Executive Summary:
European Democracy Resilience Network (EDRN)

Overview

The **European Democracy Resilience Network (EDRN)** is a blueprint initiative co-created by the CyberPeace Institute and EU DisinfoLab, alongside a cohort of 30+ civil society organisations (CSOs) working to protect democratic spaces. The pilot ran from August 2025 to January 2026 and focused on co-developing a community-informed dashboard concept to help CSOs detect, understand, and mitigate hybrid threats including disinformation/foreign information manipulation and interference (FIMI), and malicious cyber operations.

The pilot combined (I) a baseline needs assessment (survey + kick-off discussions), (II) four thematic working groups, and (III) a structured review that translated participant feedback into a refined dashboard module proposal, organised around three pillars: "Your Organisation," "EDRN Trends," and "Resources."

Key Insights

- **Hybrid threats are no longer the exception.** Across survey findings and working groups, participants consistently described converging risks where disinformation/FIMI is reinforced by cyber tactics (phishing, impersonation, account takeovers, leaks/doxxing, surveillance), producing simultaneous pressure on staff safety, systems, and organisational legitimacy.

- **The biggest gap is not awareness; it's operationalisation.** The baseline survey revealed uneven preparedness: many organisations report frequent targeting, but lack consistent monitoring, formal incident tracking, systematic training, and documented response planning. This "policy-to-practice" gap was apparant throughout discussions.

- **CSOs want actionable, lightweight tools.** Participants repeatedly prioritised pragmatic outputs: simple alerts, a "narrative radar," impersonation monitoring, and clear first-step guidance tailored to low-capacity teams. They emphasised usability for non-cyber-specialists and avoiding information overload.

- **Monitoring alone is insufficient**. Working groups stressed that effective defence requires evidence logging and archiving, clear reporting/escalation routes to platforms, regulators, and trusted-flagger-type channels. There was strong interest for reusable playbooks/templates, alongside wellbeing guidance for staff.

- **Trust makes shared situational awareness possible.** Participants highlighted a "visibility gap": many threats remain siloed, semi-private, or hard to attribute across organisations. A key EDRN element was identified to be the safe, anonymised sharing of information that can help organisations spot patterns earlier, learn from peers, and coordinate responses, reducing duplication and strengthening resilience across the ecosystem.

- **The blueprint produced a concrete, participant-driven product direction.** The final dashboard review translated working group feedback into specific modules and a roadmap-minded structure. Proposed additions include: Risk Profile & Triggers, First 24h Checklist, Incident Stories, Impersonation Trends, plus Crisis Communication Kit, Simulation Toolkit, and a Reporting Hub - designed to strengthen readiness, response, and shared learning.

Next Steps and the Need for Funding

To move EDRN from a successful pilot to a platform with sustained impact, the initiative should now focus on operationalising the blueprint into deliverable, low-burden support for CSOs facing hybrid threats. This means turning the co-designed concepts into modular, user-friendly tools and guidance that help organisations anticipate, detect, and respond to incidents. In parallel, EDRN should consolidate its trusted collaboration model, supporting safe information sharing, practical peer learning, and reusable playbooks, so that collective awareness and coordination become routine.

Dedicated funding is required to build and maintain this shared infrastructure at scale. In an increasingly hostile environment, accelerated by generative AI, and with democratic resilience funding becoming scarcer, EDRN offers a rare mechanism to reduce duplication and strengthen cooperation across the ecosystem. Investment would enable EDRN to develop and securely operate the platform and modules, resource community coordination and governance, and rapidly extend reach through the CyberPeace Institute's CyberPeace Builders network of over 600 CSOs, ensuring frontline organisations can access the support they need without delay.