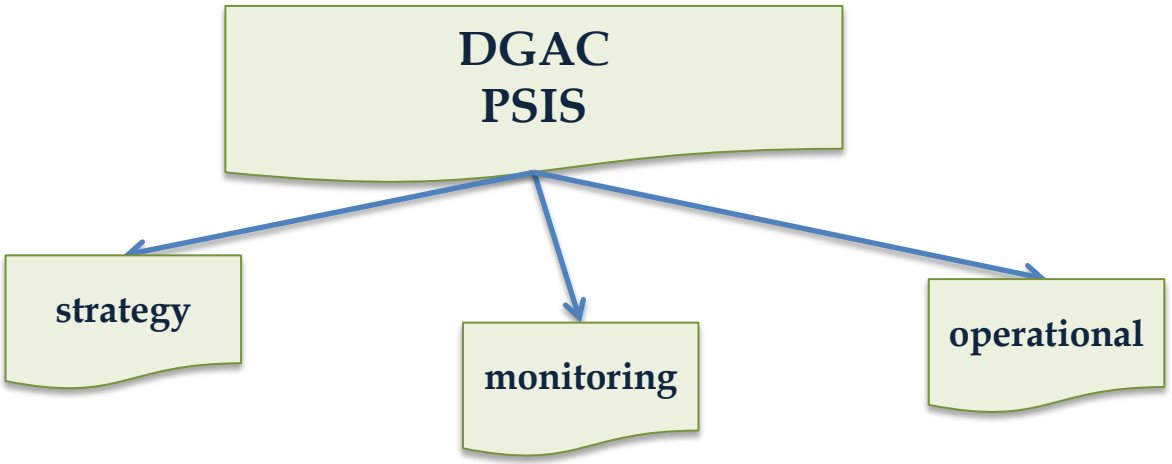
As required by the CIIP law, DGAC has defined its own Policy on Security for Information Systems (PSIS)



DGAC Policy on Security for Information Systems (PSIS)

Main objectives of DGAC PSIS

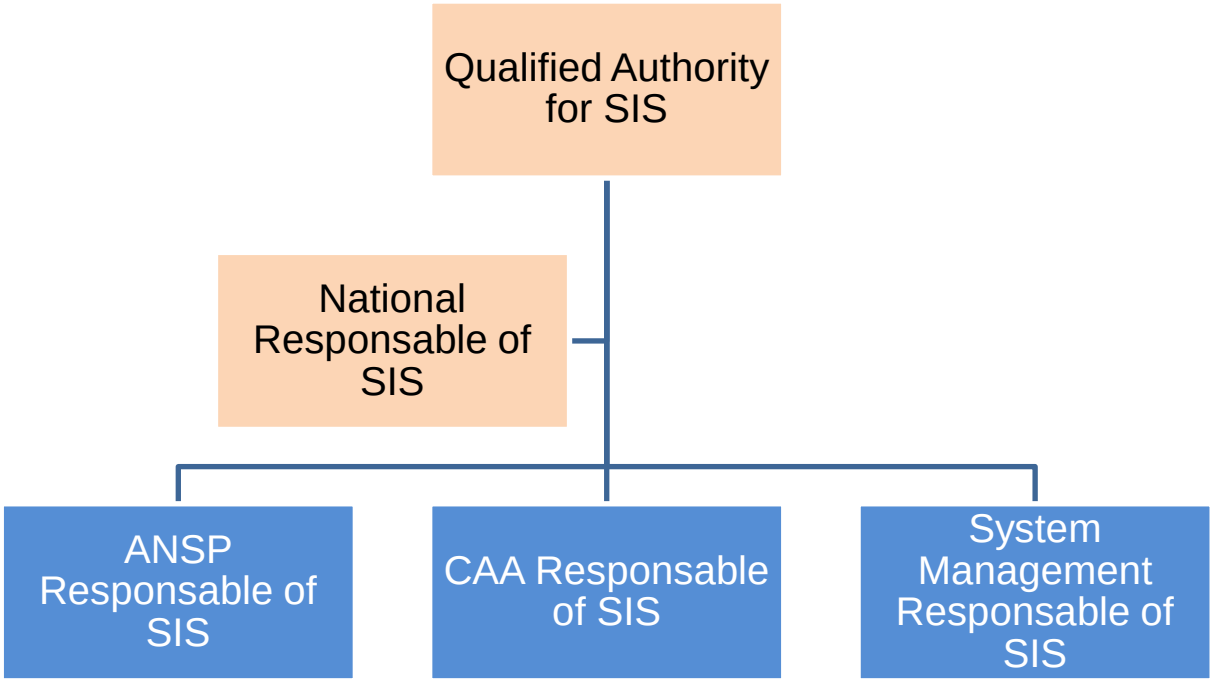
Governance & Prevention | **Protection & control** | **Detection & Reaction**



DGAC organisation on cybersecurity

Governance on cybersecurity :

- Strategy
- Monitoring
- Operational



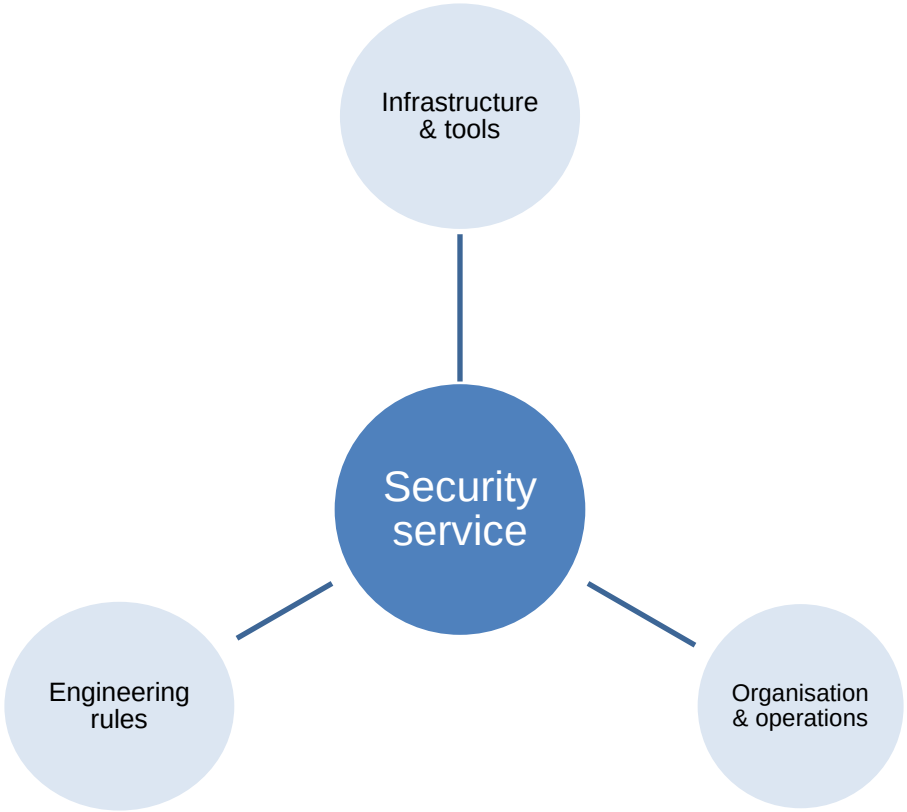
DGAC organisation on cybersecurity

Step-by-step and pragmatic approach for the monitoring and implementation of cybersecurity :

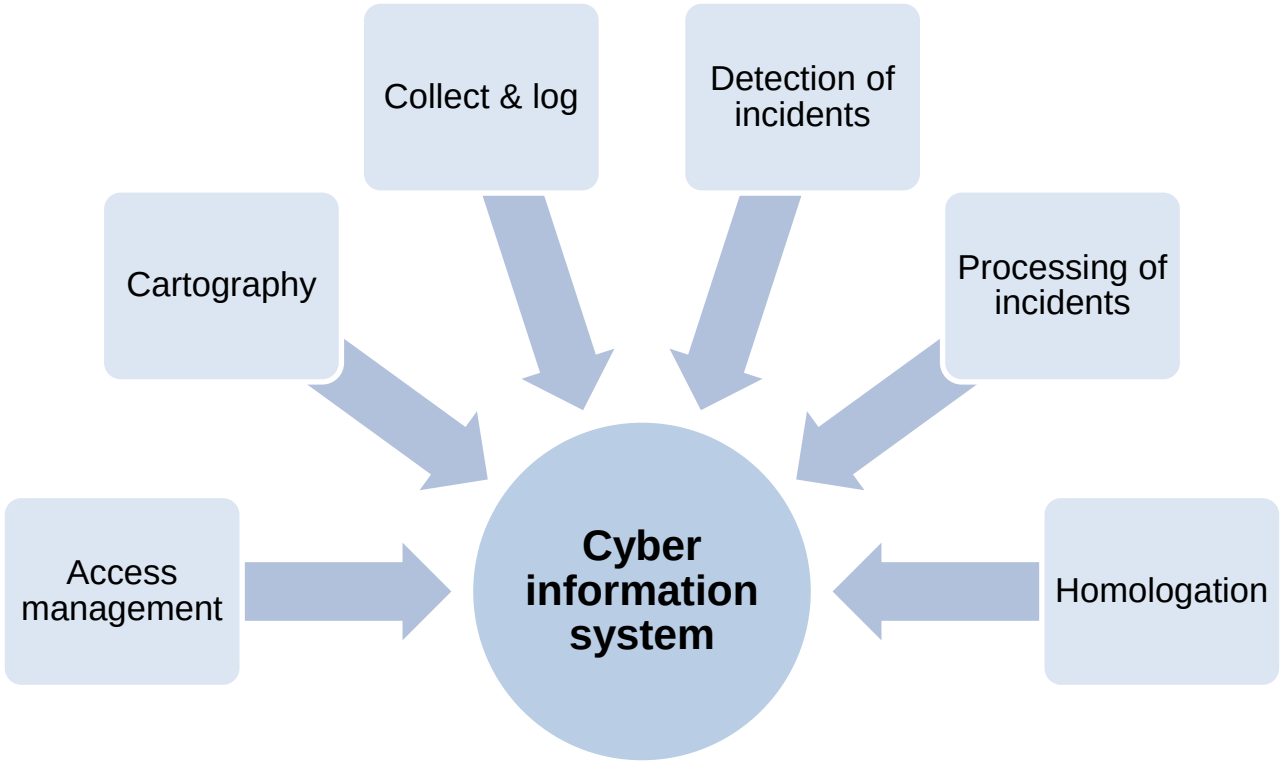
- Remain in charge of the management of cybersecurity on its systems
- Tackle the more sensitive issues first
- Take into account human and financial resources
- Integration of cybersecurity within the existing organisation, processes and culture

Cyber information system

Implementation of a cyber information system that is service oriented :



Security services

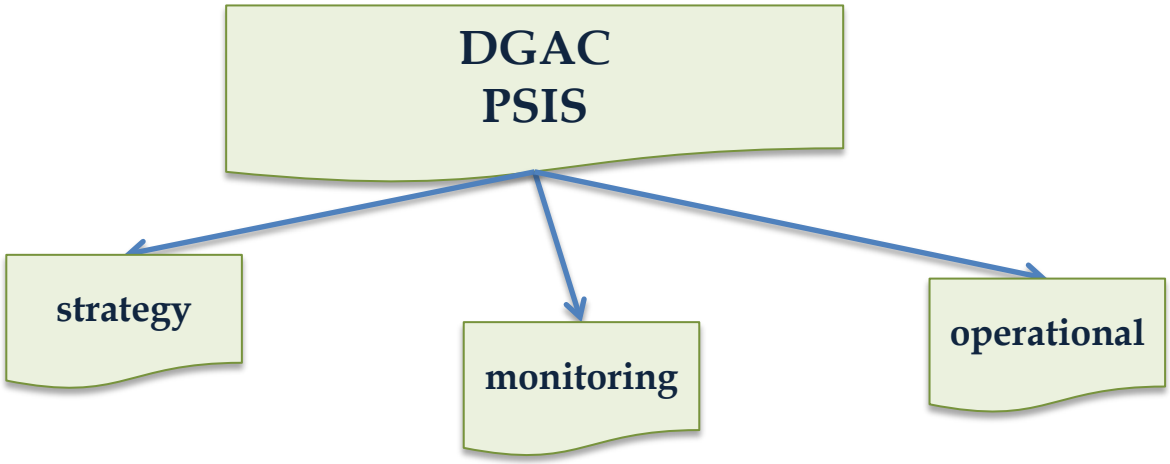


Cybersecurity at the operational level in DSNA, the French ANSP

Cybersecurity at the operational level in the French ANSP

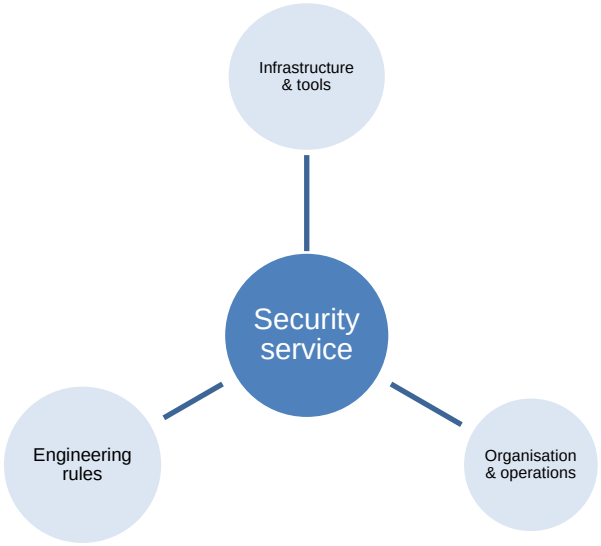
1. The French ANSP within DGAC PSIS
2. Implementation of protecting measures
3. Operational monitoring and response
4. Risk assessment
5. Promotion of cybersecurity within and outside of the French ANSP

DSNA within PSIS



- DSNA takes part in all objectives of PSIS
- DSNA has taken PSIS into account in its organisation and processes

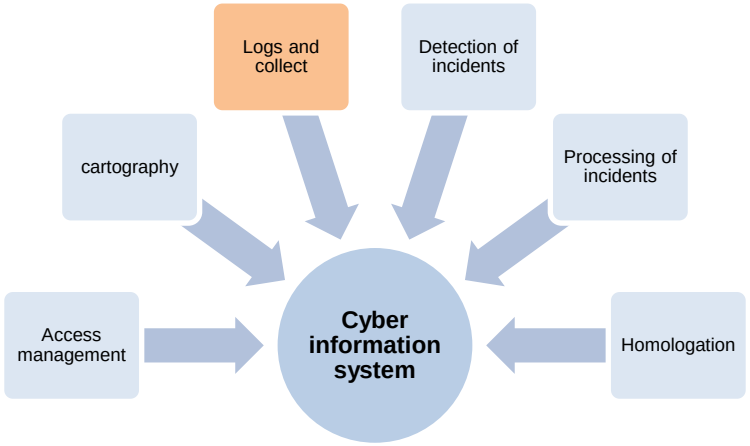
Implementation of protection measures



DSNA has implemented its protection measures following the requirements in the DGAC PSIS based on security services :

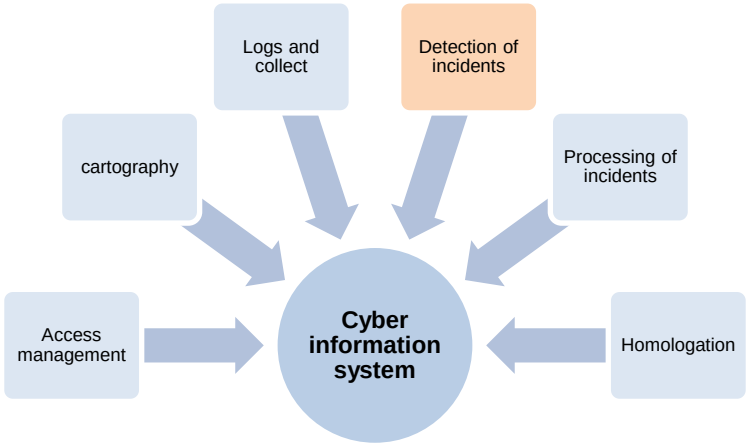
- containment between networks and systems,
- Systems protection via gateways…

Operational monitoring



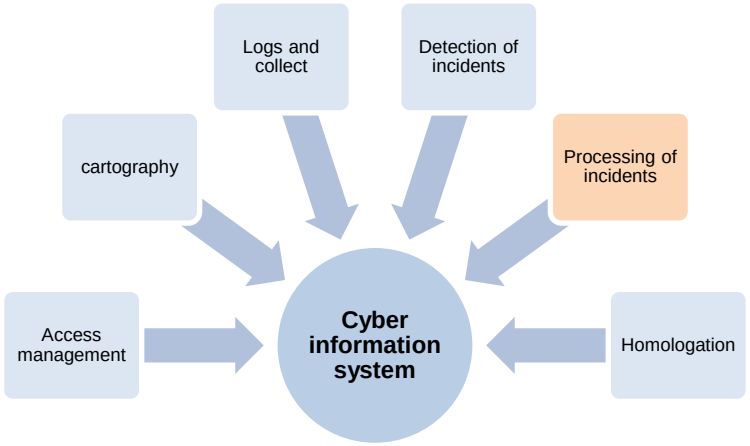
- DSNA has implemented :
  - a national Security Operations Center (SOC) with experts in detection and response to cyberthreats
  - a secured network to collect data
  - a system to process logs

Detection of incidents



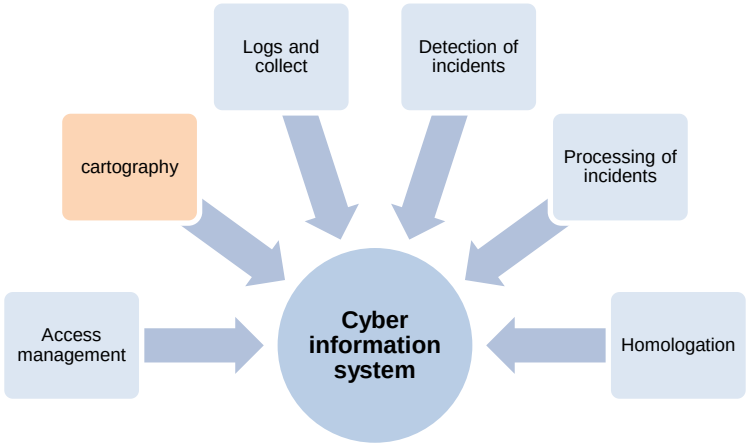
- The SOC implemented by DSNA is in charge of detection of incidents and response to these incidents
- Two types of expertise for an adequate answer to an incident:
  - Cybersecurity experts
  - Operational systems experts
- DGAC and DSNA are organised to answer to a cyber incident from technical experts to top management

Processing of incidents



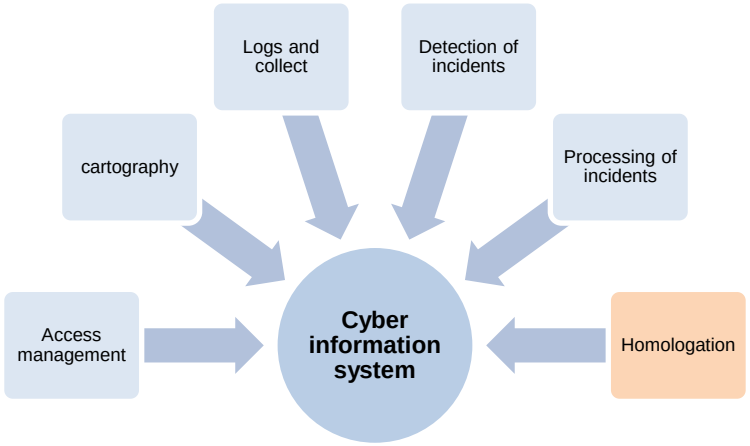
- The SOC implemented by DSNA is in charge of incident analysis at the technical level
- At monitoring level, incidents with possible impact on the activities of DSNA are reviewed
- Amendements could be implemented at appropriate level : technical, procedural, organisational…

Risk assessment



- Risk assessment for existing systems and networks in CNS and ATM :
  - changes in existing systems and network
  - Protection measures defined and implemented either at local or national level
- Risk assessment for new systems and networks in CNS and ATM :
  - Systematic assessments of cyberthreats
  - Specifications defined taking into account cybersecurity issues

Monitoring of cyber information system



- Actions towards awareness of all personnel on cybersecurity issues
- Specific trainings
- Auditing
- For SNA Antilles Guyane, part of DSNA, communication and coordination on cybersecurity issue with neighboring ANSP in meetings SAT, Reddig, E/CAR

Thank you for your attention