

DIGITAL SECURITY LAB ANNUAL REPORT

Supporting journalists, activists and human rights
defenders against digital security threats — and
advancing human rights online.



Digital Security Lab Ukraine

2025

GENERAL INFORMATION

Digital Security Lab Ukraine is a Ukrainian civil society organization founded in September 2017. It supports journalists, civil society activists and human rights defenders in addressing digital security challenges, and advances the protection of human rights online by influencing public policy in the field of digital rights.

OUR MISSION

PROMOTE THE REALISATION OF HUMAN RIGHTS ONLINE — BY STRENGTHENING CIVIL SOCIETY AND INDEPENDENT MEDIA TO RESPOND TO DIGITAL SECURITY CHALLENGES, AND BY SHAPING STATE AND CORPORATE POLICY ON DIGITAL RIGHTS.

VALUES OF THE DIGITAL SECURITY LAB

SUPPORT — the primary goal of the organisation is to assist civil society.

TEAM — the organisation cares about the well-being of its employees and consultants.

AUTONOMY — the team is capable of self-organization and can operate without supervision.

RESPONSIBILITY — it takes full responsibility for its work and actions.

INDEPENDENCE — it determines its own areas of work and is not affiliated with any political force.

PROFESSIONALISM — the team continuously develops its expertise and holds to high standards of work.

ETHICS — it ensures the confidentiality of its clients and adheres to ethical principles.

SCOPE OF WORK

DIGITAL SECURITY FOR CIVIL SOCIETY

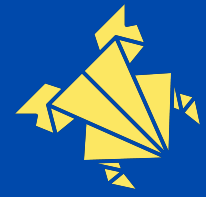
- Security audits and assessments
- Assistance with implementing security processes in CSOs (operational security advisory)
- Technical support and security consultations
- Awareness raising on digital threats
- Threat intelligence and threat detection
- Incident response

DIGITAL RIGHTS

- Analysis of legislative initiatives affecting human rights online
- Research and analysis of international human rights and internet practice
- Recommendations and proposals for legislative change on digital rights, nationally and internationally

PROGRAMME 01

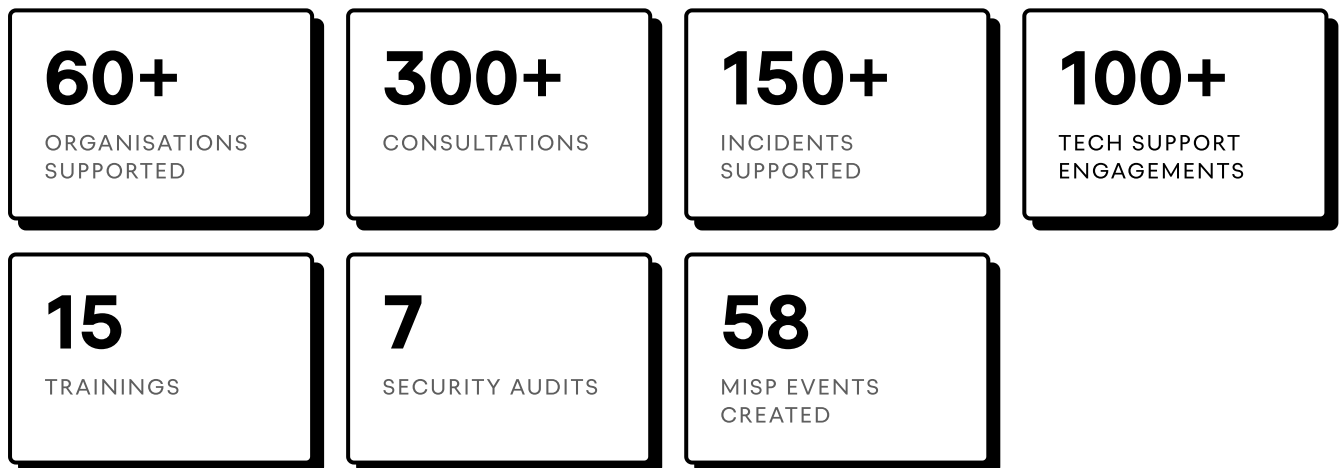
DIGITAL SECURITY



CONTEXT

2025 was a demanding year for the digital security of Ukrainian civil society, as it remained under sustained pressure from Russia-linked state actors, pro-Russian hackers and financially motivated criminal groups. Phishing and spear-phishing dominated the threat landscape, with attackers steadily improving their tradecraft, impersonating trusted services and institutions, and abusing legitimate cloud infrastructure to evade detection.

THE YEAR IN FIGURES



7 DIGITAL SECURITY AUDITS

Each audit combined a technical assessment of the organisation's digital environment, an inventory of digital assets, and a risk assessment tailored to the organisation's work. Based on the findings, each organisation received a prioritised set of practical recommendations to address identified weaknesses, improve the security of devices and accounts, and strengthen its overall digital resilience.

316 CONSULTATIONS

Consultation requests covered both individual and organisational digital security needs. The most common involved checking suspicious emails, messages, files and login notifications and possible signs of account or device compromise; restoring access to hacked, suspended or inaccessible accounts; running security checkups of devices, accounts and messengers; and strengthening account protection through two-factor authentication, security keys, password management, session reviews, backups, encryption, VPNs and secure data transfer. Journalists and activists also sought support with phishing, spyware concerns, device seizure, anonymous communication, secure work with sensitive sources and files, and onboarding to new devices. At the organisational level, consultations focused on Google Workspace and Microsoft 365 configuration, access management, onboarding and offboarding, corporate email protection, website and domain security, network and NAS infrastructure, cloud storage, licensed software, incident response procedures, security policies, asset inventories, risk assessment and longer-term cybersecurity planning.

15 TRAININGS

Digital security trainings were designed to give participants practical skills they could apply immediately in their daily work. Depending on the audience, sessions covered account, device and messenger security, common attack techniques, phishing and organisational security practices. Programmes were adapted to the needs of each organisation and complemented by onboarding sessions for new staff and longer-term capacity-building initiatives.

114 TECHNICAL SUPPORT ENGAGEMENTS

Technical support helped journalists and civil society organisations securely deploy and maintain their digital infrastructure. Assistance included secure device configuration, operating system hardening, implementation of organisational email, network and cloud services, infrastructure upgrades, data migration, malware checks, recovery after technical failures, and deployment of additional security measures to strengthen the resilience of organisational systems.

157 INCIDENTS

Security incidents were dominated by phishing and spear-phishing targeting journalists, media, civil society organisations and their administrative or financial staff. Attackers frequently impersonated Meta, Google, banks, delivery services, document-management platforms and trusted organisations, using legitimate cloud services, compromised accounts, fake CAPTCHAs and spoofed domains to evade detection. Some campaigns aimed to steal account credentials; others delivered remote-access tools, information stealers, cryptominers or other malware. During the year, DSLU created 58 CiviCERT MISP events, and sent 33 incident alerts to its closed newsletter.

INCIDENTS BY TYPE

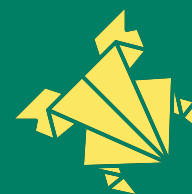
INCIDENT TYPE	CASES
Phishing URL	71
EDR / IDS / IPS alert	35
Phishing with malicious attachment	28
Account hacking	14
Threat hunting	7
PsyOps and disinformation	4
Website hacking	2
Social media account restrictions	1
DDoS	1
TOTAL	157

INCIDENT REPORTS

- PHANTOMCAPTCHA — MULTI-STAGE WEBSOCKET RAT · WITH SENTINELLABS** — A single-day spear-phishing operation targeting Ukraine, investigated jointly with SentinelLABS. [Read here](#)
- FACEBOOK ACCOUNTS — META BUSINESS SUITE ABUSE** — Attackers abuse Business Suite invites, using a phishing site and a fake page as two vectors. [Read here](#)
- FAKE META POLICY VIOLATION NOTICES** — Emails posing as Meta, alleging rules or IP violations and threatening to block the account. [Read here](#)
- UKRPOSHTA SMS PHISHING** — SMS impersonating the national logistics operator to harvest card and personal data. [Read here](#)
- TAX SERVICE MALWARE CAMPAIGN** — A mass campaign posing as Ukraine’s Tax Service, spreading malware via PDF attachments. [Read here](#)

PROGRAMME 02

DIGITAL RIGHTS



DIGITAL RIGHTS AND EU INTEGRATION

In 2025, DSLU continued its systematic work to assess Ukraine's compliance with international human rights obligations in the digital sphere. The team developed the ["Criteria for Assessing the State of Human Rights Compliance in the Digital Environment"](#) — a tool for structured analysis of how Ukraine fulfils its international commitments under conditions of digital transformation, EU integration and ongoing armed conflict.

On 15 April 2025, DSLU presented its annual report ["Human Rights in the Digital Dimension. 2024"](#), assessing Ukraine's fulfilment of international digital rights obligations in the context of full-scale war and EU accession. The report provides a comprehensive overview of legislative developments, human rights risks and policy recommendations across key digital rights domains.



DSLUXPerts in Policy Dialogue on Digital Rights and EU Integration

DSLUXperts also participated in governmental working groups on Ukraine's EU accession process under Chapters 23 and 10. As part of this, DSLUXperts submitted [proposals](#) to Ukraine's negotiation positions under Chapter 10 and prepared submissions to the EU Delegation to Ukraine for the 2025 Enlargement Report.

As Ukraine's accession process advances, institutional capacity in digital services, media, personal data protection and AI has become increasingly important. In its 2024 Enlargement Report, the European Commission highlighted the need for independent, well-resourced regulators and further alignment with EU rules such as the Digital Services Act. In response, DSLU experts began a comparative [study of regulatory models](#) in EU and EEA countries, examining their institutional design, independence safeguards, mandates and coordination mechanisms.

DSLU regularly published reviews of European Court of Human Rights (ECtHR) judgments relevant to digital rights, covering decisions on freedom of expression, privacy and surveillance: [Denysyuk and Others v. Ukraine](#), [Borzykh v. Ukraine](#), [Novaya Gazeta and Others v. Russia](#), and [Google LLC and Others v. Russia](#). These reviews contribute to public awareness of international human rights standards and their application in the digital context.

ARTIFICIAL INTELLIGENCE

In 2025, DSLU continued to deepen its engagement in national and international AI governance processes, providing expert input across regulatory, advisory and advocacy dimensions.

At the national level, DSLU submitted detailed comments and proposals to the draft [National AI Strategy of Ukraine](#), defining priorities and needs for the future regulatory and policy framework. DSLU experts also prepared and [presented](#) a [mapping of Ukraine's obligations under the EU AI Act](#), supporting the gradual and efficient harmonisation of domestic legislation with EU standards.

DSLU was also engaged in preparing sectoral recommendations on AI for specific sectors and professional communities — including [guidance for AI developers](#) and on the [safe use of AI in legal work](#) — helping operationalise responsible AI practices beyond the general regulatory framework.

Internationally, within the Council of Europe's Committee on Artificial Intelligence (CAI), DSLU contributed to drafting the Framework Convention on AI and submitted comments and proposals on the draft "HUDERIA Model", contributing to its further development and pilot testing. DSLU's input focused on refining human rights impact assessment approaches and strengthening the coherence and operational clarity of the HUDERIA resources.

PERSONAL DATA PROTECTION

In 2025, DSLU contributed to capacity-building in personal data protection. DSLU expert Tetiana Avdieieva [participated in the development of](#) a comprehensive educational course for Data Protection Officers (DPOs), [launched](#) on the Diia.Education platform — Ukraine's national online learning infrastructure. The course equips practitioners with the knowledge and skills to ensure compliance with data protection standards in both the public and private sectors. This reflects DSLU's commitment to building institutional capacity alongside its legislative and advocacy work, recognising that effective data protection reform requires not only sound legal frameworks but also trained professionals to implement them.

DIGITAL SERVICES

In 2025, DSLU continued to support Ukraine's alignment with the EU's Digital Services Act (DSA). DSLU expert Maksym Dvorovyi analysed draft national legislation implementing the DSA and formally submitted expert comments and proposals to the Ministry of Digital Transformation of Ukraine.

DSLU contributed to the work of the DSA Human Rights Alliance, participating in developing the ["Principles for a Human Rights-Centred Application of the DSA: A Global Perspective"](#). During the DSA Civil Society Roundtable in November 2025, a DSLU expert took part in a workshop organised by CDT Europe on modalities for implementing the DSA in the EU, contributing to planning the finalisation of the Principles and a roadmap for their presentation in 2026.

MEDIA FREEDOM

MONITORING AND LEGAL ANALYSIS

Throughout 2025, DSLU maintained systematic monitoring and analysis of Ukraine's media law and digital rights landscape through a series of monthly legal digests. Twelve "Media and Digital Rights Regulation in Ukraine" digests ([January](#), [February](#), [March](#), [April](#), [May](#), [June](#), [July](#), [August](#), [September](#), [October](#), [November](#), [December](#)) were prepared. The digests systematically covered key legislative and policy developments in the areas of media regulation, digital rights, digital services and artificial intelligence in Ukraine.

LEGISLATIVE AND CO-REGULATORY ENGAGEMENT

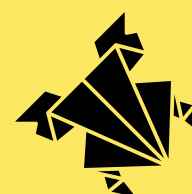
DSLU contributed to the development of draft legislation countering Strategic Lawsuits Against Public Participation (SLAPPs) within the [working group established by the Committee on Freedom of Speech of the Verkhovna Rada of Ukraine](#). DSLU [ensured](#) that

provisions of the draft laws align with Council of Europe recommendations and the EU Anti-SLAPP Directive, reinforcing safeguards for journalists, human rights defenders and civil society activists against abusive litigation.

DSLUI maintained sustained expert engagement in Ukraine's media co-regulatory processes, operating within the framework established by the Law of Ukraine "On Media". DSLUI experts took part in thematic working groups covering audiovisual and online media, contributing to the development of sectoral co-regulatory codes and criteria in areas including child protection, national security interests and online media regulation.

ACROSS ALL PROGRAMMES

COMMUNITY EVENTS



GLOBAL GATHERING

To support stronger international visibility of Ukraine's reform challenges and priorities in the digital and media policy sphere, DSLUI contributed to international policy dialogue on EU integration reforms, AI regulation and media freedoms by [organising and participating](#) in thematic sessions at Global Gathering 2025. DSLUI experts co-organised the thematic track "Digital Crossroads: EU Rules, Regional Realities", dedicated to the impact of EU digital regulation on Eastern Europe and neighbouring regions. Within this track, DSLUI experts moderated and participated in multiple discussions addressing AI and journalism, SLAPP litigation and the global effects of EU tech regulation, including the DSA.

RIGHTSCON

DSLUI experts also contributed to RightsCon 2025 by hosting and participating in thematic discussions on wartime censorship and human rights restrictions in crisis contexts. Particular attention was paid to the need for narrowly tailored, context-sensitive approaches that address security needs without undermining fundamental rights, as well as to the broader challenge of moving from fragmented responses to more coordinated and systemic solutions.

COPENHAGEN CONFERENCE ON INFORMATION INTEGRITY

DSLU [participated in the Copenhagen Conference on Information Integrity](#), an international platform for discussion on strengthening information integrity and democratic resilience, as well as the [NAM Summit](#), focused on the future of media in the context of war, artificial intelligence, digital overload and rapid transformation. Through these engagements, DSLU contributed regional expertise and rights-based perspectives to international policy discussions on digital resilience and information integrity.

DONBAS MEDIA FORUM

On 10 October 2025, DSLU participated in Donbas Media Forum 2025. The Digital Security Team conducted consultations as part of the Safety Corner, organising an interactive digital security clinic where participants received practical advice on personal data protection, information security and current cyber threats. Throughout the session, attendees were able to discuss their security concerns directly with experts and receive tailored recommendations.

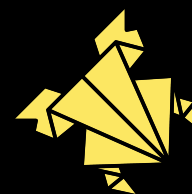


DSLU AT DONBAS MEDIA FORUM 2025 — THE SAFETY CORNER DIGITAL SECURITY CLINIC

At the same forum, DSLU experts joined the panel discussion [“Third World War or First Information War: Experience and Solutions”](#), on how Ukrainian media, the state, civil society and academia are responding to hybrid information warfare. They also contributed to [“Two Years with AI: What Practical Experience in Newsrooms Has Shown”](#), addressing how artificial intelligence is transforming editorial work — from news automation to ethical and legal dilemmas.

FINANCIAL STATEMENT

FINANCIAL REPORT



SOURCES OF FINANCIAL SUPPORT

DSLU's work in 2025 was made possible by the following partners and donors.



ARTICLE 19



THE INTERNATIONAL RENAISSANCE FOUNDATION



ZMINA HUMAN RIGHTS CENTER



DALAN FUND



INTERNATIONAL MEDIA SUPPORT (IMS)



ACCESS NOW



FRONTLINE DEFENDERS



UNESCO



FROM THE PEOPLE OF JAPAN

SUPPORT LOST DUE TO THE USAID CLOSURE

4 projects with 2 partners were discontinued during the year, requiring us to reprioritise activities and sustain core work with a reduced budget.

Media Diversity Institute

1 PROJECT

Internews Network

3 PROJECTS

EXPENSES IN 2025

TOTAL EXPENDITURE

19 505 772,40

≈ USD 460 000

UAH

EXPENSE CATEGORY	UAH	SHARE
Staff salaries	16 943 186,95	86,9%
Consultant fees	905 501,00	4,6%
Procurement, maintenance and upgrade of equipment	622 237,00	3,2%
Office rent	611 000,00	3,1%
International conferences and training	305 475,00	1,6%
Banking expenses	48 372,45	0,2%
External audit	40 000,00	0,2%
Administrative expenses	30 000,00	0,2%
TOTAL	19 505 772,40	100%

All figures in Ukrainian hryvnia (UAH).