CNTI CENTER for NEWS, TECHNOLOGY & INNOVATION.

Using global research & collaboration to promote an informed digital society

JANUARY 2026

Journalists & Cyber Threats

How can we better ensure the digital security of the press and protect against cyber threats?

Find the full issue primer, current legislation and events online: https://cnti.org/issue-primers/journalists-cyber-threats/

CNTI's Assessment

The digital security of news organizations, journalists and their sources is under threat in many parts of the world. Digital security attacks can range from spyware, account hacking, distributed denial of service (DDoS) and malware, among many other threats. These threats, in addition to their intrusive nature, can also violate journalists' sense of safety and security, creating a chilling effect and harming the broader information environment.

Policy deliberation: Governments must not surveil journalists or sources but instead foster an environment that encourages free speech.

Professional support: News organizations must proactively educate their journalists and other staff on cyber threats and provide support for those who are targeted. Journalists need to adopt strong digital security practices.

Governance: Technology companies need to ensure that working with governments to protect people does not put fundamental rights at risk.

The Issue

Journalists and their sources face digital security threats globally from a variety of actors, including states, corporations and criminal organizations. These threats can take a variety of forms, such as malware, spyware, ransomware, distributed denial-of service (DDoS) and social engineering.

Digital threats are often linked to physical threats and can result in significant mental health concerns for journalists Beyond the safety risks, digital security challenges can damage public trust in the news media. Cyberattacks can disrupt operations and business models, driving away audiences. A lack of digital security training, especially in smaller newsrooms, can cause sources and whistleblowers to fear being unintentionally exposed. These threats are difficult and expensive for news organizations to manage alone, making collaboration among policymakers, tech platforms and civil society essential.

What Makes It Complex?

1. The effectiveness of cybercrime policies depends on how "cybercrime" is defined.
2. Digital policies sometimes lead to unintended consequences that impact the digital security of journalists and the general public.
3. Governments and non-state actors are using spyware to surveil and intimidate journalists.
4. The ability to mitigate digital security risks differs across countries and across newsrooms.
5. Journalistic practices and norms can, at times, be in tension with digital security practices.

JANUARY 2026

Journalists & Cyber Threats

The Center for News, Technology & Innovation (CNTI), an independent global policy research center, seeks to encourage independent, sustainable media, maintain an open internet and foster informed public policy conversations.

State of Research

In the wake of prominent attacks and among a growing concern about AI's broader threats to journalism, academic and public attention to the impact of cybercrime, ransomware and spyware on journalists has increased.

Research has depicted the unique threats of digital surveillance to investigative journalists and marginalized people and communities, including women, queer and gender-nonconforming people, and people of color. As noted earlier, there is a relationship between journalists' digital presence and offline safety.

This research speaks to the global nature of digital security threats to an independent press. Future research should continue to examine how journalists, technology companies, researchers and policymakers can collaborate to defend against these threats, by tracking trends and sharing practices.

Notable study

Journalists Who Face High Risks Require Better Security Practices to Provide News **— CNTI (2025)**

Takeaway: The study shows that there is a gap between the experiences of journalists and organizational response. As a result, there is an opportunity for news organizations to increase engagement on cybersecurity issues and help journalists work more safely and effectively.

1 in 3

journalists surveyed by CNTI regularly face serious risks, but their level of preparedness varies. *(CNTI, 2025)*

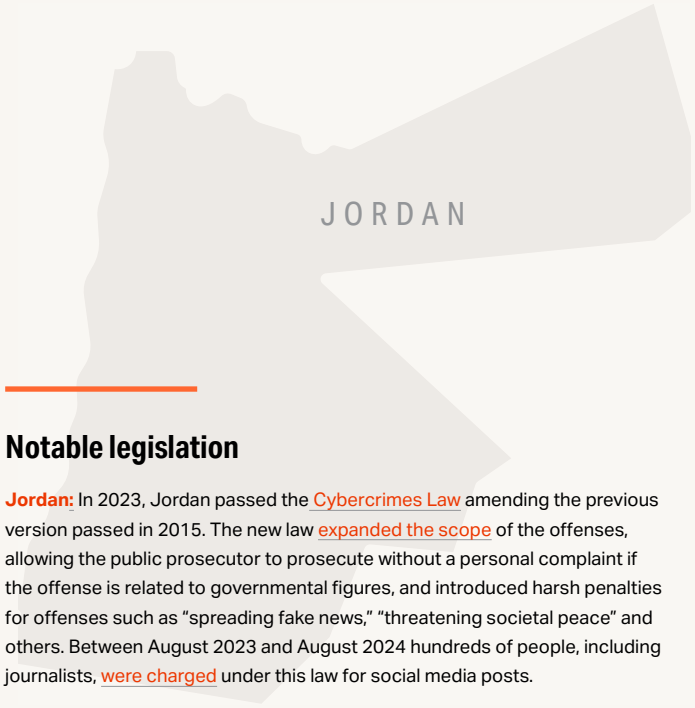
23%

of journalists surveyed by CNTI say they are "very confident" in their ability to recognize a cyber security threat, while 50% say they are "fairly confident." *(CNTI, 2025)*

State of Legislation

Cybercrime policy does not always account for — and at times directly threatens — the digital safety of journalists. Often, cybercrime policy efforts are led by countries' security or banking sectors, leading to policymaking that may be at odds with international standards for press freedom and privacy. Research has found that many cybercrime laws can be used to target journalists, thus threatening an independent press and free expression.

Over the past two decades, legal frameworks established to protect an independent press and the confidentiality of journalistic sources and information have been threatened in many parts of the world. New legislation and policies, including national security legislation, override and/or contradict existing protections. Other policies pressure or force digital intermediaries to provide private user data. When legislation does not adequately account for new digital data or new technological tools used by journalists and sources, it cannot provide them with necessary legal protections. Thus, forward-thinking policymaking is critical.



Notable legislation

Jordan: In 2023, Jordan passed the Cybercrimes Law amending the previous version passed in 2015. The new law expanded the scope of the offenses, allowing the public prosecutor to prosecute without a personal complaint if the offense is related to governmental figures, and introduced harsh penalties for offenses such as "spreading fake news," "threatening societal peace" and others. Between August 2023 and August 2024 hundreds of people, including journalists, were charged under this law for social media posts.