Countering Digital Threats in Modern Journalism

Kárpáti László

karpati.laszlo@proton.me

The 21st century has seen the transformation of the landscape of journalism. Once, physical safety was the primary concern for reporters tackling controversial topics. Now, the battlefield has shifted to the digital domain, making cybersecurity an indispensable part of journalistic practice.

The Dual Front of Harassment

While physical harassments, such as stalking and direct confrontation still remain some of the most effective methods of intimidating and silencing journalist, the rise of digital threats has introduced a new level of complexity to this field. The Pegasus spyware scandal in Hungary, where investigative journalists of the opposition were surveilled without their consent, highlighted how opposition voices are monitored and obstructed.

Beyond spyware, the tragic murder of Slovak journalist Ján Kuciak and his fiancée stands as a harrowing example of how such threats can escalate into a full-blown manslaughter for the sake of hiding the tracks of corruption. Kuciak was investigating political corruption and organized crime before being killed in 2018. This brutal act drew international condemnation and became a stark reminder of the dangers of holding power to account.

Speaking of eliminating whistleblowers on a global scale, the murders of journalists like Jamal Khashoggi, Anna Politkovskaya or Dominic Phillips illustrate the international nature of such actions taken against modern journalists. For instance, Khashoggi's assassination inside the Saudi consulate in Istanbul shook the whole

international community, while Politkovskaya's killing in Russia demonstrated how governments use violence to silence dissenting voices.

Online Harassment Takes Over the Stage

With the widespread appearance of the internet, virtually anyone can get access to both the local and global news and to those creating the news. That being said, the internet has amplified the reach and intensity of attacks on journalists by allowing for a vast arsenal of possible forms of assault. From trolling – where waves of derogatory comments tarnish reputations – to more severe threats like doxxing, the tools of online harassment grow ever more sophisticated by the year. An example of doxxing occurred during the 2020 U.S. elections when government officials covering politically sensitive topics found their private information leaked online.

Deepfake technology has also emerged as a potent weapon, allowing attackers to create highly convincing, but utterly false content. To counter such attacks, Britain has already started implementing laws promising severe punishment for those, who create deepfake explicit material. Deepfake misuse isn't confined to individuals; in 2024, fake audio clips involving Peter Magyar, the leader of the TISZA Party, were widely circulated, in an attempt to sow misinformation within the public.

Even technical attacks, like Distributed Denial of Service (DDoS), pose significant risks by paralyzing entire news platforms. During the 2021 Hungarian primaries, the news portal 444.hu was targeted in a large-scale DDoS attack, temporarily halting its operations.

Defending the Digital Front

Protecting against these threats requires both personal and organizational vigilance. For individual journalists, basic steps like creating and using strong passwords, enabling two-factor authentication (2FA), and encrypting communications are

essential. Tools like Signal and ProtonMail ensure end-to-end encrypted exchanges, while Virtual Private Networks (VPNs) like NordVPN or ExpressVPN hide a journalist's location and activity from prying eyes.

For organizations and editorial offices, cybersecurity protocols are both crucial and a must. Media outlets like The Guardian and The New York Times have dedicated teams ensuring their systems are secure against sophisticated attacks. Open-source tools like Tor or secure browsers such as Brave add extra layers of protection, thus helping journalists to minimize their digital footprints.

United We Stand: Global Efforts to Protect Journalism

International and local organizations play a pivotal role in supporting journalists and journalism under siege. Groups like Reporters Without Borders (RSF) and the International Federation of Journalists (IFJ) provide critical training and advocacy, equipping journalists with tools to combat cyber threats. The IFJ's cybersecurity workshops empower journalists to navigate online risks effectively, while the RSF campaigns for stricter legal measures against harassment.

In Hungary, the Hungarian Journalists Association (MÚOSZ) offers support and resources for local reporters, ensuring they have access to legal aid and training.

Safeguarding Press Freedom

Attacks on journalists are not just personal matters, but assaults on press freedom and democratic values. These actions aim to muffle those who dare to uncover inconvenient truths. Truths that might be painful and inconvenient for some leading force. To counter this, journalists must arm themselves with the knowledge and tools to navigate an increasingly hostile digital landscape, ensuring their work continues to inform and empower the whole of society.

By embracing cybersecurity as a core part of modern journalism, reporters can uphold their mission without compromising their safety or integrity. Free press is not a privilege; it is a necessity for a thriving democracy. Therefore, all of us must ensure its survival.