



Research Center
Transformations
of Political Violence

Policy Brief

no 4
2024



Photo: DALL-E/PRIF (May, 2023)

From Internet Shutdowns to Personal Harassment: Examining the Spectrum of Digital Violence Against Social Activists

Laura Gianna Guntrum | Christian Reuter



From Internet Shutdowns to Personal Harassment

Examining the Spectrum of Digital Violence Against Social Activists

In conflict-affected settings, activists use Information and Communication Technologies (ICTs) to attract international attention to their cause and stay informed about events. However, digital violence is a growing global concern. Perpetrators are often anonymous, making effective recourse difficult, and legal frameworks are often inadequate. Drawing on case studies of activists in Cameroon, Colombia, and Myanmar, this TraCe policy brief aims to (1) outline the challenges posed by increasing digital violence against activists and (2) identify how policymakers worldwide might respond to this issue.

by Laura Gianna Guntrum and Christian Reuter

An overview of ICT-enabled activism

From the early 2010s onwards, ICTs played an increasingly prominent role during large-scale protests in the MENA region.¹ Multiple cases worldwide demonstrate how social activists use ICTs to rapidly exchange information, including security protocols, coordinate protests, and garner international attention.² This TraCe policy brief draws on insights from qualitative interviews conducted with 16 anti-military activists in Myanmar (2021), 14 peacebuilding activists in Cameroon (2023)³, and 37 environmental defenders in Colombia (2023)⁴. In Myanmar, following the 2021 military coup, activists believed the country was not receiving sufficient global attention and thus turned to ICTs to mobilize support.⁵ Generally, ICTs have the potential to lower communication costs, reshape the availability of information sources, provide alternatives to mainstream media through crowd-sourcing initiatives, and democratize participation.⁶ They can also reduce disparities between opposing factions and mitigate barriers to participation.⁷

Although ICTs benefit protest activities and activists, they also present challenges requiring more attention.

Challenges of using ICTs for activism

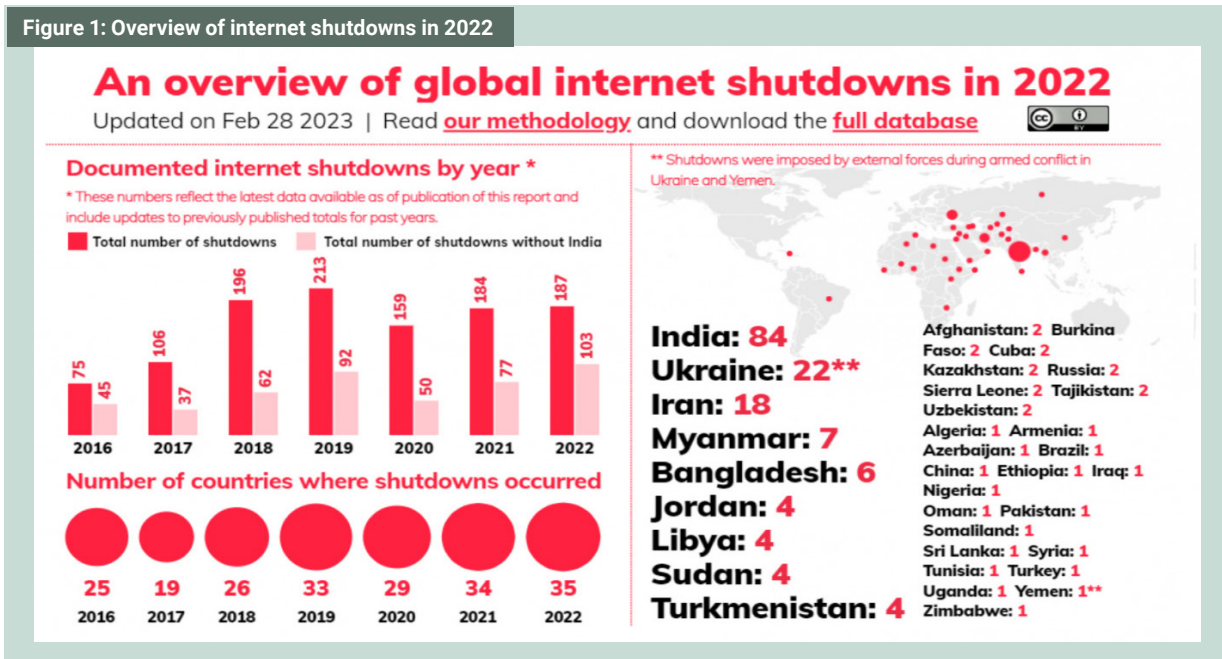
Activists face many challenges when using ICTs for their activities, including increasing digital violence. It is important to recognize that, similar to the concept of *violence*⁸, which is scientifically complex and interpreted differently across various research frameworks, there are also diverse definitions of *digital violence* and a lack of consensus. However, we aim to provide an exploratory definition illustrating just one of the many possible interpretations (see info box 1).

Digital Violence

Digital violence refers to intentional actions in the digital realm that cause harm to individuals or their belongings, whether physical, psychological, or reputational. Examples of digital violence include hate speech and cyberstalking, both of which can have tangible effects, particularly by causing psychological distress.⁹

Our interviews show that digital violence often affects particularly prominent activists but also, more broadly, those campaigning on supposedly “polarizing” issues, such as environmental problems in North Colombia’s extractivist regions. All activists interviewed reported experiencing hate speech and violent messages, including direct threats, death threats, extortion, and threats against family members. The complexity of conflict-affected contexts, such as Colombia, involving numerous actors (e.g., paramilitary, multinational companies) with varying interests and capabilities, often makes it challenging to identify the perpetrators. Interviews conducted with human rights and environmental defenders in North Colombia and Cameroon underscore the pervasive occurrence of digital violence, with indigenous, black, and female activists being disproportionately affected.¹⁰ This demonstrates that discrimination is not limited to the “real” analog world but is also prevalent in the digital space, with similar patterns evident in both online and offline environments. Our research finds that violence can happen independently in the physical or digital world but is often intertwined and/or spills over from one sphere to the other. Additionally, technology can sometimes facilitate physical violence, such as when activists are targeted through location surveillance.

Figure 1: Overview of internet shutdowns in 2022



Source: Rosson et al. (2023).¹⁴

Besides direct threats, political unrest often sees the proliferation of propaganda. In conflict, this can take various forms, including biased information disseminated to influence public opinion, manipulate perceptions, or advance a particular agenda. It can be used by different conflict parties to sway sentiment, justify actions, or demonize opponents. For instance, especially in times of conflict, propaganda might be employed to portray one side as heroic and virtuous while depicting the opposing side as villainous or deceitful, thereby shaping public perception and garnering support for specific ideologies or action.¹¹ In Myanmar, for example, the military made extensive use of digital platforms, including TikTok, to disseminate online propaganda to boost troop morale and intimidate activists by posting threatening videos online.

At a higher level, activists often encounter social media blockades and internet shutdowns, especially in times of protest. These restrictions are frequently imposed by entities such as the government or military bodies to limit ongoing activities, censor online content, and exert control over the digital realm.¹² Following the coup in Myanmar in 2021, the country witnessed internet shutdowns, limited access to whitelisted websites and online services only, and the enforcement of a new Cybersecurity Law.¹³ The latter penalizes the use of virtual private networks (VPNs), which are crucial for accessing blocked applications such as Facebook – a platform of great importance for Myanmar’s activists. Similarly, in Cameroon’s ongoing Anglophone separatist conflict, frequent internet shutdowns disrupt communication channels

and impede individuals from engaging in peacebuilding efforts through digital means. In 2022 alone, Access Now’s Shutdown Tracker Optimization Project (STOP), in partnership with the #KeepItOn coalition, documented 187 internet shutdowns across 35 countries.

As depicted in Figure 1, internet shutdowns are frequently observed in countries experiencing democratic backsliding or in (semi-)authoritarian states. Many of these countries also face terrorism and extremist groups that might exploit ICTs for their own purposes. While some may argue that controlling extremist content may be necessary in such contexts, blanket shutdowns silence all users, not just those spreading harmful content.

Activists are also contending with growing digital surveillance, exemplified by technologies like Pegasus spyware.¹⁵ Governments or other entities may monitor activists’ online activities to track their movements, communications, and associations. This surveillance can restrict their ability to organize protests, communicate with supporters, or engage in other activities without fear of reprisal. Moreover, surveillance data collected on activists can be used to justify legal or political repression, including arbitrary arrests, detention, or even physical violence.

Why we need to be concerned

Contemporary activism relies heavily on ICTs owing to their myriad advantages, including amplifying voices and providing real-time updates. However, there is a clear global trend of escalating digital violence¹⁶, aiming to

cancel supposedly critical voices and restrict activities that could incite uprisings and change. In response, some activists choose to disengage from social networks due to emotional distress and legal repercussions, leading, in some cases, to reduced participation. Disengagement and self-censorship are often what attackers seek to achieve through their acts of violence, leading to a shrinking space for engagement. While some activists consciously withdraw, others report incidents to official institutions for (legal) support, continue to mobilize for resistance, and advocate for their causes. Our interviews show that some activists have developed strategies to counter digital violence. These strategies vary widely depending on several factors, including technical expertise, emotional well-being, support networks, financial resources, and time.

Overall, everyone, including policymakers worldwide, should be concerned about the shrinking online spaces and rising digital violence that affect activists worldwide. This violence often leads to reduced political engagement in both digital and physical realms as the boundaries between these forms of violence blur. It is essential to enable activists to participate in political and socio-cultural discussions without facing censorship, internet shutdowns, or direct threats. When activists are silenced, ruling entities like military or (semi-)authoritarian governments can spread one-sided information. As activists increasingly withdraw due to the violence they experience, the foundations of democratic and peaceful spaces are threatened.

Although our examples mainly relate to Myanmar, Cameroon, and Colombia, similar phenomena can and have been observed worldwide. More systematic research into cases of digital violence would deepen our understanding of the phenomenon in all its aspects.

Reflections on what could be done

Acknowledging the complexity of making specific recommendations is important, given the diverse and unique contexts in which activists operate. Further, it is crucial to tailor actions and projects to local needs and circumstances. With this in mind, this policy brief outlines a few considerations that could enhance the protection and support of activists and organizations enabling them to continue their activities:

(1) Enhancing digital infrastructure:

Ensuring equitable access to digital infrastructure is vital for reducing discriminatory practices and promoting universal accessibility. For instance, activists in areas with limited power supply and internet access may resort to unencrypted phone calls, exposing them to poten-

tial interception and surveillance. Conversely, a reliable internet connection enables the use of encrypted communication services (e.g., via messenger calls), providing better protection. Access to robust infrastructure is indispensable for safeguarding individuals' privacy and security in today's digital age. Overall, allocating more financial resources to developing and enhancing digital infrastructures could effectively reduce disparities in access.

(2) Building resilience and learning how to handle instances of digital violence:

Besides focusing on more technical solutions, it is paramount to prioritize strengthening the resilience of activists and organizations that work with them. In the future, more attention could be paid to supporting local organizations working on digital rights, digital literacy, and digital security training so that they can independently run workshops for activists for instance. Such workshops may help activists to identify potential threats and vulnerabilities and equip them with the knowledge and skills they need to (better) navigate the digital landscape securely.

(3) Highlighting unacceptable incidents of digital violence and taking a stand:

It is essential to develop strategies to bolster support for activists and hold the entities responsible for perpetrating digital violence accountable. When perpetrators are identified, publicly disclosing their identities and enforcing consequences for their actions is critical for this accountability. This approach raises awareness and signals strong commitment to combatting digital violence and upholding human rights principles in the digital sphere. By addressing digital violence and technology-facilitated oppression, policymakers and other relevant stakeholders can reaffirm their commitment to principles such as freedom of expression, privacy, and non-discrimination in the digital age. By consistently highlighting instances of digital violence, they can increase awareness of the prevalence and impact of such behavior. This awareness-raising is essential for mobilizing public support and galvanizing action to address digital violence effectively. Publicly acknowledging incidents of digital violence sends a powerful message of solidarity and support to the activists affected. It demonstrates that their experiences are taken seriously and that they are not alone in facing such challenges. Another important measure is advocating for national and international laws to address digital violence and expanding and strengthening existing legal frameworks.

(4) Understanding the preferences of activists:

Better understanding the (technical) needs and wishes of activists affected by digital violence is essential for

several reasons. First, it allows support and resources to be tailored to their specific needs, ensuring effective and relevant interventions. By listening to activists and gaining insight into their (technical) challenges and preferences, targeted solutions can be developed that address their concerns and enhance their digital security. Further, adapting projects and technical developments based on activists' input is essential for promoting user-centric design. Rather than imposing solutions from the top down, engaging with activists facilitates cocreation of interventions that are responsive to their lived experiences. This approach fosters a sense of ownership and empowerment among activists, as they are directly involved in shaping the tools and strategies designed to support them. Support might involve funding initiatives that prioritize the technical needs identified by activists, supporting capacity-building efforts to enhance digital literacy and security skills, or collaborating with grassroots organizations to develop tailored solutions. By placing the voices and experiences of activists at the center of the design and implementation of projects, policymakers and other relevant stakeholders may better support their efforts to navigate and resist digital violence.

Text License: Creative Commons (Attribution/No Derivatives/4.0 International). The images used are subject to their own licenses.

DOI: 10.48809/PRIFTraCePB2404



Authors

Laura Gianna Guntrum (she/her) is a research associate at Science and Technology for Peace and Security (PEASEC) in the Department of Computer Science at the Technical University of Darmstadt. For TraCe, she is currently focusing on how technology might change political violence. Her research interests include the use of ICTs in protest movements and peacebuilding. Contact: guntrum@peasec.tu-darmstadt.de

Christian Reuter is a professor and Dean of the Department of Computer Science at the Technical University of Darmstadt and a TraCe principal investigator. His chair (PEASEC) combines computer science with peace and security research. He holds doctoral degrees in information systems and security policy. Contact: reuter@peasec.tu-darmstadt.de

Acknowledgements

The authors would like to thank all interviewees for their important insights. Additionally, we are deeply appreciative of everyone who played a part in facilitating and conducting the interviews: **Verena Lasso Mena** in the case of Colombia and **Emile Sunjo** and **Lynn Cockburn** for their contributions in Cameroon. Their support and assistance were of the utmost importance.

About TraCe

What effects do global developments such as technologization and climate change have on political violence? How can political violence be limited or legitimized by international institutions? How is it interpreted and conceptualized? Since April 2022, these questions are addressed by the BMBF-funded regional research center "Transformations of Political Violence" (TraCe), in which five Hessian research institutions work together with a variety of disciplinary perspectives.

More information: www.trace-center.de/en // www.linkedin.com/company/trace-violence // bsky.app/profile/trace-center.de

V.i.S.d.P. & Layout: Tina Cramer, Press and Public Relations (PRIF/TraCe), Baseler Straße 27–31, Frankfurt a. M., Germany, trace-transfer@prif.org Phone (069) 959104-0, Design: Anja Feix

This policy brief was written as part of the research project 'Regional Research Center Transformations of Political Violence' [01UG2203E], funded by the Federal Ministry of Education and Research (BMBF).

References and Further Reading

- ¹ Al-Ani, B., Mark, G., Chung, J., and Jones, J. (2012) 'The Egyptian Blogosphere: A Counter-Narrative of the Revolution', in Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work. New York, NY, USA: Association for Computing Machinery (CSCW '12), pp. 17–26. doi: 10.1145/2145204.2145213.
- ² Shklovski, I. and Wulf, V. (2018) 'The use of private mobile phones at war: Accounts from the Donbas conflict', Conference on Human Factors in Computing Systems - Proceedings, 2018-April, pp. 1–13. doi: 10.1145/3173574.3173960.
El-Nawawy, M. and Khamis, S. (2012) 'Political Activism 2.0: Comparing the Role of Social Media in Egypt's "Facebook Revolution" and Iran's "Twitter Uprising"', Online Journal of the Virtual Middle East, 6(1), pp. 8–33.
- ³ Work in progress: Guntrum, L., Cockburn, L., Sunjo, E., and Nganji, J. 'Including Perspectives of Women Using ICTs to Promote Peace in the Anglophone Cameroon Separist War'.
- ⁴ Work in progress: Guntrum, L. and Lasso Mena, V. 'Unmasking Digital Violence in the Pursuit of Human Rights and Environmental Defense in La Guajira and Cesar, North Colombia'.
- ⁵ Guntrum, L. G. (2024) 'Keyboard Fighters: The Use of ICTs by Activist in Times of Military Coup in Myanmar', in Proceedings of the Conference on Human Factors in Computing Systems. Honolulu, HI, USA: ACM New York, NY, USA, p. 19. doi: 10.1145/3613904.3642279.
- ⁶ Zeitzoff, T. (2017) 'How Social Media Is Changing Conflict', Journal of Conflict Resolution, 9(61), pp. 1970–91.
- ⁷ Valenzuela, S., Somma, N. M., Scherman, A., and Arriagada, A. (2016) 'Social media in Latin America: Deepening or bridging gaps in protest participation?', Online Information Review, 40(5), pp. 695–711.
- ⁸ Imbusch, P. (2003) 'Gewalt verstehen - Einige konzeptionelle Überlegungen Public Health Forum', 11(2), pp. 2–3. <https://doi.org/10.1515/pubhef-2003-1959>
- ⁹ Lumsden, K. and Harmer, E. (2019) Online Othering. Exploring Digital Violence and Discrimination on the Web. 1st edn. Palgrave Macmillan. doi: 10.4324/9781003200871-49.
Martínez, M. H. (2020) 'Feminist cyber-resistance to digital violence: Surviving gamergate', Revista de cultura, poder i societat, 5, pp. 287–302.
- ¹⁰ Amnesty International (2018) 'Women abused on Twitter every 30 seconds -new study', available at: <https://www.amnesty.org.uk/press-releases/women-abused-twitter-every-30-seconds-new-study>.
- ¹¹ Kyaw, N. N. (2021) 'Social media, hate speech and fake news during Myanmar's political transition', in: From Grassroots Activism to Disinformation: Social Media in Southeast Asia, pp. 86–104.
- ¹² Pallin, C. V. (2017) 'Internet control through ownership: the case of Russia', Post-Soviet Affairs, 33(1), pp. 16–33. doi: 10.1080/1060586X.2015.1121712.
Daffalla, A., Simko, L., Kohno, T., and Bardas, A.G. (2021) 'Defensive Technology Use by Political Activists During the Sudanese Revolution', IEEE Symposium on Security and Privacy, pp. 945–63.
- ¹³ Smith, R. and Smith, N. (2022) 'Use and Abuse of Social Media in Myanmar between 2010 and 2022', Athens Journal of Law, 8(3), pp. 309–28. <https://doi.org/10.30958/ajl.8-3-5>
- ¹⁴ Rosson, Z., Anthonio, F., and Tackett, C. (2023) 'Weapons of Control, Shields of Impunity: Internet Shutdowns in 2022', available at: <https://www.accessnow.org/wp-content/uploads/2023/05/2022-KIO-Report-final.pdf>
- ¹⁵ Daffalla, A. et al. (2021) 'Defensive Technology Use by Political Activists During the Sudanese Revolution', IEEE Symposium on Security and Privacy, pp. 945–63.
- ¹⁶ Bailey, J., Henry, N., and Flynn, A. (2021), 'Technology-Facilitated Violence and Abuse: International Perspectives and Experiences', in: Bailey, J., Flynn, A., and Henry, N. (eds.) The Emerald International Handbook of Technology-Facilitated Violence and Abuse (Emerald Studies In Digital Crime, Technology and Social Harms), Leeds: Emerald Publishing Limited, pp. 1–17.

SPONSORED BY THE



Federal Ministry
of Education
and Research

