Summary of Captain Briand's Presentation: France's Organization to Face Hybrid Strategies

1. Introduction and Context

Captain Briand intervenes to reassure the audience following a "worrying" presentation on hybrid threats, while emphasizing the maturity of France's organizational response. He presents jointly with a colleague and highlights the quality and importance of the work done by the Helsinki Centre of Excellence, which is crucial for raising awareness and aligning capitals on hybrid threats.

He serves at the General Secretariat for Defence and National Security (SGDSN), an institution over 150 years old, under the authority of the Prime Minister, with a direct link to the Élysée Palace.

Mission: The SGDSN coordinates interministerial actions on defence and security, with particular attention to hybrid threats.

2. National Strategic Review (July 2025)

Nature of the document: Not limited to a single defence review, but a comprehensive document covering a wide spectrum of threats and measures to address them (e.g., 10% dedicated to economic security).

Structure:

1. Threat assessment
2. Ambition for 2030
3. Means and concrete measures (e.g., new laws, budgets, organizations)

Main threats and challenges identified:

1. **Russia:** Primary threat; NATO remains essential for Europe's defence, but the EU plays a central role, particularly in developing the European defence industry and responding to hybrid strategies.
2. **Other threats:** Iran, instability in the Middle East and Africa, North Korea, terrorism, organized crime, climate change, access to raw materials.
3. **Challenges posed by China** (cyberattacks, technology theft, rivalry with the US, support for Russia) and by the evolution of US policy.

Main scenario:

1. Preparation for a conventional war in Eastern Europe by 2030, coupled with a significant increase in hybrid attacks on French/European territory.
2. **Challenges:** Military forces deployed to the East require addressing hybrid attacks on national territory primarily through other means (e.g., reserves, voluntary national service from summer 2026), managing "polycrises" (e.g., simultaneous crises in the South China Sea and Eastern Europe).

Strategic objectives (11 in total):

- **Nuclear deterrence:** Ensures France remains below the threshold of conventional war on its territory.
- **Population resilience:** France lags behind Finland, Sweden, and the Baltic states in terms of preparedness and mindset; the goal is to improve these aspects.
- **Intelligence services:** Crucial for nuclear deterrence and understanding hybrid threats (e.g., attributing information manipulation).
- **Hybrid threats:** By 2030, France aims to constrain adversaries (impose costs, manage escalation, uphold democratic rules).
- **Other objectives:** Economic security, strengthening military capabilities, protecting critical infrastructure.

4. Organization Against Hybrid Threats Doctrine: Classified, but a public version is expected in 2026.

Definition of hybrid threats: Coordinated strategies using legal/illegal, direct/indirect, military/non-military levers, aimed at weakening France/Europe while staying below the threshold of armed conflict.

Concern: Russia is increasing the frequency and violence of attacks, approaching the threshold of conventional conflict.

Priority areas (5+1): Cyber, information manipulation, "lawfare," economic security, protection of military operations, and protection of critical infrastructure (likely to be added soon).

Example: Cyber and information domains Tools: National (ANSI, Cyber Command, intelligence services) and European (Digital Services Act, Digital Markets Act).

Governance: Interministerial committee chaired by the SGDSN, with a direct link to the Élysée for sensitive decisions.

Information domain: Viginum (agency for detecting information manipulation), Ministry of Foreign Affairs for attribution, interministerial coordination.

Role of the EU and NATO:

- **EU:** Implementation of the Digital Services Act, anti-coercion instrument (developed after the Lithuania-China crisis), economic security.
- **NATO:** Ensuring the credibility of Article 5, military mobility, protection of infrastructure (e.g., cyberattacks on ports hosting military reinforcements).

5. Conclusion France is preparing for the most serious and demanding scenarios, investing particularly in resilience, intelligence, and interministerial coordination.

Objective: Constrain adversaries, manage escalation, and protect society below the threshold of armed conflict.

Call to action: Immediate reaction is necessary to avoid reaching the level of conventional conflict.