The European Union’s low-profile Intelligence and Situation Centre (INTCEN) is suddenly at the heart of a high-stakes argument about how Europe should organise power, secrecy and sovereignty in a much harsher security environment. This op-ed argues that the EU should expand and reform INTCEN as its primary intelligence hub rather than build overlapping structures in the Commission that risk politicisation and fragmentation of trust.

# What INTCEN is — and isn’t

INTCEN is not a European CIA or MI6; it has no collection powers and relies entirely on intelligence voluntarily provided by national services, open sources and diplomatic reporting. Structurally, it is a civilian intelligence analysis directorate inside the European External Action Service (EEAS), reporting to the High Representative for Foreign Affairs and Security Policy and serving the EU’s foreign, security and defence decision-making. Its core job is to fuse these inputs into all-source strategic assessments, early warning and situational awareness products—around a few hundred a year—shared under a strict need-to-know principle with EU institutions and member states.

The Commission’s new internal security strategy, ProtectEU, explicitly puts “anticipation of security threats” and “new ways of sharing intelligence and threat analysis” at its core, signalling a political appetite to move intelligence cooperation from the margins to the mainstream of EU policy. This sits alongside the EU’s Strategic Compass for Security and Defence, which pledges to “boost intelligence analysis capacities” by 2030 as part of a broader push to make the Union a more capable security actor. Yet these ambitions run up against a stubborn legal and political reality: Article 4 of the Treaty on European Union reserves “national security” as the sole responsibility of member states, making any centralisation of intelligence inherently sensitive.

The push for a stronger EU intelligence hub is not occurring in a vacuum; it is a direct

response to Russia's full-scale invasion of Ukraine and to repeated warnings from U.S. leaders about scaling back American security guarantees. Faced with hybrid attacks, cyber operations and disinformation campaigns, European capitals have learned the hard way that fragmented threat pictures can delay responses and leave vulnerabilities unaddressed. In that sense, the impulse behind the security overhaul—more sharing, faster analysis, better early warning—is not only understandable but overdue.

# Risks of a parallel intelligence hub

Instead of simply upgrading INTCEN, the Commission is exploring a new intelligence coordination unit inside its powerful Secretariat-General, staffed with seconded officers from national agencies to fuse data for strategic use. Officials in the EEAS, which oversees INTCEN, are already warning that such a unit could duplicate the Centre's work and ultimately undermine its role as the bloc's established intelligence hub. At worst, this risks creating competing intelligence poles in Brussels—one anchored in the diplomatic service, another in the Commission's political engine room—encouraging member states to pick favourites and weakening the overall incentive to share.

Member-state services are wary of any move that smells like a creeping transfer of national security competences to the EU level, especially if it empowers an institution—the Commission—whose core mandate is regulatory and political rather than diplomatic and security-focused. Intelligence is not just about secrecy; it is about relationships, reciprocity and the confidence that sensitive reporting will not be instrumentalised in day-to-day policy battles or leaked in institutional turf wars. If capitals suspect that a new central hub will essentially become another tool in Brussels' political toolbox, they will respond in the only way they can: by tightening the tap and sharing less, not more.

# Why reforming INTCEN is the better bet

INTCEN already provides a single entry point for classified information from member states' civilian intelligence and security services, handles material up to "EU TOP SECRET", and is integrated with the EU Military Staff's intelligence division as part of a Single Intelligence Analysis Capacity. That existing architecture could be significantly strengthened—more staff, better technology, clearer tasking from both the Council and Commission—without triggering the same sovereignty alarm bells as a new Commission-centric body. Crucially, keeping the main hub under the EEAS preserves a degree of institutional distance from day-to-day legislative bargaining, which helps reassure national agencies that their reporting will be used for strategic assessments rather than tactical policy fights.

If INTCEN is to become the linchpin of the EU's revamped security strategy, three guardrails are essential. First, its mandate should be explicitly reaffirmed as an analytical fusion centre with no collection powers, to respect national prerogatives and reduce fears of a stealth "EU spy service." Second, democratic oversight by the European Parliament and robust data-protection safeguards need to grow in parallel with its influence; the more central intelligence becomes to EU policy, the less sustainable the current opacity will be in a Union built on the rule of law. Third, any new Commission intelligence cell should be clearly subordinated to, or at least tightly coupled with, INTCEN rather than set up as a rival hub, with formal mechanisms for tasking and feedback that prevent duplication and mixed signals to member states.

Europe's choice is not between "more" or "less" Europe in intelligence, but between an integrated, trusted system and a messy patchwork of overlapping structures that satisfy institutional egos while failing to deliver security. A bigger role for INTCEN, anchored in the EEAS, offers the best chance of improving strategic awareness without crossing the red line of national sovereignty or politicising intelligence in the Commission's machinery. If Brussels

instead builds rival hubs and treats intelligence as just another policy file, it may discover too late that the real casualty of its security overhaul is the one resource it cannot legislate into existence: the trust of those who hold the secrets it needs.