BCSP Belgrade Centre for Security Policy

RESEARCH REPORT / 11

UNDER PRESSURE

DIGITAL SECURITY OF CIVIL SOCIETY IN THE WESTERN BALKANS AND THE EUROPEAN UNION

Anđela Savić

May 2026

RESEARCH REPORT / 11

UNDER PRESSURE

DIGITAL SECURITY OF CIVIL SOCIETY IN THE WESTERN BALKANS AND THE EUROPEAN UNION

Anđela Savić

BCSP Belgrade Centre for Security Policy

May 2026

Summary

Civil society organisations, journalists, and human rights defenders across the Western Balkans and European Union (EU) are operating in a digital environment defined by raising threats and inadequate protection. This analysis presents findings from a needs assessment survey conducted within the "Defending Digital Freedoms: Strengthening Civil Society Resilience against Digital Repression in Europe" project, gathering 239 responses from 11 countries (six Western Balkan and five EU member states).

The findings reveal a threat landscape shaped by surveillance, phishing, platform-based harassment, and account compromise, with confirmed and suspected spyware deployments in Serbia, Poland, Hungary, Italy, Greece, and Spain. Digital repression intensifies predictably during elections, protests, and publishing of investigative stories, yet most organisations lack the capacity to respond effectively. While foundational security measures are increasingly common, advanced practices and organisational protocols remain rare. Access to digital forensic support is limited and largely unknown to those who need it most.

Beyond the technical gaps, system is largely failing; legal remedies are widely perceived as weak or non-existent, institutional responses are slow and inconsistent, and organisational cooperation is underdeveloped. The most urgent needs are digital security training, affordable forensic services, trusted expert access, and dedicated funding, needs that cut across both regions, but are particularly acute in the Western Balkans.

The analysis provides cross-country evidence base for coordinated action by civil society networks, donors, national institutions, and digital platforms committed to protecting civic space in an increasingly hostile digital environment.

Table of Contents

Introduction

According to the latest Freedom House's report "Freedom in the World 2026: The Growing Shadow of Autocracy", both democratic countries and dictatorships turned to tactics such as surveillance, censorship, media regulation, and political prosecution in order to increase pressure on their citizens.[1] Moreover, in the last two decades, as noted in the report, digital surveillance increasingly affects personal expression[2] thus contributing to restriction of fundamental freedoms. Additionally, civil society organisations, human rights defenders, and independent journalists across Europe operate in an increasingly hostile digital environment, marked by deployment of sophisticated tools such as spyware in the European Union[3] as well as in the Western Balkan countries such as Serbia.[4]

Given that the civil society is operating in an increasingly hostile digital environment, it was necessary to gather evidence on their concrete needs, capacities, and protection gaps. By mapping experiences across Western Balkan and selected EU member states, Belgrade Centre for Security Policy aimed to identify the most urgent risks, needs, and opportunities for coordinated cross boarder response.

The analysis presents the findings of a needs assessment questionnaire conducted within the "Defending Digital Freedoms: Strengthening Civil Society Resilience against Digital Repression in Europe" project supported by the Stiftung Mercator[5] and led by the Belgrade Centre for Security Policy. Project partners formed the Civil Society Digital Security Network (CSDSN), a consortium of eleven civil society organisations spanning six Western Balkan countries and five European Union member states. The eleven CSDSN member organisations are: Belgrade Centre for Security Policy[6] (Serbia), Why Not[7] (Bosnia and Herzegovina), Centre for Civic Education[8] (Montenegro), Kosovar Centre for Security Studies[9] (Kosovo), Institute for Democracy 'Societas Civilis'[10] (North Macedonia), Centre for the Study of Democracy and Governance[11] (Albania), Hungarian Helsinki Committee[12] (Hungary), Amnesty International Greek Section[13] (Greece), Amnesty International Italian Section[14] (Italy), Amnesty International Spanish Section[15] (Spain), and the Institute of Public Affairs[16] (Poland).

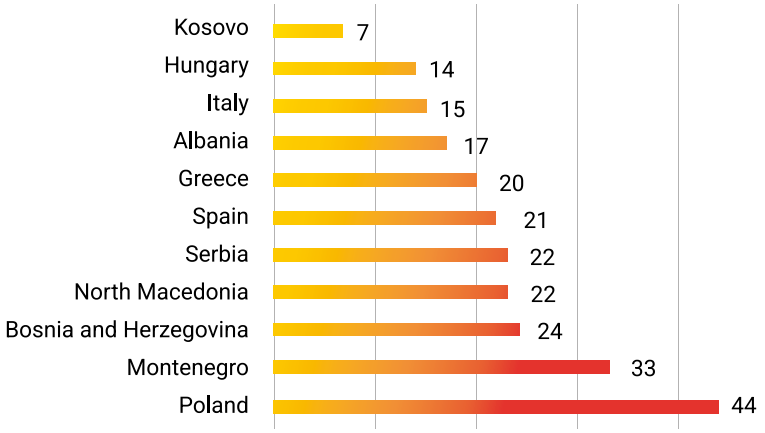
Apart from gathering basic information on the participants, the research explores digital security experiences, national digital security landscape, and cooperation among different actors. It assesses current levels of preparedness and protection, and identifies the most urgent gaps in capacity, opportunities for support, and cross-organisational cooperation. The needs assessment questionnaire, disseminated in January 2026, consisted of 38 questions, including 33 closed-ended questions (single or multiple choice) and 5 open-ended questions. Out of the total number of questions, 28 questions were mandatory, while 10 were optional. Each section of this analysis explores responses from all 11 countries while having in mind regional differences and pointing out the most important findings from each country.

Profile of Respondents

Number of Respondents and Countries They Come From

In total, the survey gathered 239 responses across 11 countries. The largest national sample came from Poland (44 respondents) and the smallest from Kosovo (7). The Western Balkans accounted for 125 respondents, while the European Union sample accounted for 114 respondents. Respondents were recruited through the CSDSN's partner organisations, each of which distributed the questionnaire to organisations and individuals in their respective countries based on existing professional relationships and knowledge of the local landscape. This gives a relatively balanced regional structure, but requires careful interpretation given the differences in sample sizes.

Table 1: Respondents per country

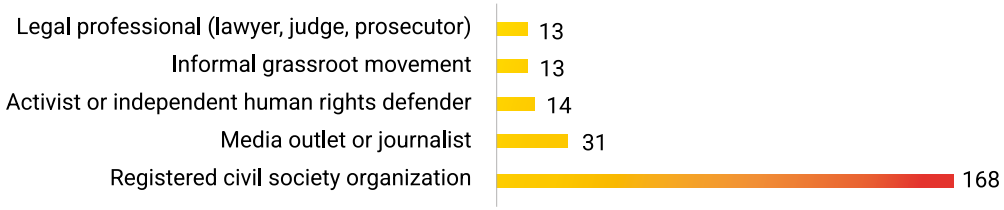


Status and Size of the Respondents' Organisations

The respondent pool is composed primarily of registered civil society organisations, which account for 168 of the 239 responses. The second-largest category is media outlets and journalists (31), followed by activists or independent human rights defenders (14), informal grassroots movements (13), and legal professionals (13).

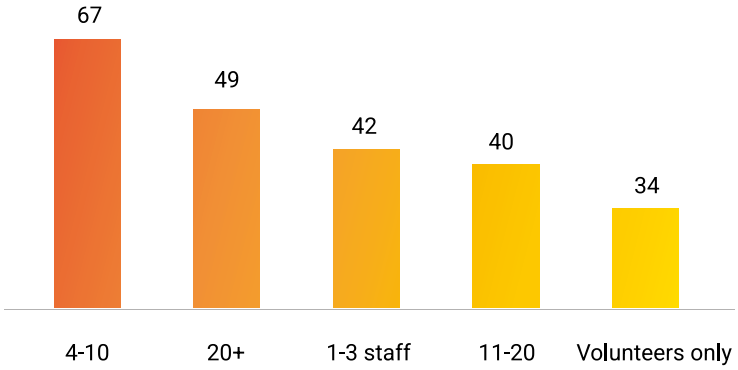
In most countries, registered civil society organisations (CSOs) are the largest respondent group, but there are differences. North Macedonia stands out as the only country in which media outlets and journalists form the largest category, with 11 respondents. Spain differs by including a comparatively strong presence of informal grassroots movements (7). Italy is distinctive because registered CSOs, media, and legal professionals are equally represented (4 each), with a notably stronger presence of legal professionals relative to other countries. By contrast, Kosovo's sample is entirely composed of registered CSOs, and Montenegro's sample is the most institutionally concentrated, with 31 of 33 respondents coming from registered organisations.

Table 2: Organisational status



The organisational size profile suggests that the sample is primarily composed of small and medium-sized organisations. Across all 11 countries, the most common category is organisations with 4–10 staff (67) while volunteer-only organisations form the smallest group (34).

Table 3: Organisational size



The dominance of the 4–10 staff category matters because small and medium-sized organisations often face high exposure to threats while lacking resources. This category is the largest in most countries, including Greece, Hungary, North Macedonia, Montenegro, Albania, Bosnia and Herzegovina, and Kosovo. However, Poland and Italy are more heavily represented by organisations with 20+ staff, suggesting a somewhat more institutionalised and resource-rich sample in those countries. Serbia stands out because its largest category is volunteer-only organisations (10), followed by 1–3 staff organisations (6). This indicates that the Serbian sample is more rooted in smaller, less formalised or lower-capacity civic structures than many others. On the other hand, Spain has an equal number of volunteer-only and 20+ staff organisations.

Main Topics Respondents' Organisations Deal With

The most prominent topics the organisations deal with are human rights, rule of law, anti-corruption, press freedom or journalism, environmental protection, and EU or democratic reform issues.

The thematic profile of the Western Balkan countries is as follows: Serbia is anchored in human rights, rule of law, environmental protection, and anti-corruption, with additional attention to minority rights, youth participation, and citizen engagement. Bosnia and Herzegovina combines human rights, especially women's rights and war-crimes accountability, with youth work, civic education, anti-corruption, and EU integration. Montenegro is marked by media freedom, journalist safety, and rights-focused work, alongside anti-corruption, democratic development, and marginalised-group rights. In North Macedonia, media and investigative journalism are dominant, along with anti-corruption, digital rights, media literacy, and rule of law. Albania is centred on human rights, democratisation, good governance, anti-corruption, and women's rights, while Kosovo reflects a mix of civic engagement, institutional monitoring, gender equality, disability rights, and community-level social issues.

In the EU sample it is noted that Hungary is shaped by independent media, investigative journalism, press freedom, rule of law, transparency, and anti-corruption, as well as the LGBTQ+ and Roma rights, refugees, and climate and energy policy. The most dominant topics in Poland include cybersecurity, civic education, rule of law and democracy, anti-corruption and transparency, human rights and legal aid, environmental protection, media, and strengthening civil society. Greece is concentrated around human rights, investigative journalism, accountability of state institutions, migration, transparency, and anti-corruption. Italy is the most legally specialised sample, with a notable emphasis on legal advocacy, migration law, criminal defence, digital rights, surveillance, and police repression. Spain appears the most movement-oriented, with particularly strong representation of environmental justice, LGBTQ+ rights, anti-racism, state violence, police repression, digital rights, and the criminalisation of human rights defenders.

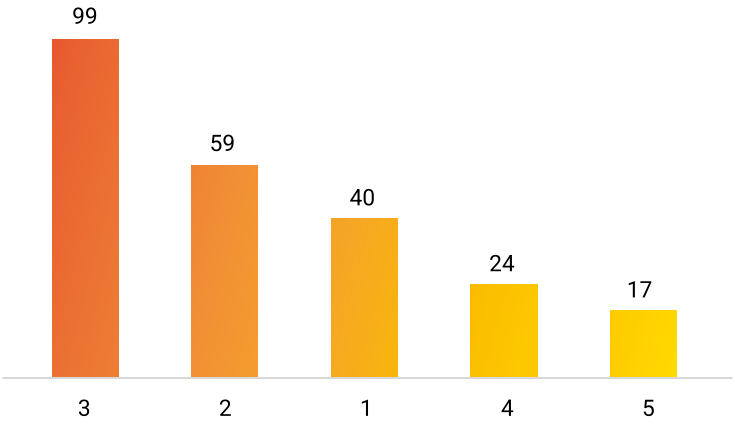
Digital Security Experiences

One of the important parts of the questionnaire was the assessment of familiarity with digital rights and legal remedies of the respondents, their participation in prior digital security training, and the existence of internal technical capacity or security practices.

Familiarity with Digital Rights and Legal Remedies

Across the full sample of 239 respondents, familiarity with digital rights and available legal remedies appears moderate but uneven. The most common response, on a scale of 1 to 5, was 3, selected by 99 respondents, indicating a basic awareness but not strong confidence in navigating digital security issues and legal protection mechanisms. Notably, lower scores (1 and 2) together account for 99 respondents, while only 17 respondents selected the highest score.

Table 4: Familiarity with digital rights and legal remedies

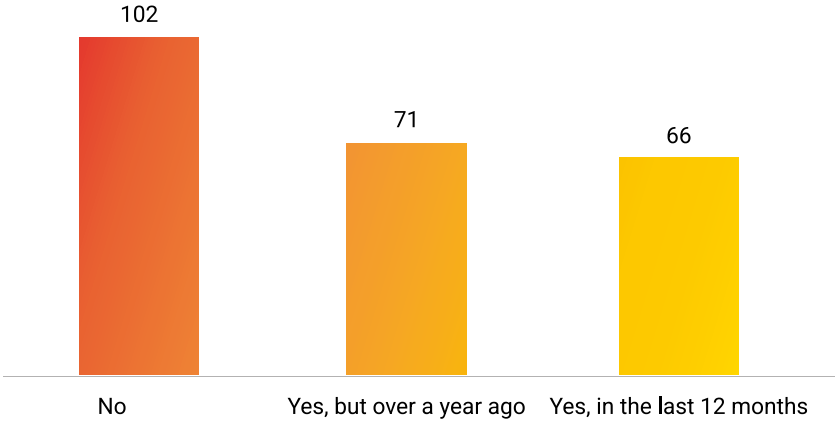


Participation in Digital Security Training

When we look at all 11 countries, most respondents attended digital security training, either in the last 12 months (66), or more than a year ago (71). However, 102 respondents have never attended digital security training. These findings are relevant given the incidents involving phishing, targeted social engineering, account takeovers, or coordinated online harassment campaigns, which calls for a combination of technical awareness and organisational procedures to mitigate these risks effectively.

Qualitative data from several countries shows the need for increased training support on both individual and organisational level. Additionally, one respondent from Hungary, argues that prior to building technical capacities, civil society needs awareness raising on the importance of digital security and protection.

Table 5: Participation in digital security training

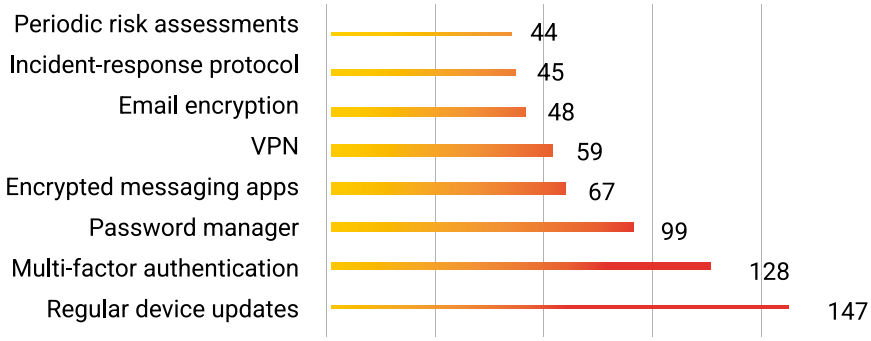


Currently Used Security Measures

When respondents were asked about digital security measures currently implemented within their organisations, results showed that basic technical practices are relatively widespread, but more advanced or procedural safeguards are less common. In that regard, the most frequently reported measures include regular device updates (147), multi-factor authentication (128), and password managers (99). These practices represent foundational digital security hygiene and suggest that many organisations are aware of at least some basic protective measures.

More notable, however, is relatively low number of organisations with structured approach to digital security. Only 45 respondents reported having incident-response procedures, while 44 are conducting regular risk assessments. While technical tools such as software updates or authentication mechanisms are widely adopted, fewer organisations appear to have structured organisational approaches to digital security management.

Table 6: Security measures in place



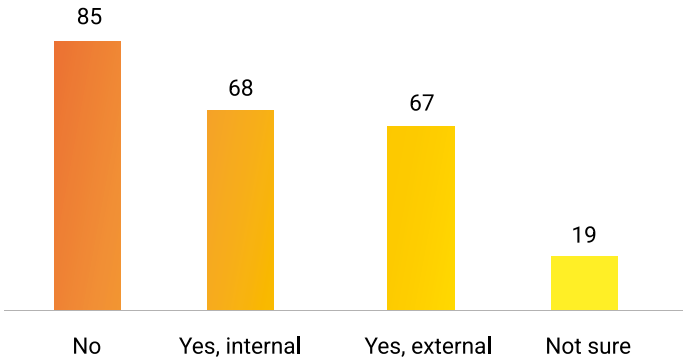
Organisations in Montenegro, Bosnia and Herzegovina, Serbia, and Kosovo most frequently report regular device updates and multi-factor authentication as their main

measures, while North Macedonia stands out for its strong usage of incident-response protocols (11) alongside high multifactor authentication use (16). Albania is distinctive because password managers are the most common measure (12), ahead of regular device updates. In Poland, the most common measures are also regular device updates (33) and multi-factor authentication (24), with relatively strong use of password managers (22) and relatively high usage of incident-response protocols (14) and virtual private network (VPN) (14). Spain stands out for encrypted messaging apps (12) and shows comparatively high use of password managers (11) and VPN (10), while Greece is notable for relatively frequent password-manager use (10) alongside device updates (12).

Designated Digital Security Staff

When we look at all countries in total, the largest group of respondents reported having no designated person responsible for digital security (85), with another 19 that are unsure. These results suggest that a significant portion of organisations operate without a clearly designated IT person in charge of digital security support. This may be particularly significant for smaller organisations, which may lack dedicated technical staff, but still face the same digital risks as larger organisations.

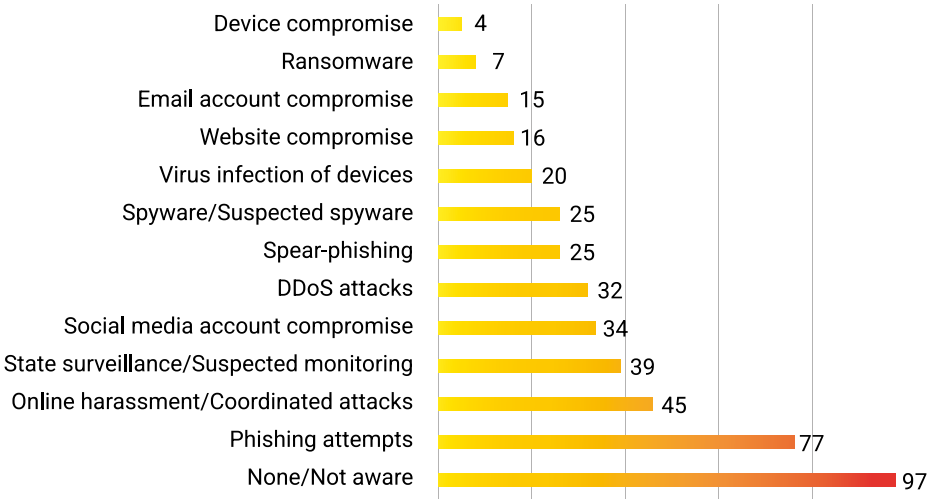
Table 7: Designated digital security focal point



Incidents That Occurred in the Past 24 Months

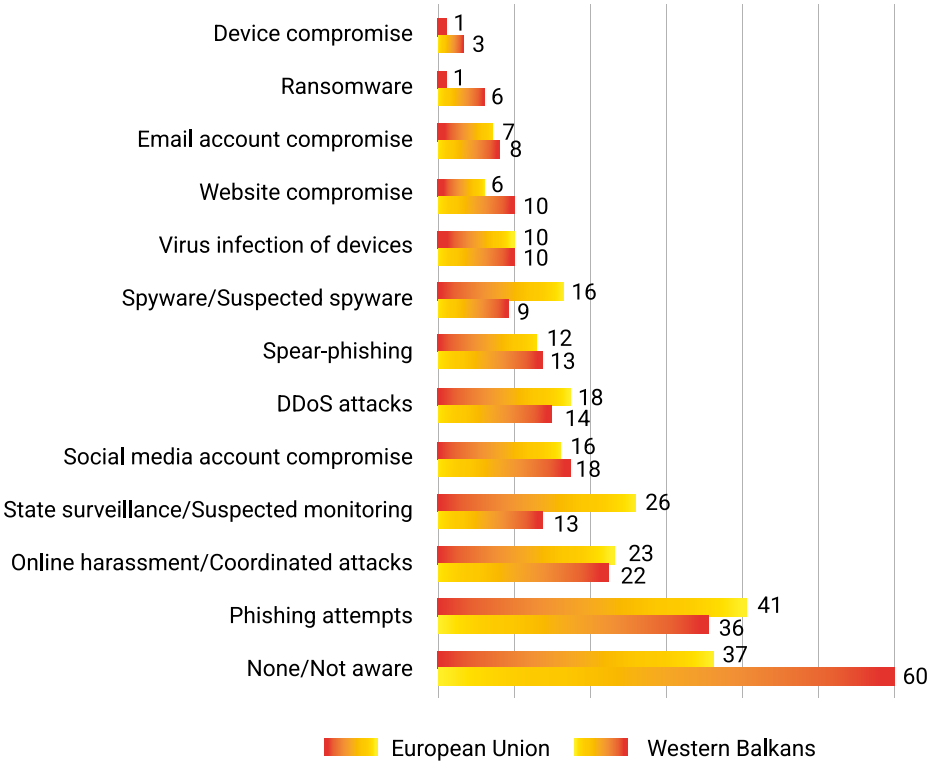
Across the full sample, the majority of respondents stated that they did not encounter a digital security incident in the past 24 months or that they are unaware of it (97). Among those who did report incidents, phishing attempts were by far the most common response (77). On the other hand, ransomware (7) and device compromises (4) were the least reported, while, notably, half of the latter responses came from Serbia. This distribution suggests that the threat environment is defined by a combination of mass and semi-targeted attacks, especially phishing, public-facing attacks, such as harassment and social media compromise, and higher-risk targeted threats, including suspected surveillance, spyware, and distributed denial of service (DDoS).

Table 8: Digital security incidents in the past 24 months



At the regional level, there is a visible difference between the two blocs. In the Western Balkans, "None/not aware" remained the most frequent response (60), while in the EU sample, however, phishing attempts (41) slightly exceeded it (37). State surveillance or suspected monitoring (26) and online harassment (23) were also more visible in the EU sample. This suggests that although phishing is a cross-regional problem, the EU sample shows stronger concentration of explicitly identified hostile activity, especially surveillance-related.

Table 9: Digital security incidents in the past 24 months by region



State surveillance was reported by 39 respondents and is one of the most common and serious categories. Greece (8), Serbia (7), Poland (6), and Hungary (5), report the highest counts that are followed by Spain (4), Italy (3), North Macedonia and Albania (2 each), and Montenegro and Bosnia and Herzegovina (1 each).

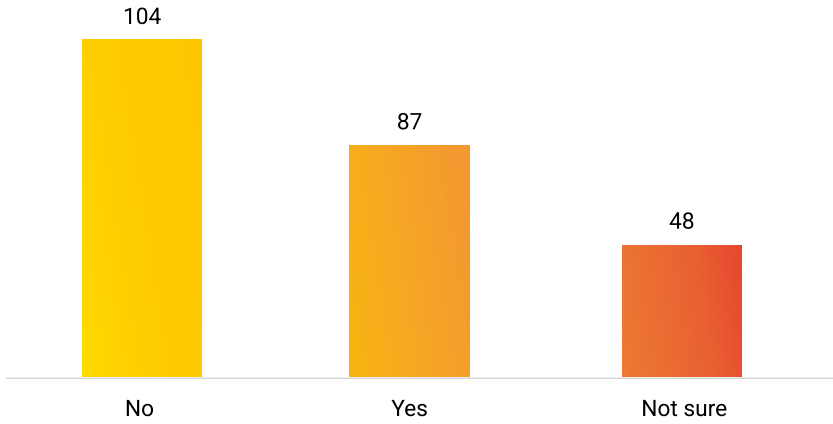
Spyware (a total of 25 responses) is concentrated in Spain (5), Poland (4), Albania (4), Serbia (4), Hungary (3), and Italy (3), but the numbers are believed to be much higher given that the detection requires professional forensic support and may have not been sought or available to everyone. Qualitative data referred to personal experiences and publicly documented cases involving the use of Pegasus spyware in Hungary, Serbia, and Spain, Paragon/Graphite spyware in Italy, and the Predator usage in Greece.

Online harassment (45) is most prevalent in Greece (7), Poland (7), and North Macedonia (6), as well as in Hungary, Albania, and Serbia with 5 respondents in each country. A consistent pattern across all regions shows that organisations working on LGBTQ+ rights are disproportionately targeted. Harassment takes the form of coordinated bot attacks, comment-section flooding, and mass reporting campaigns designed to get accounts suspended. In Hungary and Serbia, smear campaigns in pro-government media serve as a complementary public-reputational attack timed to investigations or advocacy events. Notably, North Macedonia stands out for online harassment (6) and DDoS attacks (6), which aligns closely with the large media-oriented profile of its respondents.

Unusual Behaviour of Mobile Device

A high number of respondents did not notice unusual behaviour of mobile devices (104), while 87 respondents did. However, 48 respondents could not reply with certainty. Respondents were further asked if the unusual device behaviour started after a particular event.

Table 10: Unusual mobile device behaviour

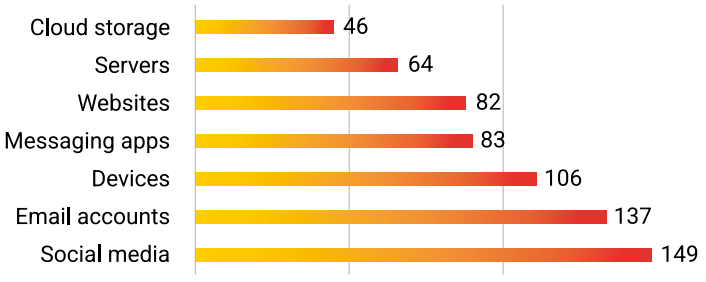


In most countries, respondents could not confidently tie anomalies to a single trigger, but a suggestive pattern emerges. Across the region, respondents reported device anomalies, call interference, and login difficulties during politically sensitive periods. Open-ended questions show us that in Serbia, suspicious behaviour followed police contact, detention, and phone confiscation. In Bosnia and Herzegovina, similar issues surfaced around the 2014 Tuzla protests. In an open-ended question one respondent from the Bosnia and Herzegovina noted that device anomalies tend to appear before high-risk events rather than after, thus suggesting anticipatory surveillance, not reactive monitoring. In Montenegro, anomalies correlated with public criticism and source contact, while North Macedonia featured one account of long-term recurring surveillance tied to political connections. Furthermore, suspicious behaviour of devices coincided with the conversations with journalists investigating a wiretapping scandal (Greece), an activist trial (Spain), Pride events and a civil society transparency law (Hungary), meetings with foreign diplomats (Albania), and a Facebook post about a planned protest in Turin (Italy).

Most Vulnerable Tools and Assets

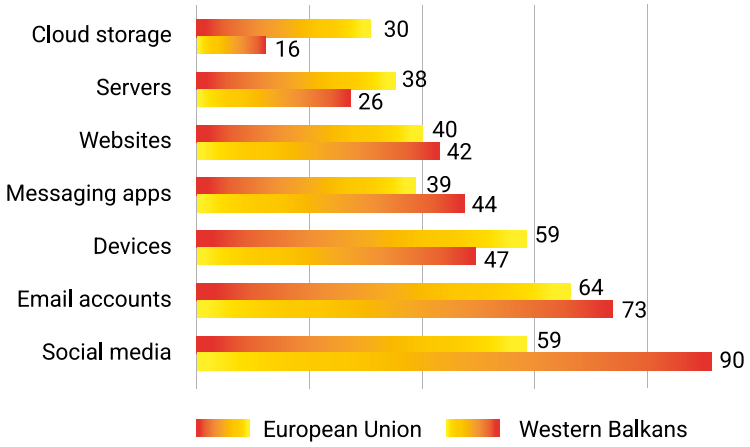
Social media (149) and email accounts (137) are the most cited vulnerable assets, the two most widely used, and most commonly attacked tools. Devices (106) rank third, with Spain (17) and Italy (14) showing the highest concern, consistent with confirmed personal device surveillance in those countries. Messaging apps (83) are most assessed as most vulnerable in Montenegro (14) and Italy (9). Servers (64) are most cited in Poland (20), reflecting larger organisational digital infrastructures, while cloud storage (46) is least frequently cited as vulnerable overall. This shows that the greatest concern is placed on the tools that are central to daily communication, public visibility, and external engagement. Social media and email accounts are main means of communication, but also the points where harassment, phishing, impersonation, and reputational attacks most often occur.

Table 11: Most vulnerable tools and assets



There are some regional distinctions. In the Western Balkans, social media (90) clearly stands out as the most frequently selected vulnerability, while in the EU sample concern is more evenly distributed across email accounts (64), devices (59), and social media (59).

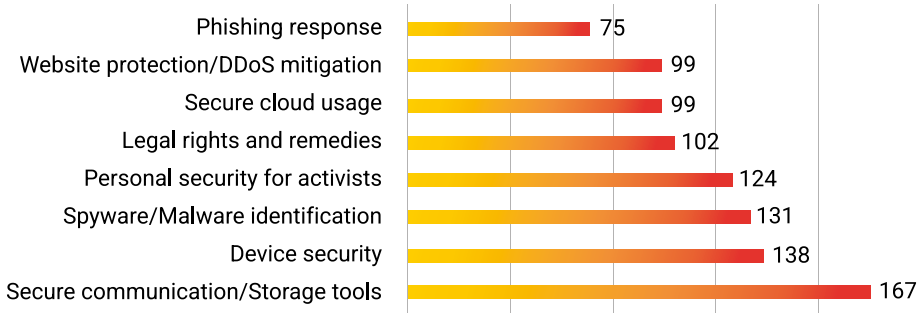
Table 12: Most vulnerable tools and assets by region



The Most Important Digital Security Topics

When asked about digital security issues and topics that are currently important or may become important in the future, across all countries, the most frequently selected topic was secure communication and storage tools (167 selections). This was followed by device security (138) and spyware and malware identification (131) particularly interesting for Poland (28) and Montenegro (22). There is high interest in spyware and malware in Bosnia and Herzegovina (13), Spain and Serbia (11 each), as well as in Greece, North Macedonia, and Italy (10 each). These countries are followed by Hungary (7), Albania (5), and Kosovo (4). Personal security for activists (124) follows closely, with Montenegro (17) and Spain (16) leading on activist security which is consistent with its confirmed surveillance and police infiltration cases. Legal rights and remedies (102) show notably high demand in Montenegro (18), Poland (12), and Greece (11), consistent with those countries' surveillance issues. It is interesting to highlight that phishing response (75) ranks lowest, even though it is a prevalent form of the attack.

Table 13: Important digital security topics

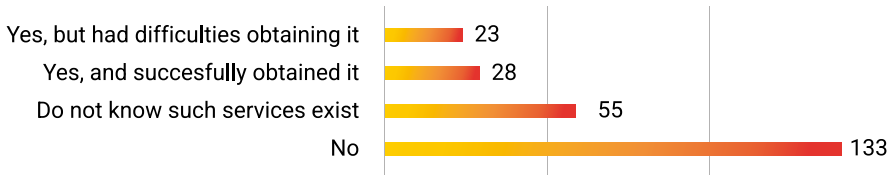


Digital Forensic Support

The final dimension of respondents' digital security experience concerns access to specialised forensic support. While earlier responses demonstrated that civil society actors frequently encounter digital threats or suspicious device behaviour, the availability of technical investigation support remains limited. Respondents were asked whether they had ever needed digital forensic support, such as professional examination of devices for spyware or other forms of compromise. The results, across the full sample of 239 respondents are the following:

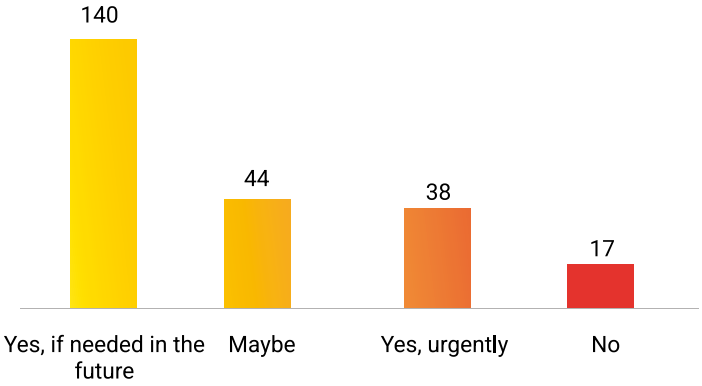
A total of 133 respondents reported that they had never needed digital forensic support, while a notably high number (55) were unaware that such services exist. This means that beyond technical capacity gaps, there is also a knowledge and awareness gap regarding available digital investigation resources. Among the respondents who did need forensic support, the split between those who successfully obtained it (28) and those who experienced difficulties (23) is nearly even, meaning that roughly half of organisations seeking forensic support struggled to access it. As we have seen, the number of incidents and the need for support are high, but limited accessibility of forensic services and the need for skilled experts represent the gap that needs to be corrected. This gap can leave organisations in a position where they suspect malicious activity, but cannot prove it, limiting both legal action and advocacy.

Table 14: Access to digital forensic support



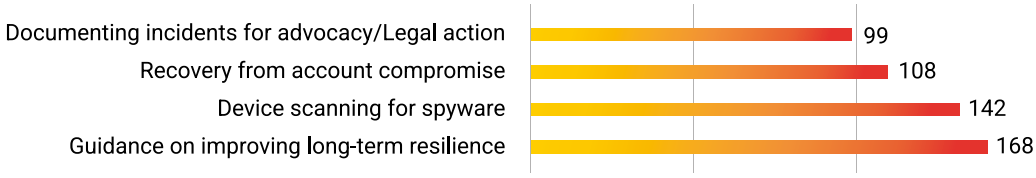
Respondents from all countries are highly interested in Digital Forensic Clinic. Out of all respondents, 140 indicated they would be interested in receiving support if needed in the future, while 38 respondents reported an urgent need for such support. Only 17 respondents stated they would not be interested. Greece, Spain, and Montenegro show the largest number of respondents expressing an urgent need for support (5 each), followed by Serbia and Italy (4 each), Bosnia and Herzegovina, North Macedonia, and Kosovo (3 each), and Hungary, Albania, and Poland (2 each).

Table 15: Interest in the Digital Security Clinic



When asked what types of forensic assistance would be the most useful, the responses indicated that civil society actors are seeking not only reactive investigation services, but also broader security support that strengthens long-term resilience. Across the full sample, guidance on improving long-term resilience dominated with 168 responses followed by device scanning for spyware (142). Notably, on one hand, organisations require technical diagnostics, such as device scanning and incident recovery. On the other hand, they also need strategic and procedural support that helps them prevent future incidents and respond more effectively when attacks occur.

Table 16: Most useful types of forensic support

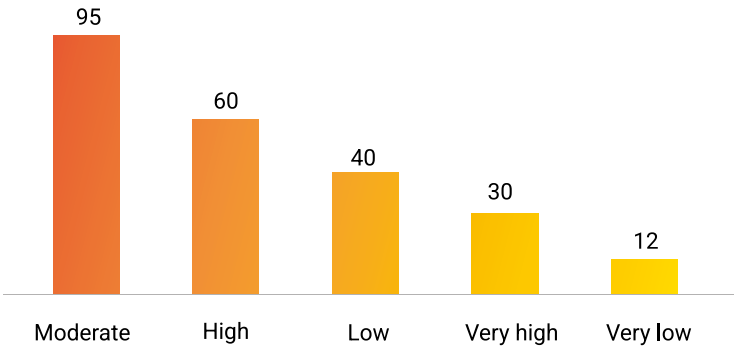


National Digital Security Landscape

Estimated Level of Digital Repression

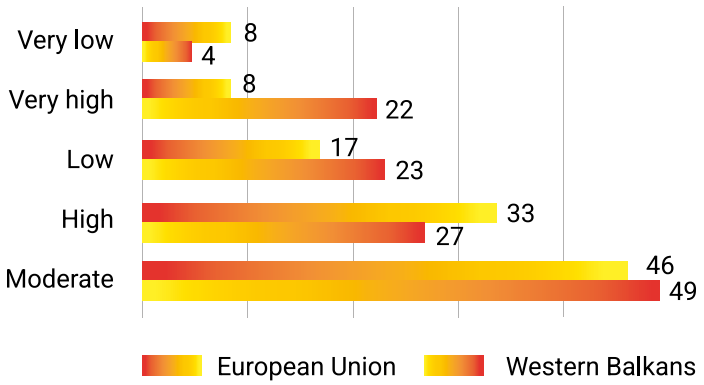
Across the full sample, respondents most often assessed the level of digital repression in their countries as moderate (95). Combined, high and very high assessments account for 90 respondents, while only 12 respondents across 11 countries selected very low. Digital repression, hence, presents an ongoing, persistent, and structural pressure, not an isolated occurrence. However, it is not perceived as equally intense everywhere.

Table 17: Level of digital repression



Both the Western Balkans and the EU groups commonly chose moderate repression (49 in the Western Balkans and 46 in the EU). However, the Western Balkans show somewhat stronger concentration of high and very high responses combined (49) compared to 41 in the EU. This is particularly visible in Serbia, where respondents concentrated around high (10) and very high (9) repression, making it the clearest response in the entire questionnaire. Italy and Greece follow, with 12 and 9 respondents rating the repression as high. By contrast, Poland, Montenegro, North Macedonia, Bosnia and Herzegovina, Spain, and Hungary, are more concentrated in the moderate category, though this should not be read as an absence of pressure.

Table 18: Level of digital repression by region



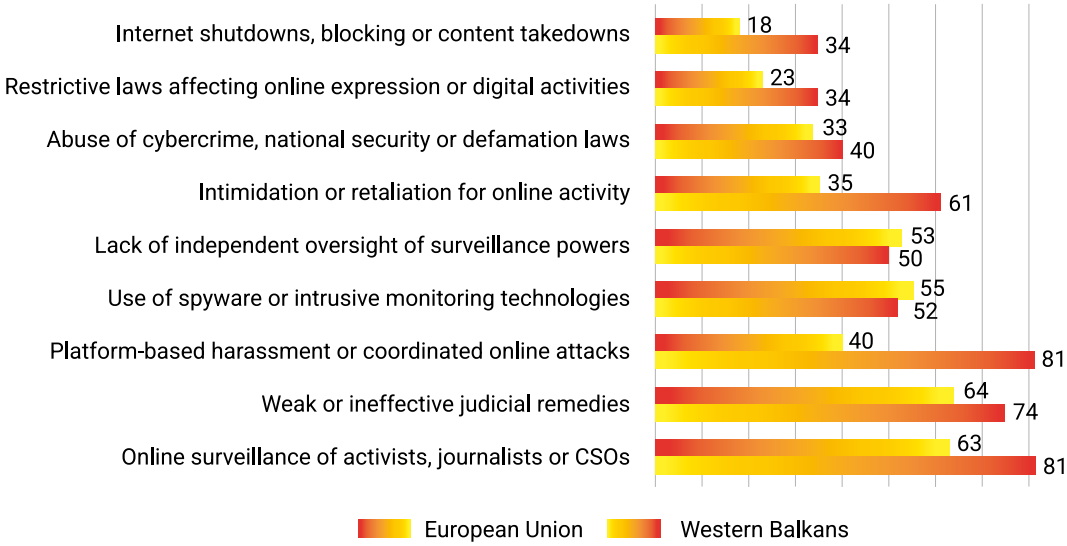
Reasons Behind Digital Repression Assessment

Across all countries, the two most frequently selected reasons for digital repression are online surveillance of activists, journalists, or CSOs (144 selections) and weak or ineffective judicial remedies (138) while internet shutdowns (52) are the least reported both in Western Balkans and the EU. The findings related to the assessment of digital repression are significant because they show that repression is perceived as both technical and political.

Table 19: Reasons behind digital repression assessment

There are important regional differences here. In the Western Balkans, the most prominent reasons behind the assessment of digital repression are online surveillance (81) and platform-based harassment (81). In the EU sample, by contrast, weak or ineffective judicial remedies (64) slightly surpass online surveillance (63), while spyware or intrusive monitoring technologies (55) were especially prominent.

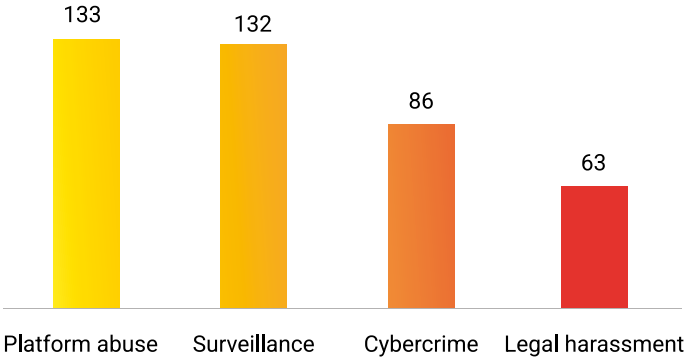
Table 20: Reasons behind digital repression assessment by region



The Most Prevalent Digital Threats

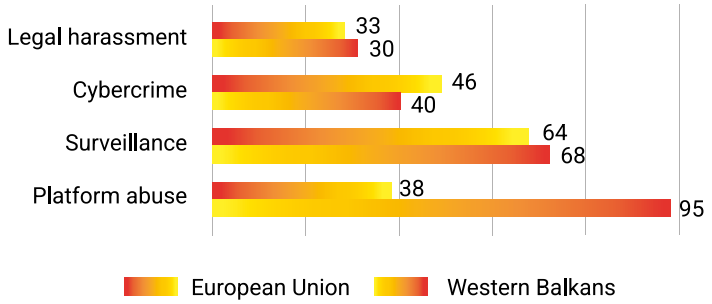
Respondents identify platform abuse (133) and surveillance (132) as the two most prevalent threats in civic space, indicating that digital repression is experienced both through state monitoring and attacks conducted via online platforms.

Table 21: Prevalent digital threats



Regional differences are evident since in the Western Balkans, platform abuse (95) is the dominant threat, followed by surveillance (68), while the EU sample emphasises surveillance (64) as the primary threat, followed by cybercrime (46) and platform abuse (38).

Table 22: Prevalent digital threats by region

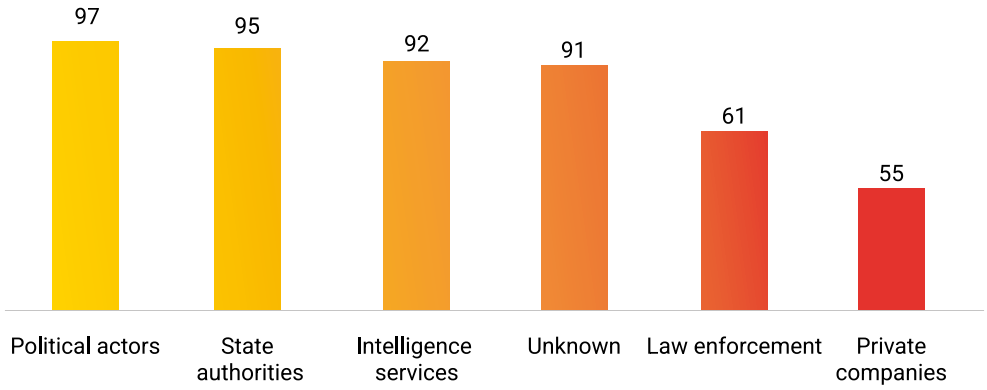


Country-level patterns reinforce this distinction. Poland stands out with cybercrime (30) as the most prominent threat, while Serbia, North Macedonia, Montenegro, Albania, Bosnia and Herzegovina, and Kosovo primarily report platform abuse, often linked to harassment campaigns and manipulation of social media spaces. Moreover, Greece, Hungary, Italy, and Serbia identify surveillance as the leading threat, consistent with qualitative reports of spyware use, monitoring concerns, and state-linked intrusion. Notably, Serbia shows a dual pattern where surveillance and platform abuse are equally prominent (18 each), reflecting both state-sponsored monitoring and online pressure.

Actors Behind Digital Repression

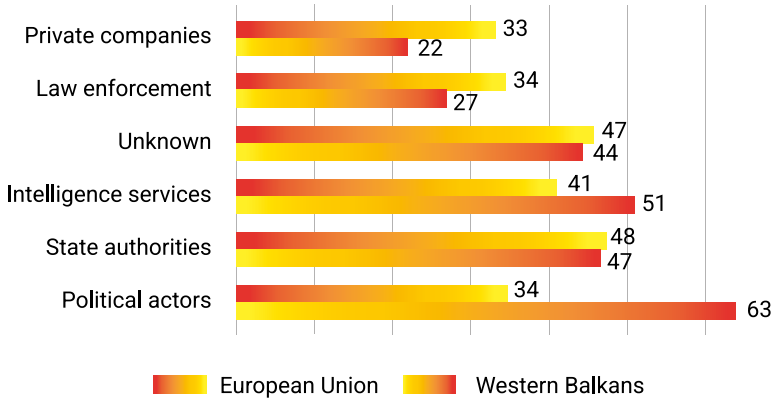
Respondents' views on who is behind digital threats point to strong political reasons behind the assessment of digital security environment. In all countries, the most mentioned are political actors (97), state authorities (95), and intelligence services (92).

Table 23: Main actors behind digital threats



In the Western Balkans, political actors (63) are the most frequently identified source of threats, followed by intelligence services (51) and state authorities (47). In the EU sample, state authorities (48) and unknown actors (47) lead, followed by intelligence services (41). This suggests that Western Balkan respondents frame digital threats as political.

Table 24: Main actors behind digital threats by region

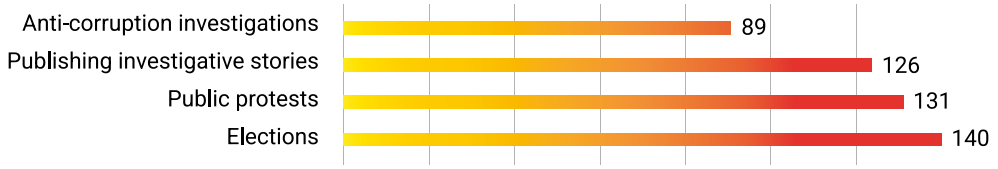


Country examples make this more concrete: Serbia strongly points to state authorities (20) and intelligence services (16), Montenegro emphasises political actors (21), Hungary points to state authorities (12) and intelligence services (9), Italy identifies intelligence services (11) as the leading actor, while Spain is distinctive for placing law enforcement (13) at the centre and Greece has the most mentions of private companies (10).

Triggers for Increased Digital Repression

Across the surveyed countries, respondents identify clear patterns regarding when digital repression intensifies. Elections (140) are the most consistent trigger, but high representation of other politically sensitive moments suggests that digital repression escalates during times when political stakes and civic mobilisation rise.

Table 25: Triggers for increased digital repression



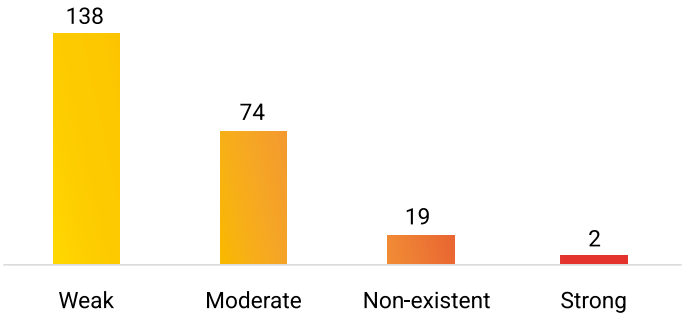
The pattern is broadly similar across regions, though in the Western Balkans, elections, investigative reporting, and protests rank very highly, while in the EU sample, elections and protests dominate slightly more than investigative reporting.

The increase of digital threats is often closely connected with elections with this pattern being especially pronounced in Poland (29), Albania (15), and Hungary (12). Montenegro (22) and Serbia (21) stand out for public protests as primary trigger, while Spain also follows this pattern (13). North Macedonia differs in that publishing investigative stories is the most cited trigger (18), although elections and public protests are also reported at high levels (15 each). Greece is distinctive because threats are most strongly associated with anti-corruption investigations and publishing investigative stories (14 each), while in Bosnia and Herzegovina, elections and public protests are tied as the most frequently cited activities (16 each). In Italy public protests (10) and publishing of investigative stories (9) stand out the most.

Legal Protection Against Digital Attacks

Perceptions of legal protection against digital attacks are predominantly negative. Across the full sample, 138 respondents rated legal protection as weak, while only 2 assessed it as strong. Both of those responses came from the EU sample (Poland and Spain), which makes this one of the clearest findings in the needs assessment.

Table 26: Legal protection against digital attacks



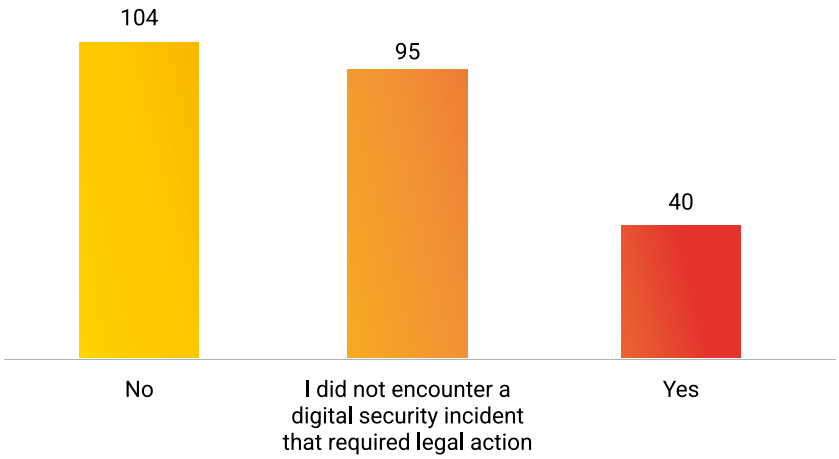
The Western Balkans show a more pronounced deficit in perceived legal protection compared to the EU sample. In the Western Balkans, 75 respondents rated legal protection as weak and 15 as non-existent, while no respondent considers it strong. In the EU sample, 63 respondents rated protection as weak, 40 as moderate, and only 2 as strong.

At the country level, particularly negative assessments appear in Serbia (18 rate it as weak) and Montenegro (21 rate it as weak), while Poland also shows a strong concentration of weak ratings despite its larger sample (26). By contrast, Spain and Italy display a more mixed pattern between weak and moderate assessments. In Spain, 10 respondents assessed it as weak and 10 as moderate, while in Italy, there were 7 responses for each of those two options. Kosovo stands out as relatively more positive example, mostly assessing legal protection as moderate (5).

Legal Measures (Not) Taken by Respondents

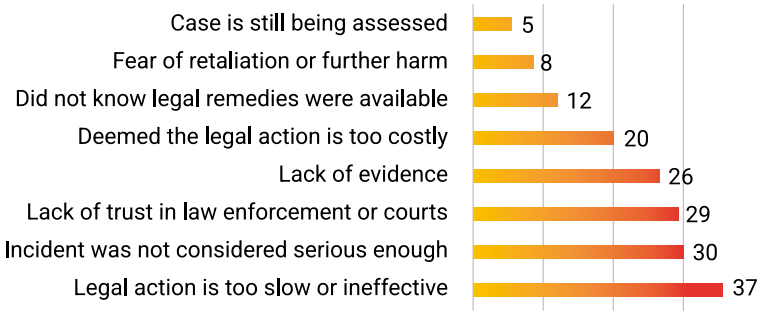
Legal remedies are rarely used following digital security incidents, reflecting respondents' scepticism about their effectiveness. Across the sample, only 40 respondents reported taking legal action, while 104 did not take them. In the Western Balkans, 59 respondents reported not pursuing legal action compared to 19 who did, while in the EU sample the gap is smaller but still clear (45 no and 21 yes).

Table 27: (Not) taken legal actions



The most common reason for not taking action is that legal procedures are too slow or ineffective (37). The lack of trust in law enforcement or courts was also notably high (29). Only 12 respondents cited not knowing legal remedies existed. This suggests that legal channels are primarily not used because respondents lack confidence in their effectiveness, rather than because they are unaware of them. Additionally, in open-ended questions respondents described police in Serbia "playing naive" about digital threats, while in Bosnia and Herzegovina, months of inaction after a formal report led respondents to conclude that it is better not to report incidents at all. There were significant difficulties in Italy even getting the postal police to accept a formal complaint.

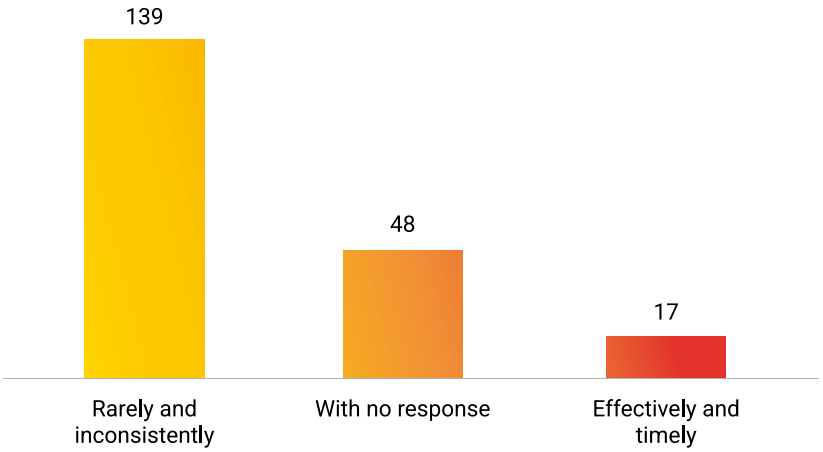
Table 28: Reasons for not taking legal action



Institutional Response to Digital Attacks

Respondents' assessments of institutional responses to digital attacks are predominantly negative. Out of the total number, 139 respondents stated that national institutions respond rarely and inconsistently, while only 17 indicated that responses are effective and timely.

Table 29: Institutional response to digital attacks



The pattern is particularly pronounced in the Western Balkans, where only one respondent from Kosovo reported an effective institutional response, compared to 76 who said that institutions react rarely and inconsistently, and 33 who reported no response. Although the EU sample shows slightly more positive responses, the overall picture remains critical.

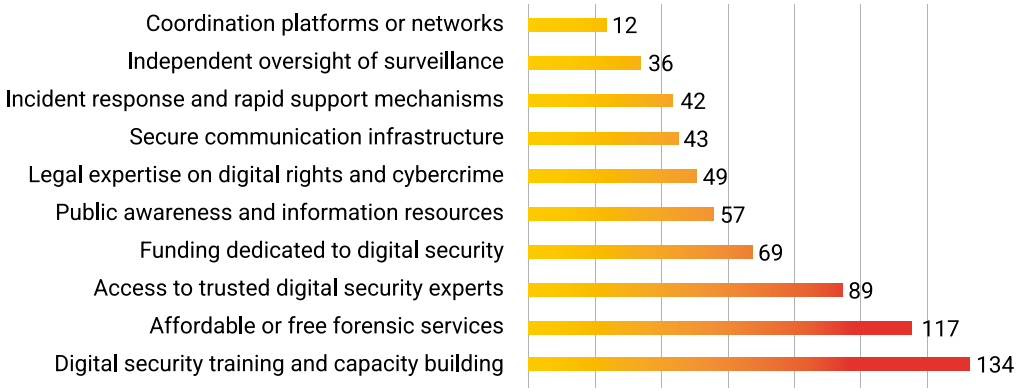
Rare and inconsistent responding pattern is especially pronounced in Poland (23), Montenegro (20), and North Macedonia (18). It is followed by Greece (14), Bosnia and Herzegovina (13), Serbia (11), Albania (10), Hungary and Italy (9 each), Spain (8), and Kosovo (4). However, Poland stands out as the only country where a more positive assessment is reported, with 12 respondents saying institutions respond effectively and timely, although rare and inconsistent responses remain the most common overall.

Bosnia and Herzegovina (8), Italy and Albania (6 each), and Montenegro (7) are distinctive for relatively high shares reporting no response from institutions. Overall, the clearest pattern is that respondents across countries see institutional responses as weak and mostly absent, while effective and timely intervention is rare.

Lacking Digital Security Resources

Respondents across the surveyed countries identify several key gaps concerning the digital security support. The most frequently cited missing resources are digital security training and capacity building (134) and affordable or free forensic services (117). On the other hand, independent surveillance oversight (36) and platforms for coordination (12) appear to score the lowest. The findings indicate that the main challenge is not the absence of a particular tool or service, but a broader systemic deficit, where organisations lack knowledge, support, technical capacity, and financial resources.

Table 30: Lacking digital security resources



In the Western Balkans, respondents emphasise training, forensic services, and access to trusted experts, pointing to basic infrastructure and expertise gaps. In the EU sample, while training and forensic support remain key needs, there is relatively greater emphasis on public awareness and independent oversight of surveillance, reflecting concerns about systemic governance and accountability.

Organisations in Montenegro, Poland, North Macedonia, Bosnia and Herzegovina, Greece, Spain, Italy, and Kosovo most frequently identify digital security training and capacity building as the key missing resource, with the highest counts in Montenegro (24), Poland (19), Bosnia and Herzegovina (15), and North Macedonia (14). In many of these countries, the next most common gap is affordable or free forensic services, which is especially prominent in Montenegro (22), Spain (12), North Macedonia (12), Hungary (11), Poland (11), and Italy (9). Hungary and Serbia differ slightly in that affordable or free forensic services emerge as the most frequently cited missing resource (11 in Hungary and 10 in Serbia), while in Serbia this is followed by funding dedicated to digital security (9). Greece is notable for relatively high demand not only

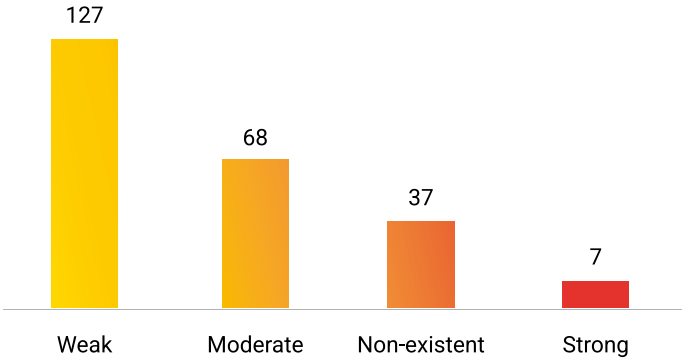
for training and capacity building (12), but also for access to trusted digital security experts (10), while Poland stands out for the number of needs reported, particularly training (19), public awareness and information resources (16), and funding (15). Overall, the findings suggest that civil society actors operate in environments where digital threats are increasing but support structures remain insufficient, leaving organisations to manage risks with limited technical, institutional, and financial support.

Cooperation Among Different Actors

Strength of Cooperation

Cooperation among organisations working on digital security issues is generally perceived as limited. Most respondents describe cross-organisational cooperation as weak (127), while only 7 respondents consider cooperation strong, indicating that despite shared exposure to digital threats, coordination among civil society actors remains underdeveloped.

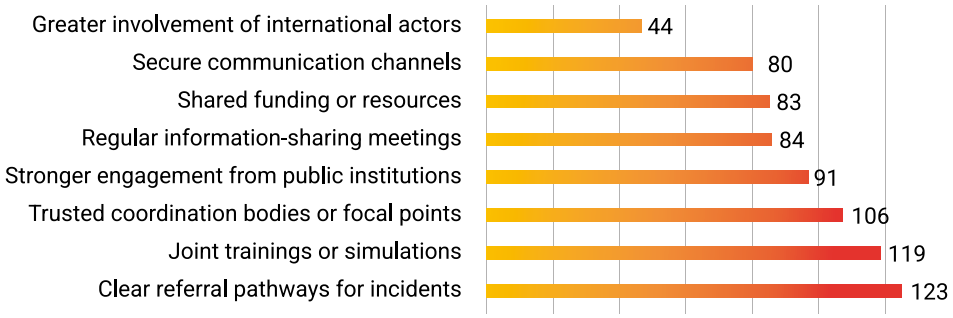
Table 31: Cooperational strength



Opportunities for Improvement

However, respondents suggested opportunities for improvement such as clear reporting pathways for digital security incidents (123) and joint training and simulations (119). Somewhat smaller number of respondents (44) calls for greater involvement of international actors. Overall, suggestions indicate that civil society actors are seeking more structured, predictable, and coordinated mechanisms for collaboration, rather than ad hoc or informal cooperation.

Table 32: Opportunities for improving cooperation

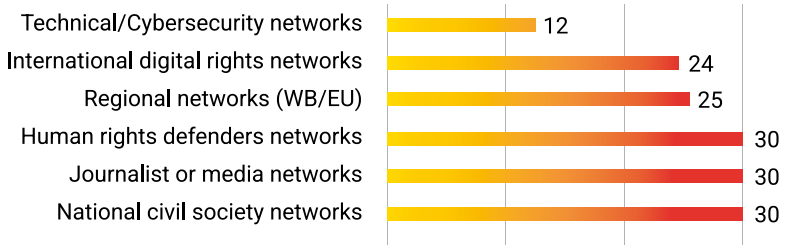


Participation in Different (Inter)National Networks

Participation in different formal networks remains limited. Across the full sample, 169 respondents report not being connected to any national, regional, or international networks, while 70 respondents indicate that they are currently part of such networks. The gap is particularly large in Montenegro (27 no, 6 yes), Poland (35 no, 9 yes), Bosnia and Herzegovina (19 no, 5 yes), and Spain (18 no, 3 yes), while Serbia stands out as the most balanced case, with responses evenly split (11 yes, 11 no) along with Greece (10 yes, 10 no).

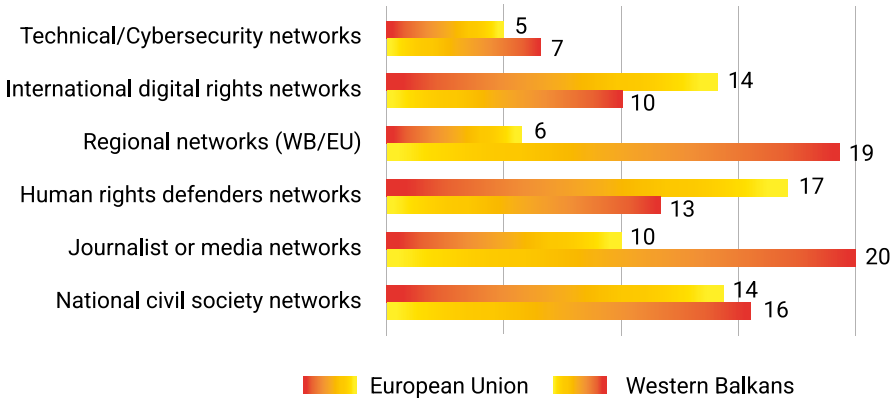
Overall, the respondents often mention national civil society networks, journalist or media networks, and networks of human rights defenders (30 each). The smallest number of respondents (12) is connected to technical networks focused on cybersecurity and they come from Poland and North Macedonia (3 each) as well as Greece, Spain, Kosovo, and Bosnia and Herzegovina (1 each).

Table 33: Types of existing networks



In the Western Balkans, respondents are mostly connected through regional networks and journalist/media networks, with Serbia standing out for national civil society and regional networks (6 each) and North Macedonia for journalist/media networks (9). In the EU, respondents are somewhat more linked to international digital rights networks and human rights defender networks, with Greece standing out most clearly, especially for human rights defender networks (7).

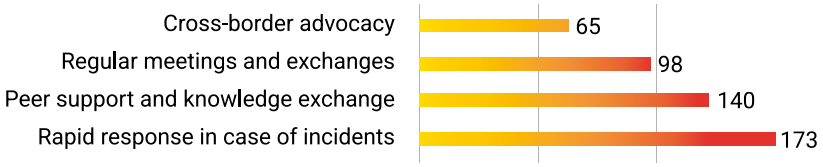
Table 34: Types of existing networks by region



Expectations from the Civil Society Digital Security Network

Respondents' expectations from the CSDSN focus primarily on practical support and coordinated responses to digital threats. The most frequently requested form of support is rapid response assistance in case of digital security incidents (173), standing out clearly as the top priority and reflecting a strong need for a reliable, accessible first line of help. Overall, respondents expect CSDSN to act as both a practical support mechanism during incidents and a platform for sustained cooperation and knowledge sharing across countries.

Table 35: Expectations from CSDSN



Conclusion

The findings of this needs assessment demonstrate that civil society across the Western Balkans and the European Union faces a digital threat environment that is persistent, politically motivated, and institutionally not addressed. Surveillance, spyware, phishing, and platform-based harassment, are deployed most intensively during elections, protests, and investigative reporting, precisely when civic actors are most exposed. Simultaneously, the protection mechanisms available remain critically insufficient. The organisations most exposed to these threats are, in the majority of cases, operating without adequate technical capacity, forensic support, effective legal recourse, or consistent institutional backing.

Data shows that moving forward several priorities require coordinated response. One of the priorities reflects the need for capacity building that would not only require one-off training, but rather long-term and sustainable support that encompasses training and simulations, access to experts, and rapid coordination in case of emergencies. Access to digital forensic support represents another significant gap, given that a substantial share of respondents was either unaware that such services exist or needed them but could not obtain them. Furthermore, legal protection against digital attacks was assessed as weak or non-existent by the majority of respondents across all 11 countries and low assessment of legal remedies reflects lack of confidence in their effectiveness. Strengthening legislative frameworks on digital rights and surveillance oversight, alongside dedicated legal support for organisations willing to pursue cases, is essential. At the institutional level, national authorities and digital platforms must improve their responses to attacks targeting civil society. Moreover, cooperation among civil society actors remains underdeveloped, unlike the scale of shared risk. Moving from informal engagement to structured coordination is necessary for the development of strong, joint response against digital repression.

Finally, sustaining all of the above requires dedicated funding that lasts over the years, funds services such as training, digital forensic clinics, expert access, and organisational resilience, a funding that treats digital security as a core component of civil society resilience. The scale and persistence of the threats documented here, set against the depth of the identified protection gaps, shows that sustained, coordinated investment in the digital security of civil society is a prerequisite for the continued functioning of independent civic space across the Western Balkans and the European Union.

Sources and Notes

1 Yana Gorokhovskaia, Cathryn Grothe, and Amy Slipowitz, "Freedom in the World 2026: The Growing Shadow of Autocracy," Freedom House, March 2026, p. 16, https://freedomhouse.org/report/freedom-world/2026/growing-shadow-autocracy.

2 Gorokhovskaia, Grothe, and Slipowitz, "Freedom in the World 2026: The Growing Shadow of Autocracy," p. 17.

3 European Parliament, "Spyware: MEPs sound alarm on threat to democracy and demand reforms," May 8, 2023, https://www.europarl.europa.eu/news/en/press-room/20230505IPR84901/spyware-meps-sound-alarm-on-threat-to-democracy-and-demand-reforms.

4 Amnesty International, "'A Digital Prison': Surveillance and the suppression of civil society in Serbia," December 2024, https://www.amnesty.org/en/documents/eur70/8814/2024/en/.

5 Stiftung Mercator, https://www.stiftung-mercator.de/en/.

6 Belgrade Centre for Security Policy, https://bezbednost.org/en/.

7 Zašto ne? [Why not?], https://zastone.ba/en/.

8 Centre for Civic Education, https://cgo-cce.org/en/.

9 Kosovar Centre for Security Studies, https://qkss.org/en/.

10 Institute for Democracy 'Societas Civilis' - Skopje, https://idscs.org.mk/en/.

11 Centre for the Study of Democracy and Governance, https://csdgalbania.org/.

12 Hungarian Helsinki Committee, https://helsinki.hu/en/.

13 Amnesty International Greek Section, https://www.amnesty.gr/.

14 Amnesty International Italian Section, https://www.amnesty.it/.

15 Amnesty International Spanish Section, https://www.amnesty.org/en/location/europe-and-central-asia/western-central-and-south-eastern-europe/spain/.

16 Institute of Public Affairs, https://www.isp.org.pl/en.

Abbreviations

BCSP	Belgrade Centre for Security Policy
CSO	Civil Society Organization
CSDSN	Civil Society Digital Security Network
DDoS	Distributed Denial of Service
EU	European Union
VPN	Virtual Private Network
WB	Western Balkans

List of Tables

About the Author

Anđela Savić is a researcher at the Belgrade Centre for Security Policy, with a particular interest in human rights, digital security, and trends contributing to repression and the shrinking space for the independent and critical work of civil society.

Before joining BCSP, she worked on issues related to war crimes, transitional justice, and conflict prevention, as well as media and the economic and social rights of marginalised groups. She is experienced in research and writing and is the author of several articles and publications dealing with the wars of the 1990s in the former Yugoslavia, their legacy, and their impact on contemporary socio-political developments.

She has also gained experience in programme and project development and management, civil society capacity-building, monitoring, evaluation and learning (MEL) practices, and the organisation of public events through cooperation with domestic, regional, and international organisations, as well as with human rights defenders, activists, media representatives, academia, and the donor community.

About the Belgrade Centre for Security Policy

The Belgrade Centre for Security Policy (BCSP) is an independent research centre dedicated to building a democratic society with accountable institutions, in which security is a public good and people are free, equal, and live without fear. Through research, public advocacy, community development, and education, the BCSP contributes to improving citizens' security in line with democratic principles and respect for human rights. Guided by the values of human rights and freedoms, democracy, accountability and transparency, integrity, and solidarity, the BCSP seeks to contribute to shaping the future development of the Western Balkans.

Founded in 1997, the Centre operated under the name Centre for Civil-Military Relations (CCMR) until 2010. Since 2012, it has consistently been ranked as the highest-rated think tank from the Western Balkans working on defence and national security, as well as foreign policy and international relations, in the most prominent global ranking of research centres – the Global Go To Think Tank Index Report.

The BCSP is the founder of the Belgrade School of Security Studies and specialist postgraduate programmes that later evolved into the successful master's programme International Security at the Faculty of Political Sciences, University of Belgrade. It is also one of the founders of the National Convention on the European Union and serves as the coordinator of Working Group for Chapter 24 (Justice, Freedom and Security). In addition, the BCSP is the founder and coordinator of the prEUgovor coalition, which monitors reforms under Chapters 23 (Judiciary and Fundamental Rights) and 24 (Justice, Freedom and Security) of Serbia's EU accession negotiations. The Centre is one of the organisers of the Belgrade Security Conference, an international event that for more than a decade has brought together leading experts in the fields of security and foreign policy.

Among the BCSP's strategic objectives are: supporting the development of civil society organisations and agents of change in order to create an environment conducive to more transparent and accountable functioning of state institutions; producing analyses on issues related to security, the rule of law, and Serbia's foreign and security policy; and providing support to human rights activists, freedom fighters, and whistleblowers in order to strengthen their mission and enhance the democratic capacities of society as a whole.

BCSP website: https://bezbednost.org/en/.

RESEARCH REPORT / 11

UNDER PRESSURE

DIGITAL SECURITY OF CIVIL SOCIETY IN THE WESTERN BALKANS AND THE EUROPEAN UNION

Publisher
Belgrade Centre for Security Policy
Đure Jakšića 6/5 Belgrade
www.bezbednost.org

Author
Anđela Savić

Design
Srđan Ilić

ISBN-978-86-6237-279-6

DOI: https://doi.org/10.55042/NAAQ4804

May 2026 - Belgrade

This publication is part of the project Defending Digital Freedoms: Strengthening Civil Society Resilience against Digital Repression in Europe, funded by Stiftung Mercator. The views and opinions expressed in this publication are those of the authors and do not necessarily reflect the views or positions of Stiftung Mercator.

BCSP Belgrade Centre for Security Policy

Civil Society Digital Security Network

www.bezbednost.org

ISBN-978-86-6237-279-6

DOI: https://doi.org/10.55042/NAAQ4804