European Democracy Resilience Network

Kick-Off Workshop Summary Report

15 September 2025

Overview

On 15 September 2025, the CyberPeace Institute (CPI) and EU DisinfoLab (EUDL) hosted a kick-off meeting of the European Democracy Resilience Network (EDRN). This initiative, running from August 2025 to January 2026, is designed to strengthen democratic resilience in Europe by supporting civil society organisations (CSOs).

EDRN responds to the growing nexus of threats (cyberattacks and information manipulation) facing CSOs by working with them to co-develop a blueprint for integrated support. The blueprint will combine approaches to disinformation resilience, complemented by cybersecurity insights from the CyberPeace Builders programme.

Initial outreach drew strong interest, with more than 30 organisations attending the kick-off to share their experience and expertise. Eligible participants were briefed on how to access the CyberPeace Builders programme which provides immediate cybersecurity assistance to eligible organisations.

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. During the meeting, they were also shown a mock-up dashboard; while not yet functional, it served as a visual starting point for how EDRN could integrate monitoring, reporting, and resilience features in one place.

This report summarises the survey findings and kick-off discussions that will inform the EDRN blueprint. A presentation of the draft blueprint is planned for January 2026.

In this report

- **Survey results:** disinformation exposure, monitoring practices, cybersecurity readiness, and incident-response capacity.
- **Breakout discussions:** qualitative insights on threats, resource gaps, and priority tools.
- **Next steps & timeline:** checkpoints toward a **January 2026** presentation of the draft EDRN blueprint
- **Working groups:** focus areas shaping the blueprint - social media monitoring & weak signals; shared resources & support; threat intelligence & trends; risk assessment & crisis comms.

Challenges identified by participants:

- Frequent exposure to disinformation campaigns
- Inconsistent monitoring and incident tracking
- Gaps in both technical protection and organisational preparedness

These insights highlight urgent demand for practical tools, shared resources, and training, and they form the foundation of EDRN's blueprint so that proposed support reflects the real needs of participating organisations.

Survey Results

A pre-meeting survey of **29 organisations** (90% nonprofits) shows frequent disinformation exposure, uneven cybersecurity preparedness, and gaps in incident tracking and response. These insights define the project baseline and where EDRN support will add most value. *(Percentages throughout these results are rounded; n=29)*

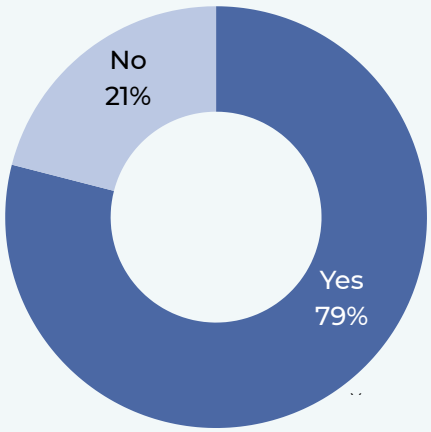
The survey reveals consistent patterns in the challenges faced by CSOs engaged in democratic resilience. Awareness of threats such as disinformation and cyberattacks is high, but many organisations lack the formal systems, resources, and capacity to monitor, track, and respond effectively. Recurrent gaps in operational security, incident preparedness, and coordinated response point to the need for practical tools, shared resources, and training. These conclusions shape where EDRN could add the most value.

Disinformation

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

- **52%** report coordinated online attacks such as troll campaigns, fake accounts, or data exposure.
- **28%** frequently - or almost constantly - encounter false or misleading online narratives mentioning their organisation or staff; and **31%** experience them occasionally.
- Incidents often involve **false claims about staff, affiliations, or funding**.
- Some responses refer to **media outlets** being used to legitimise disinformation or misrepresent leaked private materials.
- While the level of detail varies, several organisations describe **hybrid threats**, where disinformation is reinforced by cyber intrusions or surveillance.

Has your organisation ever been the target of disinformation (false or misleading claims about your work, staff or funding)?



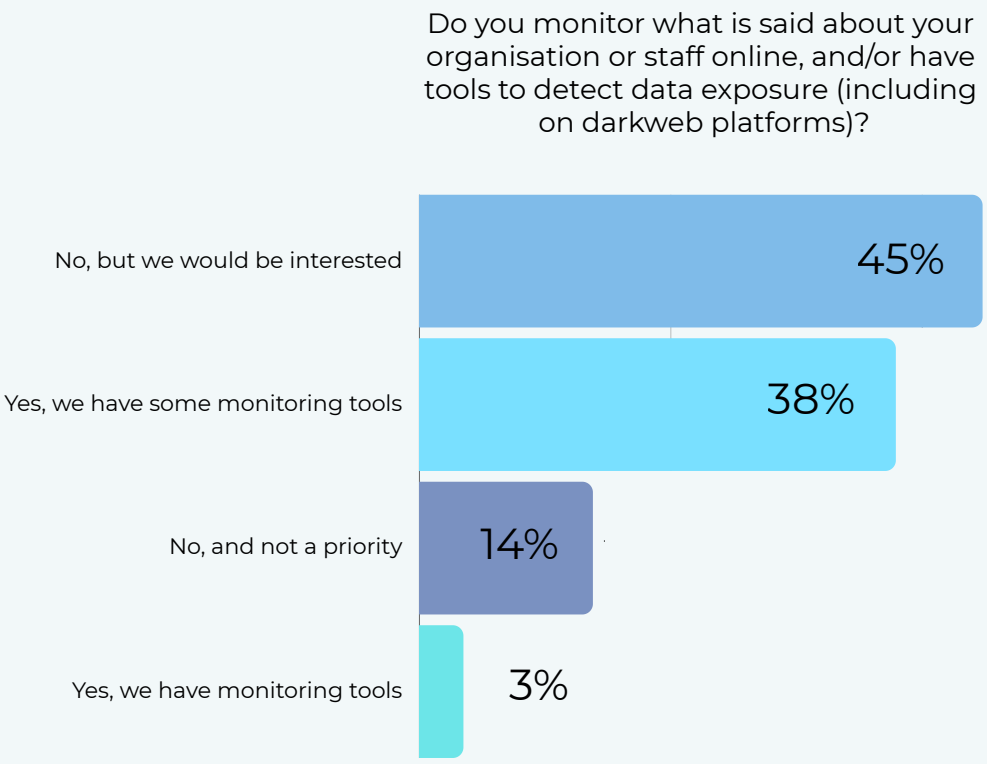
Incident Tracking

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

A few organisations use basic monitoring tools, while others explicitly state they lack capacity or resources for systematic reporting. This highlights 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 is inconsistent across participating CSOs. While some organisations actively track social media and news coverage, most respondents either lack systematic monitoring or do so only informally. Nearly half **(45%)** say they would like to have monitoring tools but do not currently use them.



Policy & Organisational Preparedness

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

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

Together, these results reveal a clear internal policy gap **-** while awareness of threats is widespread, the translation into organisational procedures is inconsistent. Addressing this gap will be critical for EDRN's blueprint, particularly through the development of response templates, simulation exercises, and shared best practices.

Baseline Protection & Technical Readiness

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

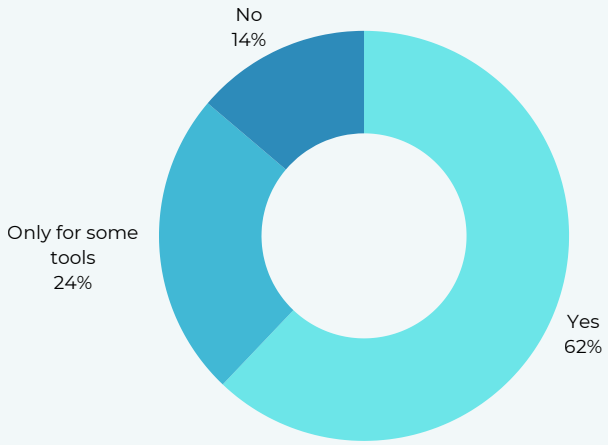
Vulnerability scans and audits

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

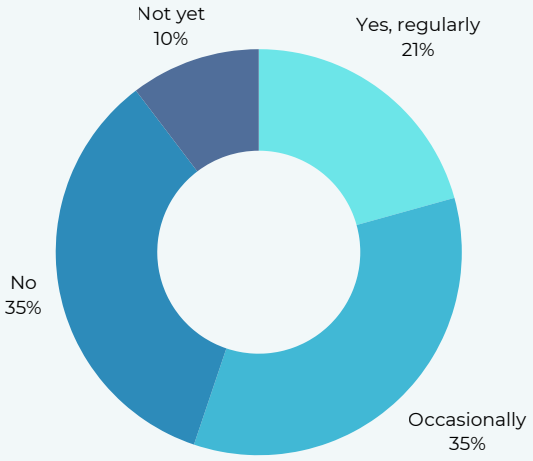
Device and server protection: When asked to rate the protection of their devices and servers (e.g., antivirus, firewalls, malware detection) on a scale of 1–5, responses were spread across the spectrum: **10%** scored 1, **17%** scored 2, **21**% scored 3, **24%** scored 4, and **28%** scored 5. This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

Multi-factor authentication (MFA): Just under two thirds **(62%)** report using MFA across key platforms, while **24%** apply it only to some tools, and **14%** do 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 shows 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%** have not yet begun training efforts.

Challenges

Organisations highlight a wide range of challenges in their open-text survey responses, including:

- Escalating threats in authoritarian or unstable environments.
- Capacity gaps in technical security and legal protection.
- Difficulties in distinguishing between organic criticism and coordinated disinformation.
- Pressure from hostile media or state actors

Breakout Room Discussions

Participants engaged in breakout group discussions to explore specific threats and resilience needs in greater depth. These conversations aimed to expose the types of disinformation and cyberattacks organisations encounter, the tools and resources they most require, and the forms of monitoring and alerts that would be most useful. The discussions also underscored the importance of community-wide situational awareness and shared strategies for responding to hostile narratives and attacks. The following section summarises the main themes and priorities that emerged.

1. What kinds of disinformation or cyber threats affect organisations like yours?

Across all breakout rooms, organisations described a broad spectrum of digital threats. These range from coordinated disinformation campaigns and smear efforts to phishing, hacking, impersonation, and infrastructure compromise (e.g., website breaches, blocked accounts). Several organisations emphasised hybrid threats, where disinformation narratives are reinforced or enabled by cyber intrusions. Threats were often linked to politically sensitive topics such as elections, transparency, or investigative journalism. A number of organisations reported intimidation tactics, such as personal threats, trolling, or government-driven harassment. Notably, both individual and organisational attacks were common, highlighting the need for personal-level protections alongside institutional security.

2. What information or tools would be most useful to see in one place?

Participants consistently expressed interest in tools that provide narrative tracking, monitoring of mentions (including in fringe/dark web spaces), and alerts tied to evolving threats. There was also support for multi-language processing and manual input functionality, to complement automation. A recurring theme was the need for a system that offers structured insights, early warnings, and a way to monitor both internal and community-wide risk trends. Several organisations wished to be able to share and access legal, technical, and informational resources in a centralised manner, including examples of previous incidents and responses.

3. Which kinds of risks or attacks do you most want help spotting?

The top priorities include identifying coordinated disinformation campaigns, bot-driven amplification, narrative manipulation, and early indicators of influence operations. Many also flagged the need to detect phishing attempts, account takeovers, leaks/doxxing, and surveillance (including spyware or passive social media monitoring). Some respondents expressed concern about state-affiliated actors, especially in environments with weakened press freedom. A number of CSOs explicitly asked for help connecting weak signals across seemingly unrelated threats.

4. What kind of alerts or updates would be useful for your organisation?

Participants valued both organisation-specific alerts (e.g. sudden spike in mentions, reputation attacks) and broader situational awareness (e.g. coordinated narrative shifts, targeting of peer organisations). Many expressed that systemic alerts, based on shared vulnerabilities or observable disinformation trends, could help them act before escalation. Alerts tailored to specific roles (e.g., communications vs. IT) were also mentioned. There was also interest in receiving alerts/information across multiple languages. There is strong interest in a simple, intuitive alert format that doesn't overwhelm but still offers depth when needed.

5. Would you find more value in seeing your own organisation's data, community-wide trends, or both?

There was near-universal agreement that both levels are essential. While understanding their own exposure is critical for risk management, participants noted that tracking community-wide patterns enhances strategic situational awareness, supports collective learning, and reduces blind spots. Many see value in identifying if they're being targeted in isolation or as part of a coordinated attack wave. Community visibility was also framed as a solidarity-building and trust-strengthening mechanism.

6. What should the dashboard do for you?

The dashboard is expected to act as both a threat detection system and a response support hub. Key functions mentioned include: real-time monitoring, flagging of suspicious narratives, attack documentation, and data collection for legal/policy purposes. Several participants emphasised it should also facilitate comms during crisis moments and serve as a shared system for lessons learned across incidents. Clarity, usability, and flexibility were repeated design priorities.

7. If you had this dashboard today, what would you hope it tells you at a glance?

- **Who is targeting us**
- **What are they saying**
- **How severe is the current threat**

Organisations also want to know whether a narrative is gaining traction, whether similar organisations are being targeted, and how the attack may escalate or evolve. Simplicity was emphasised: a dashboard should provide a clear summary while allowing users to explore more granular data if needed.

8. How would this dashboard make your work easier or safer?

The main benefit cited is proactive risk reduction. Automating monitoring would free up staff time while enabling quicker, more confident decision-making. Several mentioned that real-time signals would allow for more strategic communication responses, documentation for rebuttals or legal recourse, and overall reduced exposure to harm. Others saw it as a way to build institutional memory, improve internal training, and ultimately scale their resilience capacity.

9. If we could only add one feature at launch, which would you choose?

The most popular response was a "narrative radar" – a visual tracker showing how disinformation narratives are evolving across the ecosystem and whether a specific organisation is being referenced or implicated. This was followed by the ability to track mentions and threats in fringe and mainstream platforms, as well as an alert system for early warning. Participants also called for a central repository of attack data and responses as a foundational feature.

Implications

The survey findings and breakout discussions indicate that civil society organisations working within the democratic resilience sphere face high exposure to digital threats but uneven access to structured protection mechanisms. The following recommendations outline where EDRN is uniquely positioned to create value.

1. Establish a core resilience baseline across participating organisations
Although most organisations are aware of the risks they face, only around half report having internal safeguards such as sensitive information policies or staff guidelines. Rather than introducing complex systems, the most immediate impact will come from standardising minimum viable protection measures, such as shared policy templates, incident reporting formats, and starter security protocols that can be rapidly adopted regardless of organisational capacity.

2. Provide collective threat visibility rather than isolated intelligence
Nearly 80% of organisations have been targeted by disinformation or reputational manipulation, yet only a small amount have monitoring tools. The ability to detect escalation patterns or determine whether an attack is isolated or coordinated is currently limited. EDRN should focus on building a shared threat awareness layer, offering narrative tracking, pooled observation of fringe and mainstream channels, and structured early-warning signals that help organisations to act before harm escalates.

3. Treat resilience as a shared infrastructure
Both survey data and group discussions show that CSOs do not simply need tools - they need validation, comparators, and coordinated response mechanisms. Participants consistently emphasised that confidence increases when they see how others respond to similar incidents, or when communication lines are open during moments of pressure. EDRN should therefore function not only as a service provider, but as a facilitator of collective defence, by enabling real-time coordination channels, shared case repositories, and peer-based escalation pathways.

In summary, the findings confirm that resilience is currently distributed unevenly across organisations. EDRN's value lies in making practical resilience accessible to every actor in the network.

Next Steps

The next steps of the EDRN project consist of the following:

- (Optional) The initiative will move forward with the onboarding of nonprofit participants into the CyberPeace Builders (CPB) network
- Launch of a dedicated Mattermost channel to support ongoing collaboration
- Scheduling of monthly checkpoints that will provide opportunities for smaller group engagement around blueprint components (see Working Groups)
- (Optional) Attending the EUDL Conference in October 2025 in Ljubljana, Slovenia - and participating in an in-person EDRN lunch lecture
- Distribution of a concise summary from the EDRN lunch lecture, including a top-line practical guide to mitigating influence operations and common cyber threats (e.g., quick checks, response steps, and resource links)
- Building on both the survey insights, breakout sessions, and the mock-up dashboard demonstrated during the kick-off, the project team will use the monthly checkpoints to gather additional input and refine these concepts into a dashboard blueprint for presentation in January 2026
- Efforts to secure funding for a minimum viable product (MVP)

Working Groups

Drawing on both survey findings and breakout discussions, four thematic working groups are proposed to guide the blueprint development. Organisations do not have to participate in every working group, but are encouraged to pick two or three groups that interest them the most.

WG1: Social Media monitoring & weak signals

- Fully validated by strong demand for narrative tracking and coordinated disinfo detection
- Could also include language-specific monitoring challenges.
- *Taking place October 2025*

WG2: Shared resources & access to support

- Matches requests for legal, technical, and cybersecurity aid pooling
- Could also cover administrative support like insurance, better resource management via shared software access, and playbooks etc
- Taking place November 2025

WG3: Threat Intelligence & trends

- Aligns with the need to map coordinated campaigns, track actor TTPs, and analyse ecosystem-wide shifts
- Could benefit from close collaboration with the private sector
- *Taking place November 2025*

WG4: Risk Assessment & crisis comms

- Strong alignment with needs for incident response templates, post-breach comms, and preparedness training
- May also cover incident simulation exercises and strategic narrative rebuttal
- *Taking place December 2025*

European Democracy Resilience Network

15 September 2025

Kick-Off Workshop Summary Report