European Democracy Resilience Network

EDRN Blueprint Report

February 2026

Table of Contents

Table of Contents

Executive Summary

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 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.

Overview

The European Democracy Resilience Network (EDRN) is a blueprint initiative co-created by the **CyberPeace Institute (CPI)** and the **EU DisinfoLab (EUDL)** with a cohort of more than 30 civil society organisations working to protect democratic spaces. This pilot initiative ran from August 2025 to January 2026 and focused on the co-development of a dashboard blueprint used to protect CSOs operating in the democratic sphere from hybrid threats including disinformation, foreign information manipulation and interference (FIMI) and malicious cyber operations. This work was complemented by cybersecurity insights from the **CyberPeace Builders programme** (CPB)**.** The success of EDRN's community-building efforts was made possible in large part thanks to the foundational networks and trust cultivated by EU DisinfoLab, whose longstanding engagement with civil society actors across Europe laid the groundwork for rapid collaboration and uptake.

EDRN aims to strengthen the defensive capabilities of these organisations against digital threats and hybrid attacks, especially those combining cyber tactics and information manipulation.

A dedicated webpage for the EDRN Pilot Project can be accessed here: **https://edrn.cyberpeaceinstitute.org/**

Timeline

August 2025

- Identification of organisations operating in the democratic resilience sphere
- Initial contact for expression of interest

September 2025

- Surveys conducted
- Kick-off Meeting with survey results, breakout discussions, and a mock-up dashboard as a starting point; 30+ organisations attended.

October 2025

- Onboarding organisations into CPB program
- Creation of EDRN webpage
- Pilot presentation at EUDL Conference #DIsinfo2025
- 1st working group - Social Media Monitoring & Weak Signals

November 2025

- 2nd working group- Shared Resources & Access to Support
- 3rd working group - Threat Intelligence & Trends

December 2025

- 4th working group - Risk Assessment, Crisis Communications & Policy Uptake

January 2026

- Blueprint presentation to EDRN participants
- EDRN Blueprint Report

Initiative Takeaways

Kick-Off Meeting and Survey Results

On 15 September 2025, the CyberPeace Institute and EU DisinfoLab hosted a kick-off meeting for EDRN. Initial outreach drew strong interest, with more than 30 organisations attending the kick-off session to share their experience and expertise. Eligible participants were also briefed on how to access the CyberPeace Builders programme. Ahead of the meeting, participants completed a survey that offered an initial snapshot of their experiences as targets of disinformation campaigns, their cybersecurity practices, and incident-response capacity.

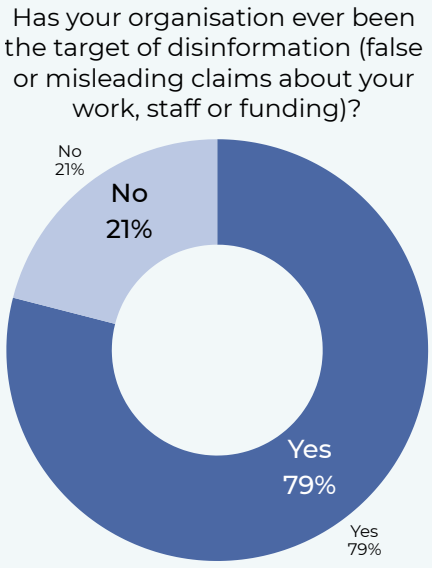
Summary of Survey Results:

A pre-meeting survey of 29 organisations (90% nonprofits) showed frequent disinformation exposure, uneven cybersecurity preparedness, and gaps in incident tracking and response. These insights defined the project baseline and where EDRN support would add most value. A breakdown of the survey results has been included.

Disinformation

Most participating CSOs reported exposure to disinformation. 23 out of 29 **(79%)** say their organisation has been targeted.

- **52%** reported coordinated online attacks such as troll campaigns, fake accounts, or data exposure.
- **28%** frequently - or almost constantly - encountered false or misleading online narratives mentioning their organisation or staff; and **31%** experienced them occasionally.
- Incidents often involved **false claims about staff, affiliations, or funding**.
- Some responses refered to **media outlets** being used to legitimise disinformation or misrepresent leaked private materials.



- While the level of detail varied, several organisations described **hybrid threats**, where disinformation was reinforced by cyber intrusions or surveillance.

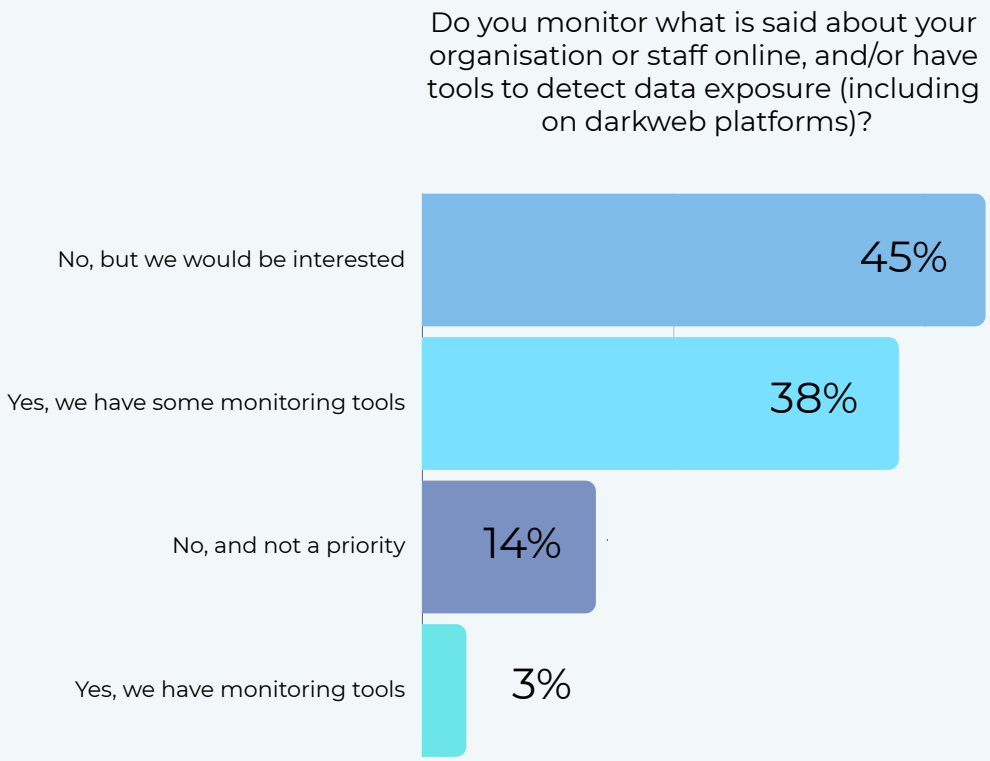
Incident Tracking

A majority of respondents did not have formal tracking systems in place. Where tracking did occur, it was typically manual or limited in scope, often relying on individual staff noticing patterns or mentions.

A few organisations used basic monitoring tools, while others explicitly stated they lacked capacity or resources for systematic reporting. This highlighted a need for lightweight, easy-to-use tracking mechanisms that can integrate into CSO workflows without requiring advanced technical infrastructure.

Monitoring Practices

Monitoring for mentions online or potential data leaks was inconsistent across participating CSOs. While some organisations actively tracked social media and news coverage, most respondents either lacked systematic monitoring or do so only informally. Nearly half **(45%)** said they would like to have monitoring tools but do not currently use them.



Policy & Organisational Preparedness

Organisations showed mixed levels of preparedness when it comes to policies and organisational preparedness. Just over half (52%) reported having internal guidelines on protecting sensitive information, such as staff use of social media or what can safely be shared publicly. Others noted that while staff are generally cautious, no formal protocols were in place. This uneven implementation highlighted the demand for clearer templates, training, and awareness materials.

When it comes to incident response planning, nearly half of organisations (45%) reported that they rely on informal or ad hoc arrangements, while just over one-third (35%) have no plan at all. Only 10% reported having a formal, documented plan for responding to cyberattacks, disinformation, or data breaches, and a further 10% were unsure whether such a plan exists. The findings suggested that many CSOs remain vulnerable once incidents occur, even when basic awareness exists.

Together, these results revealed a clear internal policy gap - while awareness of threats is widespread, the translation into organisational procedures is inconsistent. Addressing this gap was identified as critical by EDRN, particularly through the development of response templates, simulation exercises, and shared best practices.

Baseline Protection & Technical Readiness

Basic technical protections were uneven across participating organisations. While some had adopted multi-factor authentication (MFA) or had conducted a vulnerability scan or security audit, a significant share had not. This indicated varying levels of preparedness to withstand cyber incidents.

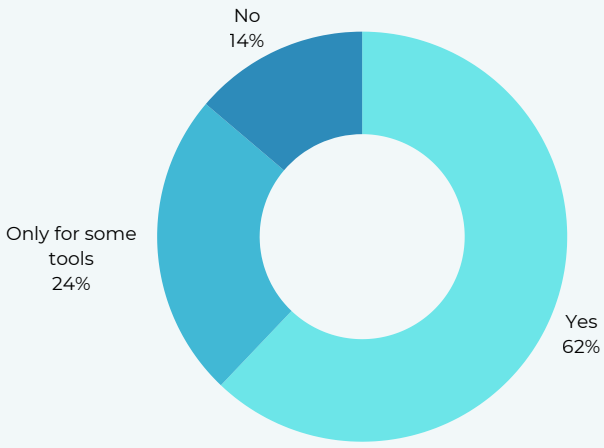
Vulnerability scans and audits

Nearly half **(45%)** of organisations were not sure if they had ever conducted a security audit or vulnerability scan. **21%** reported having done so once. Only **14%** said they do so regularly, while another **21%** reported never having conducted one.

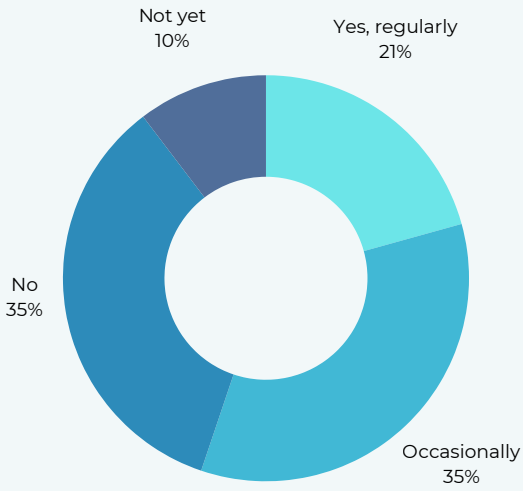
Device and server protection: When asked to rate the protection of their devices and servers (e.g. antivirus, firewalls, malware detection) on a scale of 1–5, responses were spread across the spectrum: **10%** scored 1, **17%** scored 2, **21**% scored 3, **24%** scored 4, and **28%** scored 5. This highlights a split between organisations with strong safeguards and those with only moderate protection levels.

Multi-factor authentication (MFA): Just under two thirds **(62%)** reported using MFA across key platforms, while **24%** apply it only to some tools, and **14%** did not use it at all.

Do you use multi-factor authentication (MFA) for accessing key platforms or sensitive systems (e.g., email, social media, finance tools)?



Do you provide basic cybersecurity or digital resilience training to your staff or volunteers?

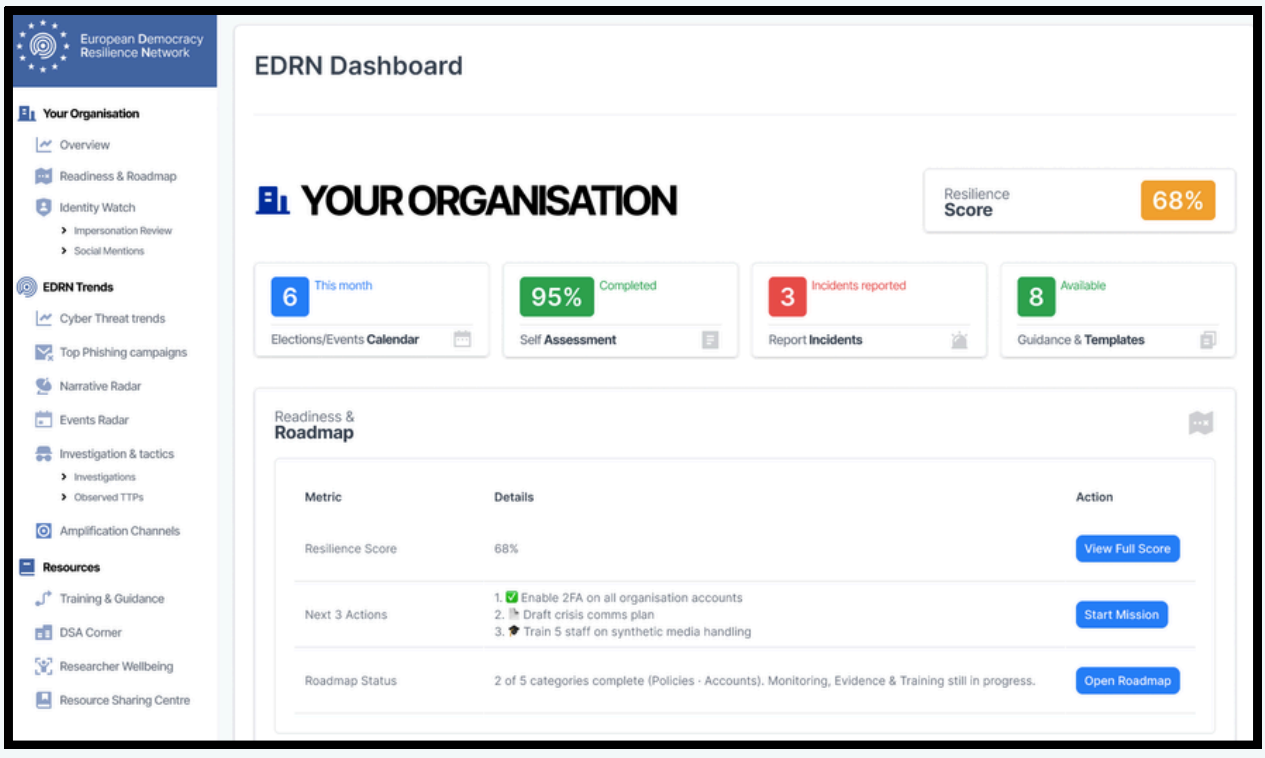


The survey also showed that training is not systematic across the participant organisations. Only **21%** provide regular cybersecurity or digital resilience training to staff and volunteers, **35%** do so only occasionally. **35%** provide no training at all, and **10%** had not yet begun training efforts.

Dashboard Prototype:

Following the presentation of the survey results, participants were then shown a prototype dashboard; while only a demo, it served as a visual starting point for how EDRN could integrate monitoring, reporting, and resilience features in one place. This dashboard included three main components, “Your Organisation”, “EDRN Trends” and “Resources”.

The “Your Organisation” component included tools such as a readiness & roadmap, resilience scores, next steps for your organisation, an identity watch with mentions on social media. “EDRN Trends” included overall threats to EDRN organisations, top phishing threats, a narrative radar, an events radar, investigations & TTPs, and amplification channels. “Resources” included training & guidance, researcher wellbeing, and a resource sharing center. A more in-depth review of this prototype is included in a later section of this report.



Breakout Discussions:

Following the dashboard presentation, participants were then divided into breakout groups for discussions. In these discussions, participants described facing a broad mix of digital threats including, but not limited to coordinated disinformation and smear campaigns, phishing, hacking, impersonation, and infrastructure compromise like website breaches or blocked accounts. Several participants also highlighted "hybrid" dynamics where cyber operations reinforce disinformation narratives, often around politically sensitive work and are accompanied by intimidation and harassment targeting both individuals and organisations. Participants repeatedly asked for a single place to see narrative tracking, cross-platform mention monitoring (including fringe/dark web spaces), and multilingual alerts that can uncover coordination (bot amplification, early influence-operation indicators) as well as direct risks like account takeovers, leaks/doxxing, and spyware. Participants wanted alerts that work at both levels, organisation-specific signals (e.g. sudden mention spikes or reputation attacks) and community-wide situational awareness (e.g. coordinated narrative shifts or peer targeting) in a simple format that especially doesn't overwhelm non-cyber specialised personnel. Moreover, they strongly favoured launching a "narrative radar" that shows how disinformation/FIMI narratives evolve across the ecosystem and whether a specific organisation is being referenced, alongside a shared repository of attack data and response examples to support faster, more confident action and collective learning.

Breakout Group Takeaways

- Participants reported a wide range of digital threats: coordinated disinformation/smear campaigns, phishing, hacking, impersonation, and infrastructure compromise
- Several emphasised "hybrid" attacks
- Participants repeatedly asked for a single hub for:
  - narrative tracking
  - cross-platform mention monitoring (including fringe/dark web spaces)
  - multilingual alerts
- Participants wanted alerts that can identify both:
  - coordination signals (e.g., bot amplification, early influence-operation indicators)
  - direct risks (e.g., account takeovers, leaks/doxxing, spyware)
- Participants asked for alerts at two levels:
  - organisation-specific signals
  - community-wide situational awareness

- Participants stressed the output should be accessible and not overwhelming for non-cyber-specialist staff.
- Strong preference to launch a “narrative radar” showing how disinformation/FIMI narratives evolve and whether specific organisations are referenced.
- Participants also wanted a shared repository of attack data and response examples to enable faster action and collective learning.

Participation at Disinfo2025 (Ljubljana, October 2025)

At the 2025 edition of the EU DisinfoLab conference in Ljubljana, Slovenia, the EDRN was featured both through a dedicated lunch session and ongoing visibility at the venue. Informational brochures and flyers were distributed in the main networking areas, offering an overview of the project, key conclusions from its first phase, and information on how organisations could join. During the lunch session, Inês Narciso (CyberPeace Institute) and Alexandre Alaphilippe (EU DisinfoLab) presented EDRN’s scope and relevance. While Narciso introduced the blueprint initiative and its aims to defend CSOs from hybrid threats, Alaphilippe shared a real-world case study involving a phishing email and disinformation campaign that targeted multiple civil society actors.

The session emphasised the growing mismatch between the expectations placed on civil society to monitor, investigate, and respond to information manipulation and the resources or protection available to do so. It underscored the urgent need for institutional support that empowers independent actors to act without fear or exposure to escalating hybrid threats. The presentation also highlighted the enthusiastic reception to the EDRN project: interest exceeded room capacity, and follow-up working groups confirmed how the network fosters trust, collaboration, and open sharing. The project’s defensive and community-led approach has proven key in creating solidarity and resilience in a space increasingly shaped by competition, scarcity, and high-stakes exposure.

Summary of Working Groups

This section covers the individual working group sessions held in late 2025. Working Group 1 featured a presentation and discussion led by CPI and EUDL. Working Groups 2–4 followed the same format, with an added live poll. Results reflect input gathered and represent a limited, indicative sample intended to draw out concepts for further exploration and broader community validation.

WG1: Social Media Monitoring & Weak Signals

WG1 focused on how CSOs can use social media and adjacent channels to detect "weak signals" and get earlier warning of hybrid threats, and what the EDRN dashboard should prioritise. Participants stressed that information manipulation and cyberattacks are increasingly converging, and that CSOs need actionable alerts rather than generic awareness. "Weak signals" were framed as early indicators that can reveal emerging risks or coordination, such as sentiment shifts, bursts of mentions/hashtags, coordinated reposting, misuse of logos/imagery, and look-alike URLs/domains.

In terms of lived experience, participants described coordinated targeting on social platforms (bot-like, near-identical comments kept just below hate-speech thresholds; hostile waves hitting promoted posts and forcing deletions), traffic/referral anomalies and outages (sudden spikes, unusual referrers like messaging applications, downtime and DDoS concerns), and "operational flooding" like sudden surges of incoming emails used to disrupt work. They also highlighted how narratives can incubate in small or semi-closed channels and later scale into larger platforms with a shift toward negative tone making it hard to observe escalation inside closed groups. Harassment and reputational harm (e.g., insulting calls, false accusations, name/brand collisions) and "adversary signalling" (actors bragging about attacks) were also cited.

The group's needs map directly to dashboard priorities: real-time detection of spikes/surges (mentions and web traffic, ideally with geolocation), impersonation monitoring across accounts and domains (including reappearance tracking after takedowns), and cross-platform narrative awareness with multilingual coverage. They also asked for clearer escalation guidance (how/when to report to platforms, registrars/hosts, and possibly regulators), concise readiness materials (short checklists, brief self-assessments, basic playbooks), and case logging of account takeovers and platform responses to support policy pressure. A core takeaway was a "visibility gap": many threats play out semi-privately or invisibly (impersonation, inbox flooding, hostile ads, smear campaigns), so without a trusted shared space like EDRN, incidents remain siloed and patterns across organisations are missed underlining the value of anonymised sharing and collective situational awareness.

WG1 Takeaways

- Disinformation/information manipulation and cyberattacks are increasingly converging; CSOs want actionable alerts, not generic awareness.
- "Weak signals" matter as early indicators of risk/coordination (sentiment shifts, mention/hashtag bursts, coordinated reposting).
- Other weak signals cited: misuse of logos/imagery and look-alike URLs/domains.
- Participants described coordinated social targeting (bot-like near-identical comments, attacks on promoted posts prompting deletions).
- Participants reported traffic/referral anomalies and outages (spikes, odd referrers like messaging apps, downtime/DDoS concerns).
- "Operational flooding" was noted, including email surges designed to disrupt work.
- Narratives are often cultivated in semi-closed channels, then scale to major platforms with a shift to negative tone.
- Harassment/reputational harm and "adversary signalling" (e.g., bragging) were common.
- Priority needs: real-time spike detection (mentions + web traffic, ideally geolocated), impersonation monitoring (accounts/domains + reappearance tracking), and multilingual cross-platform narrative awareness.
- Participants want clearer escalation guidance, concise readiness materials, and shared/anonymised incident logging to close the "visibility gap" and spot patterns across organisations.

WG2 : Shared Resources & Access to Support

WG2 focused on what shared resources would be most useful for CSOs dealing with cyber threats and disinformation/FIMI, and how EDRN could structure community-driven sharing. The session prompted participants to prioritise immediate resource needs, identify blockers to pooling resources, rank which playbooks/templates should come first, and specify what guidance is needed to apply legal frameworks alongside researcher wellbeing and preferred formats for sharing (including a community "sharing board").

A central theme was that monitoring is not enough without escalation, archiving, and evidence logging. Participants emphasised platform escalation routes (including trusted-flagger-type pathways), noting cases where legitimate public-interest content was removed and, in some instances, entire archives were not recovered suggesting a network like EDRN could carry more weight in escalations. They strongly advocated pairing monitoring/alerting tools with archiving plus evidence logging to prevent irreversible loss after takedowns and to support reporting and follow-up. They also prioritised reusable playbooks and templates to standardize response protocols (e.g. digital footprint assessments; attack reporting and "who to report to"; first steps for suspected cyber incidents; impersonation/account recovery; doxxing response; and incident briefs for boards/donors).

On legal and wellbeing support, participants wanted practical, case-based guidance, decision trees and example "case packs" showing what worked or didn't, including privacy complaints and spyware targeting, and how GDPR-like standards may apply even in non-EU contexts where comparable protections exist. They also underscored researcher/staff wellbeing and organisational readiness as a resilience requirement (harassment protection, self-care practices, signposting to health support, and examples of effective techniques). For delivery, they preferred concise, usable formats: one-page checklists, copy-ready template packs, directories/contacts, short video walkthroughs (including free courses/MOOCs), and vendor discounts/shared seats, plus collaboration spaces for country-specific fact-checking, expert referrals, and partner matching. Key blockers to sharing/pooling included limited time/capacity, uncertainty about what's most useful to share, data sensitivity/PII, language/region coverage gaps, lack of a trusted network, and vendor license constraints.

WG2 Takeaways

- Participants prioritized immediate resource gaps, blockers to pooling, which playbooks/templates should come first, and what legal + wellbeing guidance is needed.
- Core message: monitoring alone isn't enough; escalation pathways, archiving, and evidence logging are essential.
- They emphasized stronger platform escalation routes (including trusted-flagger-style channels), citing cases of wrongful takedowns and unrecovered archives.
- Strong preference to pair monitoring/alerts with archiving + evidence logging to prevent irreversible loss and support reporting/follow-up.
- They prioritized reusable playbooks/templates to standardize response (e.g. footprint assessments; reporting routes; first steps for incidents; impersonation/account recovery; doxxing response; board/donor incident briefs).
- Legal support needs: practical, case-based guidance, decision trees, and example "case packs" (e.g. privacy complaints, spyware), including how GDPR-like standards may apply outside the EU.
- Wellbeing/readiness needs: harassment protection, self-care practices, signposting to health support, and proven techniques to build resilience.
- Preferred delivery formats: one-page checklists, copy-ready template packs, directories/contacts, short video walkthroughs/MOOCs, plus vendor discounts/shared seats and collaboration spaces (fact-checking, referrals, partner matching).
- Key blockers to sharing: limited capacity, uncertainty about what to share, data sensitivity/PII, language/region gaps, lack of a trusted network, and vendor license constraints.

WG3 : Threat Intelligence & Trends

WG3 explored what “threat intelligence” should mean for EDRN and what a shared dashboard/system would need to do to make it usable for civil society. Participants discussed expectations for threat intelligence, the most relevant threat actors and threats, current monitoring practices, priority outputs (org-specific vs community-wide trends), and preferred delivery formats (alerts vs reports), alongside conditions for sharing anonymised incident data.

Participants described a converging threat landscape where disinformation campaigns are frequently paired with harassment, impersonation, phishing, and infrastructure pressure, creating simultaneous strain on staff safety, systems, and reputation. Concrete examples included doxxing/smear campaigns against fact-checkers (especially in the context of platform policy changes), increasingly sophisticated phishing (including grant-themed lures and spoofed services), and recurring impersonation/cloned-website attacks where adversaries replicate branding on new domains to publish inflammatory content and then amplify it. Many CSOs rely on low-cost stacks, and noted gaps in baseline web/app security and chronic capacity constraints (often no dedicated security lead, or small teams split between “classic” cyber and information manipulation).

The needs that emerged were strongly pragmatic: early warning on narratives/campaigns (a “radar” for sudden mention spikes, likely coordination/inauthenticity, and escalation risk), plus focused, organisation-specific alerts for direct threats like new impersonating domains/accounts or suspicious use of a name/logo rather than complex portals. Participants also asked for clear, basic guidance for common tools (website management tools, cloud storage, SSL/admin hardening, lightweight OpSec), and support models that reflect limited internal capacity (outsourced/community-based security and shared tooling). On sharing and governance, there was openness to contributing anonymised incident data inside a trusted EDRN space, provided there is transparency on who has access, clear storage/access policies and security measures, and enough volume/diversity to reduce re-identification risk. The group saw value in combining community incident reports with carefully selected external feeds (public-sector, civil society networks, OSINT, and some private-sector intel), while excluding tools that require sensitive data sharing back to vendors or have problematic jurisdictional ties.

WG3 Takeaways

- Participants described a converging threat landscape: disinformation paired with harassment, impersonation, phishing, and infrastructure pressure hitting staff safety, systems, and reputation at once.
- Examples included doxxing/smear campaigns against fact-checkers, and more sophisticated phishing (e.g. grant-themed lures, spoofed services like DocuSign).
- Recurring impersonation/cloned-website attacks were highlighted: adversaries mirror branding on new domains, post inflammatory content, then amplify it as "look what they posted."
- Many CSOs operate on low-cost stacks with gaps in baseline web/app security and chronic capacity constraints.
- Strong preference for pragmatic outputs: early-warning "radar" for narrative spikes/coordination and escalation risk, plus simple org-specific alerts for direct threats (impersonating domains/accounts, logo/name misuse).
- Participants wanted clear, basic hardening guidance for common tools (website management tools, cloud storage, SSL/admin protection, lightweight OpSec).
- They asked for support models that match limited capacity (outsourced/community-based security and shared tooling).
- Willingness to share anonymised incidents in a trusted EDRN space if access is transparent, storage/access controls are clear, security measures are robust, and re-identification risk is minimised via sufficient volume/diversity.
- Value seen in combining community incident reports with selected external feeds (public sector, civil society networks, OSINT, some private intel), while avoiding tools that require sensitive data sharing to vendors or have problematic jurisdictional ties.

WG4 : Risk Assessment, Crisis Communications & Policy Uptake

WG4 centered on risk assessment, crisis communication, and policy/platform uptake, specifically, how EDRN members manage combined cyber and disinformation/FIMI risk and what would help them act effectively in the first 24–72 hours of an incident. WG4 examined confidence in first-day response, the most worrying incident types over the next year, how cyber and disinformation risks are managed today, whether organisations have crisis response plans and comms building blocks (spokesperson, templates, secure channels, approvals), how often they run drills, and where reporting pathways break down.

The core finding was partial readiness with weak institutionalisation. Participants reported that confidence in the first 24 hours is mixed, and their top near-term worries tend to be "hybrid" incident bundles coordinated disinformation alongside account takeovers, data leaks/doxxing, and staff harassment. While real incidents (notably phishing and impersonation) are being detected and handled quickly, participants described little structured follow-up, investigation, or internal learning afterward. Risk management is often informal and case-by-case, and several participants noted uncertainty about which reporting/escalation channels exist (platforms, regulators, trusted flaggers) and what actions are realistically available, especially as platform-policy context can intensify staff targeting and raise wellbeing needs alongside technical and comms demands.

WG4 converged on a set of practical, lightweight outputs that EDRN could build into the blueprint/dashboard: a simple "first 24 hours" checklist with role prompts for non-specialists; a combined cyber + disinformation crisis plan model; reusable crisis simulations/tabletops (optionally involving legal expertise and, where relevant, law enforcement perspectives); and short playbooks/templates for crisis communications fundamentals (templates, approvals, secure coordination basics). Participants also asked for more "made practical" reporting support - clear pathways and step-by-step guidance for engaging platforms, regulators, and trusted flaggers - plus proactive, context-aware warnings when upcoming events (e.g. elections) may raise risk. Finally, they saw value in safe community sharing of early signals and anonymised "incident stories" (even minor impersonation/phishing attempts) so organisations can spot patterns earlier and adapt before harm escalates, while acknowledging the main obstacles are capacity/time, limited leadership buy-in, rare drill practice, and the real-world difficulty of platform reporting.

WG4 Takeaways

- Participants reviewed: first-day response confidence, most worrying incident types for the next year, current risk management, crisis-plan "building blocks" (spokesperson, templates, secure channels, approvals), drill frequency, and where reporting pathways fail.
- Core finding: partial readiness but weak institutionalisation; confidence in the first 24 hours is mixed.
- Top near-term worries are "hybrid" bundles: coordinated disinformation plus account takeovers, data leaks/doxxing, and staff harassment.
- Phishing and impersonation incidents are often detected/handled quickly, but there's limited follow-up, investigation, or internal learning afterward.
- Risk management is frequently informal and case-by-case; many are unsure which escalation/reporting routes exist (platforms, regulators, trusted flaggers) or what actions are realistic.
- Platform-policy context can amplify targeting and increase wellbeing needs alongside technical and comms demands.
- Desired EDRN outputs: a simple "first 24 hours" checklist with role prompts for non-specialists, and a combined cyber + disinformation crisis plan model.
- Also requested: reusable crisis simulations/tabletops (optionally with legal and, where relevant, law-enforcement perspectives) and short comms playbooks/templates (templates, approvals, secure coordination basics).
- They want practical reporting support (clear pathways + step-by-step guidance for platforms/regulators/trusted flaggers) and proactive, context-aware warnings for high-risk events (e.g. elections).
- Value seen in safe community sharing of early signals and anonymised incident stories (even minor attempts) to spot patterns early; main obstacles are capacity/time, limited leadership buy-in, rare drills, and the difficulty of platform reporting.

EDRN Dashboard Module Review and Redesign Proposal

Having conducted all four working groups, we conducted a further review and redesign of the EDRN blueprint. The table below outlines revisions to the dashboard modules based on feedback from our four working group reports and the original structure. Modules are categorised under the three main dashboard sections: “Your Organisation”, “EDRN Trends”, and “Resources”. Each module includes a description and an assessment of complexity (Low, Medium, High).

‘Your Organisation’

Name	Description	Complexity
Overview	Snapshot view of incidents, score, alerts, and risk levels (from risk assessment).	Medium
Readiness & Roadmap	Self-assessment results, priority checklist, progress tracker.	Medium
Identity Watch	Real-time alerting for impersonation and misuse.	High
Social Mentions	Monitors organisation name and staff mentions across social media and alternative platforms.	High
New: Risk Profile & Triggers	Includes context-aware risk signals (e.g. upcoming elections), triggers for attention.	Medium
New: First 24h Checklist	A clear, printable and interactive checklist for immediate action post-incident tailored to each org, based on their resources and capabilities defined in the risk assessment.	Low

‘EDRN TRENDS’

Name	Description	Complexity
Cyber Threat Trends	Aggregated cyber threat landscape updates.	Medium
Phishing Campaigns Tracker	Aggregated phishing trends targeting CSOs.	Medium
Narrative Radar	Detects and displays dominant narratives targeting civic space.	High
Events radar	Timeline of elections, political events, and legal developments increasing risk.	Medium
Amplification Channels	Identifies key actors (domains, handles) driving harmful narratives.	Medium
New: Impersonation Trends	Tracks recurring impersonation techniques and attack formats.	Low
New: Incident Stories	Anonymous short logs of attacks submitted by organisations for shared learning.	Low

‘RESOURCES’

Name	Description	Complexity
Training & Guidance	PDF guides, short videos, templates on response, readiness, OpSec, digital hygiene.	Low
DSA Corner	Guidance on reporting under the DSA; checklists and escalation tips.	Medium
Researcher Wellbeing	Resources on burnout, vicarious trauma, self-care, mental health signposting.	Low
Resource Sharing Centre	Vetted legal, technical, comms contacts; access request form.	Medium
New: Crisis Communication Kit	Templates, spokesperson briefing forms, secure comms checklist.	Low
New: Simulation Toolkit	Reusable tabletop exercises and simulation guidelines for incident preparedness.	Medium
New: Reporting Hub	Clear guidance and up-to-date links for reporting to platforms, regulators, and flaggers (maybe integrating the DSA one into this module).	Medium

Summary of Changes

Added Modules (New):

- Risk Profile & Triggers
- First 24h Checklist
- Impersonation Trends
- Incident Stories
- Crisis Communication Kit
- Simulation Toolkit
- Reporting Hub.

Merged or Reframed:

- Social Mentions and Identity Watch kept as separate due to differing functions (brand monitoring vs impersonation).
- Readiness & Roadmap implicitly incorporates organisational score and checklist.

Potential for Deletion:

- Events Radar may be merged with Risk Profile & Triggers if redundant.

January Presentation

During the final meeting on 29 January 2026, partners reviewed the overall progress of the EDRN pilot, confirming that the initiative successfully helped surface key challenges faced by civil society organisations in the democracy resilience space - particularly the growing convergence of cyber and information manipulation threats. The discussion highlighted how the four working groups helped identify persistent gaps in monitoring, escalation pathways, and preparedness, and directly informed the evolution of the EDRN blueprint. The updated dashboard concept was presented as a community-driven tool, structured around three pillars (organisation-specific view, aggregated EDRN trends, and shared resources), with new modules including risk scoring, incident-sharing, impersonation trend monitoring, and a concise “first 24 hours” response checklist for CSOs facing an incident. Participants also discussed next steps for sustainability and fundraising opportunities, including exploring multiple funding avenues, prioritising high-impact & low-cost features, and maintaining momentum by building on the success of the initiative.

Next Steps: Defending Civil Society in a Hostile Era

The EDRN project has led to three essential conclusions that must guide its future development. First, the current geopolitical environment is increasingly hostile to civil society organisations working on politically sensitive or contested issues. Regardless of where these organisations stand ideologically, no democratic society should tolerate attacks such as doxing, impersonation, false claims, hate speech, digital surveillance, or cyber sabotage as legitimate forms of dissent. These tactics aim not to debate but to disable. In this context, equipping CSOs with defensive capabilities is not merely optional; it is a democratic imperative. As generative AI continues to lower the barrier for such attacks, the urgency to act is only increasing.

Second, despite a growing civil society ecosystem, funding in the democratic resilience space is scarcer than ever, leading to fragmentation, duplication, and competition between actors. EDRN has demonstrated that defensive capacity-building creates a unique environment where collaboration is actively sought after. The shared experience of being targeted has allowed organisations to lower their guard, share openly, and co-design tools across divides that would have otherwise kept them apart. In this way, EDRN is a proof of concept for funders seeking to foster cooperation, reduce duplication, and build stronger, more connected civic ecosystems.

Third, EDRN is not starting from scratch. It directly complements the CyberPeace Institute's existing CyberPeace Builders program, which currently supports over 600 CSOs globally on cybersecurity. By developing modular tools focused on information manipulation and hybrid threats, EDRN can immediately scale impact across this existing network, reaching frontline organisations without delay, and without needing to rebuild a new ecosystem.

For these reasons, the EDRN initiative must now be elevated as a strategic priority. It is one of the few projects that not only protects civil society, but also brings it together. In an era of growing threats and shrinking resources, this kind of shared infrastructure is not only helpful; it's essential.

European Democracy Resilience Network

January 2026

Final Report