SANA'A CENTER

Electronic Blackmail in Yemen:

A Digital Weapon Exploiting State Fragility

Anonymous hackers carry out a cyber attack. // Photo credit: Alamy/Dragos Condrea

By: Bashar al-Aqab

April 24, 2026

The Sana'a Center for Strategic Studies is an independent think-tank that seeks to foster change through knowledge production with a focus on Yemen and the surrounding region. The Center's publications and programs, offered in both Arabic and English, cover political, social, economic and security related developments, aiming to impact policy locally, regionally, and internationally.

Cybersecurity has become an inseparable part of national security and stability, as the digital realm now encompasses communications, administration, services, and vital data. With the growing reliance on digital services, the potential risks from technical vulnerabilities and the absence of institutional protection are rising. In Yemen, cybersecurity is constrained by limited technical infrastructure and weak institutional frameworks governing data access. Those who control the telecommunications sector can regulate information flows, monitor individuals, and direct public discourse, turning «digital infrastructure» into a tool of control rather than a mere technical service. This makes implementing cybersecurity a complex issue, as technical factors intersect with institutional structures and societal norms. In the meantime, the lack of legislation, enforcement, and digital protections leaves many at risk of exploitation, particularly Yemeni women.

Data from the Digital 2024 – Yemen report, an annual report that compiles digital data on internet usage and social media trends worldwide, and from Internet Society Pulse, a non-profit platform that aggregates data from reliable sources, highlight the limitations and underdevelopment of Yemen's digital infrastructure. The Digital 2024 report estimated that internet users numbered approximately 6.16 million, 17.7 percent of the total population, while active mobile connections reached nearly 20.83 million, representing 59.8 percent. The number of social media users was 3.6 million, or 10.3 percent of the population. Mobile networks remain the primary means of internet access, and the digital divide among segments of Yemeni society persists, reflecting the fragility of the communication infrastructure and the limited reach of modern digital services. Connectivity is treated by users as a scarce resource that requires careful management. Internet use is tied to periods when the network and power are available, and most rely on low-cost Android smartphones, which account for the majority of smart devices in Yemen.

The weak institutional structures in Yemen have given rise to local initiatives. Small technical support networks have been established in neighborhoods and shops, where maintenance and app cloning are conducted informally. Over time, these activities have given rise to a social-digital system based on expertise and practical knowledge, alongside attempts to develop electronic payment services and simple digital transactions. However, these practices open the door wide to cyber risks, as they prioritize low costs over security and grant access to personal data that can be exploited, including for digital blackmail and fraud.

Data from Digital 2024 and a special Reuters report indicate a digital gender gap; Yemeni males constitute the vast majority of internet and social media users. Women make up just 13 percent of Facebook users in the country. This disparity reflects a set of economic, social, and knowledge constraints that limit women's access to technology. The high cost of devices and connectivity, a lack of technical skills, and cultural restrictions on internet use lead to cumulative digital marginalization.

Yet women are increasingly the victims of cybercrime. Digital loopholes are exploited to create one of the most dangerous and complex forms of gender-based violence, as criminals manipulate societal norms to carry out electronic blackmail and online harassment. Personal photos and information are exploited in threatening practices that damage reputation and social standing. Yemeni society places the burden of "family honor" on women. Any breach of privacy, even if accidental or the result of a hack, becomes a source of social punishment and isolation. Consequently, the threat of publishing photos or personal conversations is often an effective means of silencing victims, given a deep-seated fear of reputational damage.

Social and educational constraints exacerbate the problem. Many Yemeni women lack access to secure personal devices and the digital skills and equitable education needed to use them safely. The gap is not only a technical one; reliance on local intermediaries or informal maintenance shops, combined with restrictions on women's freedom of movement and ability to seek help directly, increases their susceptibility to exploitation and turns privacy violations into mechanisms of social and financial pressure.

Another challenge is Yemen's weak cybersecurity: the country lacks a national cybersecurity strategy, legislation to protect personal data, or laws to combat cybercrime. This legislative vacuum leaves individuals and institutions exposed to data breaches, ransomware attacks, and digital surveillance activities. The weakness of the justice system and the failure of existing laws to adapt to the nature of digital crimes allow perpetrators to escape punishment, making victims, particularly women, even more vulnerable. Often, these cases are handled through the prism of protecting honor rather than protecting rights, allowing perpetrators to escape punishment while victims are punished with stigma and blame. In the absence of specialized cybersecurity agencies or technical and legal support centers, Yemeni women remain exposed to a predatory digital space where blackmail is entrenched as a tool of social and economic oppression. The lack of legal frameworks for governance and an institution to monitor violations and prosecute offenders has turned the digital realm in Yemen into an open space for blackmail and surveillance, with the government unwilling or unable to protect its citizens.

In a conflict-affected state like Yemen, with weak political stability or institutional capacity, alternative approaches may be necessary. Digital literacy could be strengthened to protect citizens, with support from informal education, community initiatives, media, and civil society organizations. Public discussions could be held about digital privacy and dignity as rights in themselves. With sufficient engagement, the normalization of digital violence can be curbed, even in the absence of legislative frameworks. But until the government implements substantial reforms to strengthen cybersecurity, Yemeni society will be left to face escalating digital risks, with few tools to fight them.

Bashar al-Aqab is the Chairperson and Founder of the Jaadal Center for Peace and a Cyber Security student at the University of Jordan. Bashar has a strong interest in digital security, peace, and community coexistence. He has extensive experience in engaging youth, managing cultural projects, and leading community initiatives. His writings and contributions emphasize the importance of promoting digital security and fostering peace.

This publication was produced as part of the second phase of the Yemen Peace Forum (YPF), a Sana'a Center initiative that seeks to empower the next generation of Yemeni youth and civil society activists to engage in critical national issues. The YPF is funded by the Government of the Kingdom of the Netherlands.

SANA'A CENTER

www.sanaacenter.org