CNTI

CENTER for NEWS,
TECHNOLOGY & INNOVATION.
Using global research & collaboration
to promote an informed digital society.

innovating.news

Information & Cybersecurity

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

CNTI's Assessment

The digital security of publishers, journalists and their sources is under threat in many parts of the world. At the governmental level, policymakers must acknowledge the very real threats facing journalists and ensure that digital policy initiatives both protect them and, in doing so, do not threaten free expression, basic privacy rights, or encryption and VPN protections. At the platform level, technology companies can establish and protect human rights and privacy safeguards, but they also must at times navigate challenging state demands (at times via legislation) to provide private data and information on their users, potentially permitting governments' abuses of power. At the publisher level, proactive efforts around cyber education, safety and support, as well as sharing experiences within the industry, are equally critical. Finally, researchers and civil society need to do their part to collaboratively shed light and provide data on the risks, harms and potential avenues forward.

Find the full issue primer, current legislation, events, and changemakers online

https://go.innovating.news/DzsquU

The Issue

Digital security and cybersecurity threats, in particular, have become more important than ever for the global news media as journalists and publishers are becoming high-profile targets for malware, spyware and digital surveillance, compromising their and their sources' personal information and safety.

Cybersecurity threats facing the global news media represent a broad range of actions, including spyware, denial-of-service (DDoS) and malware, ransomware, and phishing attacks. A range of actors can be involved in these practices, including nation-states and politicians, powerful individuals, corporations, criminal networks and extremist organizations. Broader digital security threats include growing concerns about software vulnerabilities, uses of digital surveillance, attempts to chip away at encryption protections, and digital safety and privacy concerns on social media platforms.

There is a critical connection between digital and physical threats to journalists: For instance, the use of spyware has been linked to hundreds of acts of physical violence around the world. Aside from the clear safety concerns, cybersecurity risks also threaten trust in the global news media and can create chilling effects for sources and whistleblowers.

These threats are expensive and difficult to protect against via newsroom efforts alone, and that difficulty is magnified for independent journalists or publishers operating in (or in exile from) countries with hostile governments or authoritarian regimes. Thus, collaboration among policymakers, platforms, researchers and domestic and international civil society organizations is critical to ensure the digital security of the global press.

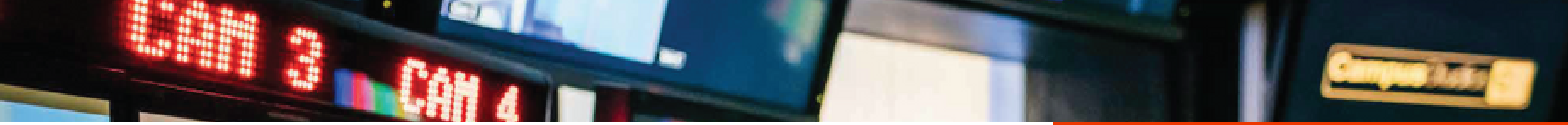
What Makes It Complex

I. Addressing the scope of cybercrime threats through policy – both in general and for journalists and sources specifically – fundamentally depends on the definition and scope of cybercrime.

II. Policies related to digital matters can sometimes lead to unintended consequences that impact the cybersecurity of both journalists and the general public.

III. The ability to mitigate digital security risks differs across countries and across newsrooms.

IV. Journalistic practices and norms can, at times, be in tension with digital security practices.



State of Research

Academic and public attention to cybersecurity, including ransomware and spyware, has grown in the wake of prominent cyber attacks and amid growing concerns about the threats of generative AI technologies to digital privacy and security.

Research has found that journalists and their sources are increasingly concerned about or experiencing a range of digital security threats, but this does not always translate into changing practices or policies to counter such threats. Research has also revealed the relationship between journalists' digital presence and offline abuse. These risks are often amplified in non-Western regions and in areas of conflict. A majority of cybercrime laws include provisions that can be used to target an independent press and free expression, often via vague or broad wording and few safeguards to protect against investigatorial overreach.

Future research can continue to examine how journalists, technology companies, researchers and policymakers can collaborate to defend against these threats. Some basic questions lack global evidence: It is largely unclear, for instance, how or to what extent digital security technologies such as encryption software have been implemented by journalists in various parts of the world, including in non-Western contexts.

Notable studies

Weaponising the law: Attacks on media freedom
Thomson Reuters Foundation & Tow Center for Digital Journalism (2023)

Summary: Cybercrime, including cyber libel, is identified as one of eight key legal threats to independent journalists around the world.

CNTI's Takeaway: This work illustrates two critical elements of digital policies: that they have definitional clarity (e.g., ensuring laws are clearly worded and not too broad or narrow) and that they offer specific oversight processes and safeguards.

State of Legislation

As of 2021, the UN Conference on Trade and Development found that 156 countries (80%) had enacted cybercrime legislation, though adoption rates fluctuate by region. However, cybercrime policy (including but not limited to "cyber libel," "cyberterrorism," and "online hate speech" laws) does not always account for – and at times directly threaten – journalists' digital safety. Legal frameworks protecting the confidentiality of journalistic sources and information have also been under threat in many parts of the world.

Global experts have called for collaborative approaches to global cybersecurity regulations, including through private and public sector coordination as well as through strengthened international data protection frameworks.

Notable legislation

United Nations:
In September 2023, the latest negotiations concluded for the UN's proposed global treaty on cybercrime. While intended to help countries share information on such crimes, autocratic governments have sought to broaden the scope of cybercrime, which could curtail an independent press and free expression. Consensus was not reached on fundamental issues, including the scope and definition of cybercrimes or human rights safeguards. Experts have noted concerns that a flawed treaty may empower human rights abuses and authorize broad cross-border surveillance.