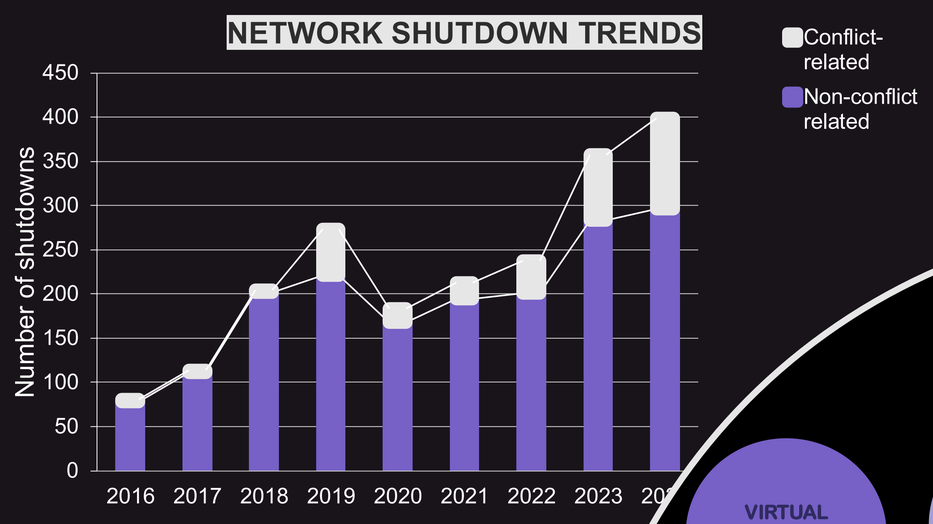
FROM SATELLITES TO SIMS: A LAYERED TAXONOMY OF NETWORK SHUTDOWN CIRCUMVENTION TECHNOLOGIES USED IN ADVERSARIAL SETTINGS

Ammara Yasin, Anna Maria Mandalari, Volker Stocker

University College London, Weizenbaum Institute for the Networked Society

BACKGROUND AND GOALS

- The weaponization of network shutdowns has reached unprecedented levels: 2024 marked **a historic peak of 296 documented incidents, 103 of which were conflict-related, more than doubling since 2022**.
- In conflict zones (e.g., Russia/Ukraine, Palestine/Israel), shutdowns are no longer ancillary disruptions but central to military strategy: fibre optic cables are severed, ISP offices seized, satellite terminals disabled, and infrastructure destroyed. (Access Now, 2023).
- The use of widely-adopted circumvention tools like VPNs and mesh networks overlooks critical risks. **The same technologies that circumvent shutdowns often expose users to surveillance, retaliation, or physical harm.**



WHAT IS A NETWORK SHUTDOWN?

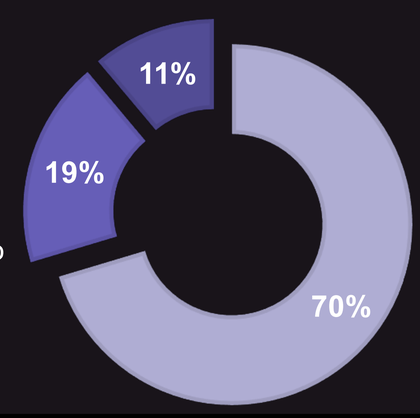
We follow Access Now (2023b) and Rydzak (2020), in defining 'network shutdown' as a **deliberate, politically-motivated disruption of entire channels of electronic communication within a given geographical area and/or affecting a predetermined group of citizens.**

This does **not** include reactive social media bans, suspension of fixed and mobile telephone services, deliberate slowdowns etc., and only considers complete shutdowns of Internet connectivity.

HOW IS A SHUTDOWN IMPLEMENTED?

We drew upon Access Now's (2022) taxonomy of technologies behind a shutdown, cross-referenced these with the literature collected, mapped all 27 papers to an implementation method.

We found that 70% of shutdowns were implemented through a **manipulation of network routing**, 19% through **physical damage to communications infrastructure** and 11% through a specific form of **throttling** which makes it appear as though internet access is available, but the level of interference is enough to make the service or resource effectively useless.

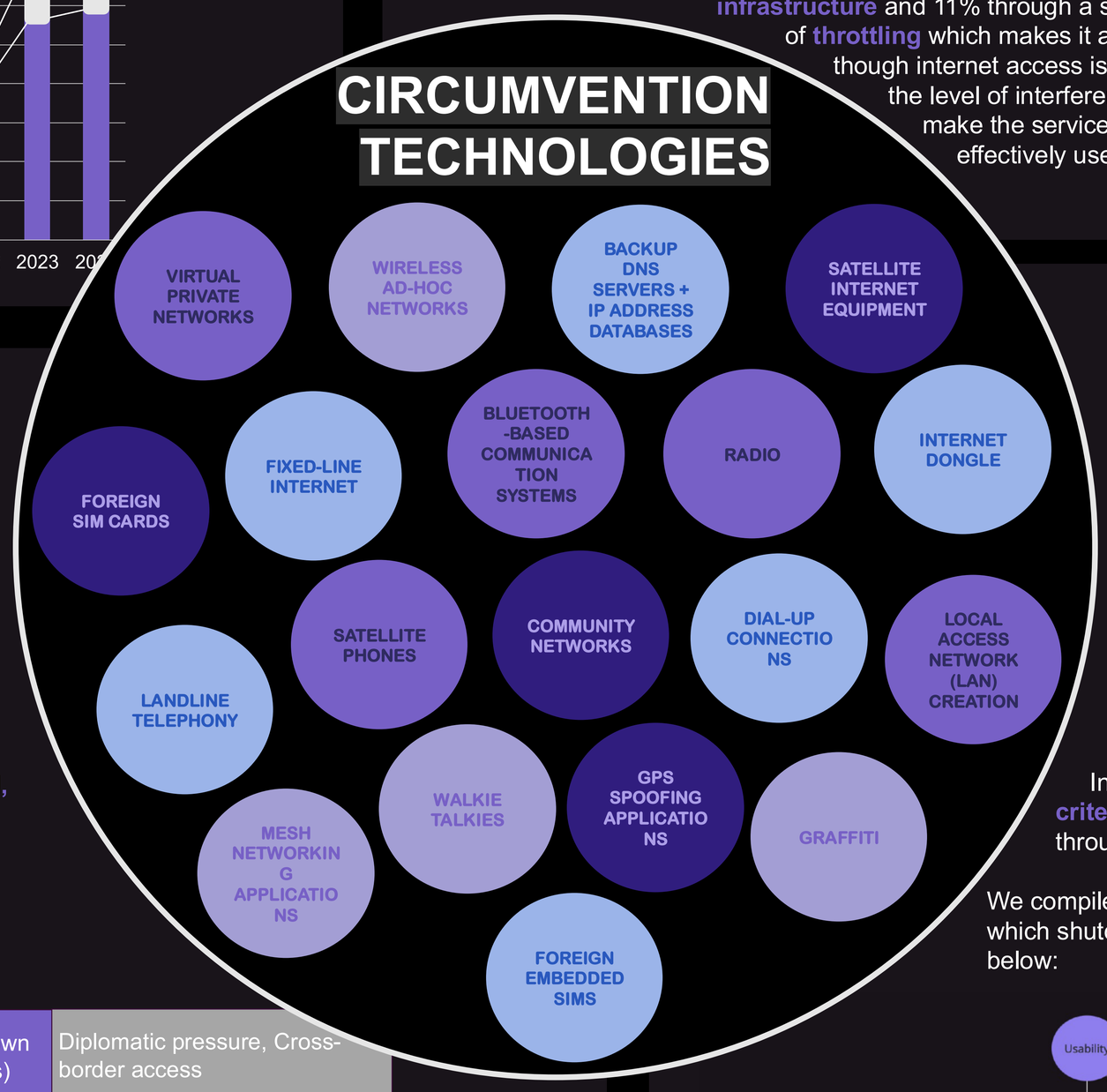


A MULTI-LAYERED ECOSYSTEM

- This taxonomy adapts and extends the **layered model** proposed by Lehr et. al (2019) for the internet ecosystem
- We recontextualise it to analyse both **network shutdown mechanisms** and **circumvention strategies**.
- Traditional models focus solely on technical infrastructure, but this framework incorporates **political, legal, and socio-technical dimensions**, reflecting the complexities that exist within a network shutdown.

The draft model below places shutdown dimensions on the left and circumvention strategies on the right:

Political and Legal (shutdown orders, surveillance laws)	Diplomatic pressure, Cross-border access
Transport and Protocols	VPNs, VPSs, Proxy severs, GPS spoofing
Content and Applications	Mesh messaging, Low-technology methods
Network Management (IP blocking, DNS spoofing, BGP hijacking)	Foreign SIM cards, embedded SIM cards, DNS servers
Physical Infrastructure (telecommunication towers, satellite infrastructure, etc.)	Alternative infrastructure

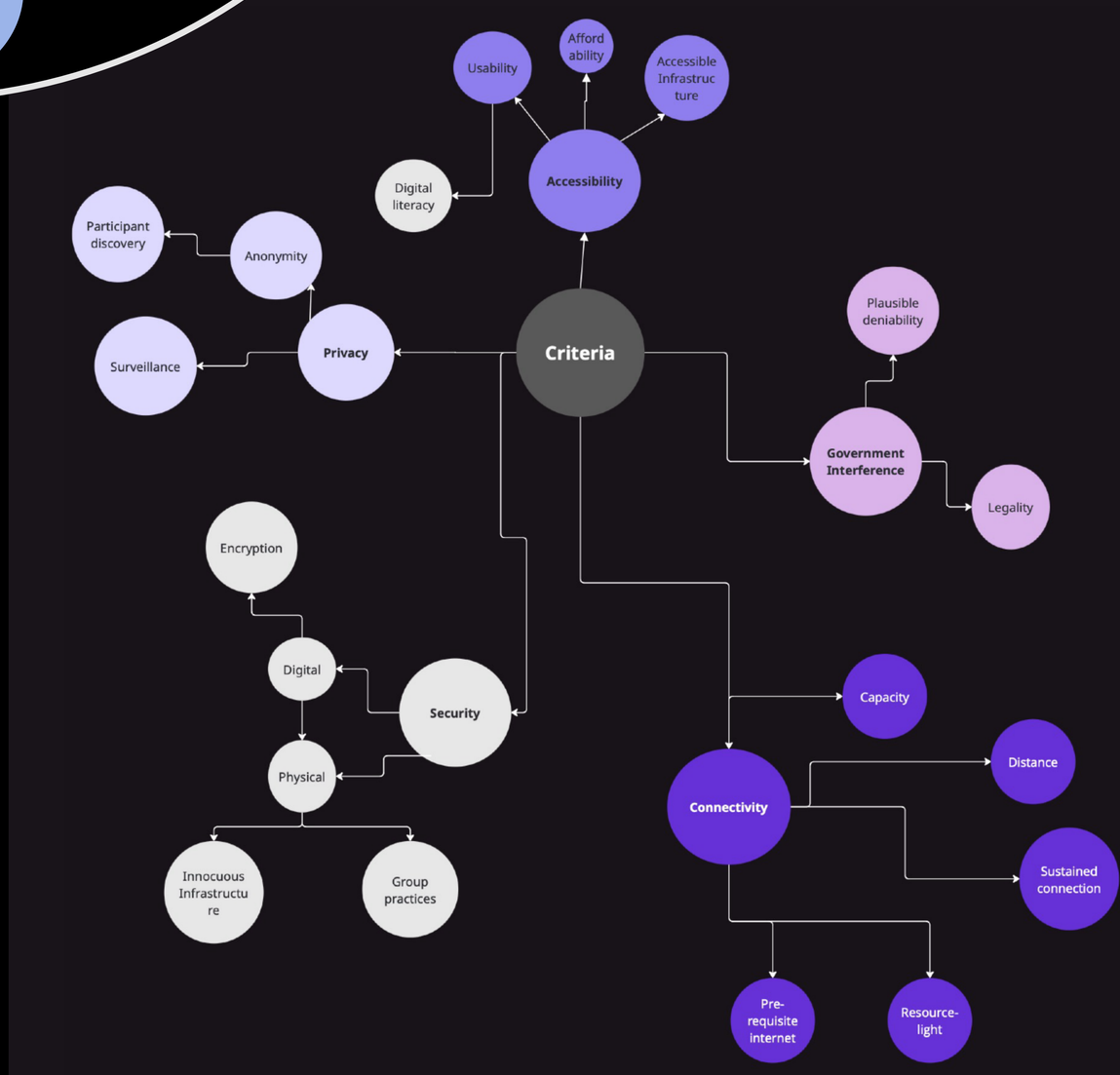


CRITERIA

- An important facet of this research is the emphasis that these circumvention technologies **must have an aim beyond simply regaining connectivity.**
- In situations of protest or conflict, one can argue that forcibly reconnecting to the network without consideration of and resilience to the **specific security and privacy concerns of each context**, including the monitoring or surveillance of users, can pose a greater threat than that posed by disconnection alone.

In that vein, this research extracts a set of **criteria by which to assess each technology,** through a system of coding.

We compile the technical, social and political contexts into which shutdowns are introduced. A draft of these criteria is below:



REFERENCES

Access Now (2022) *A taxonomy of internet shutdowns: the technologies behind network interference*. Available at: https://www.accessnow.org/wp-content/uploads/2022/06/A-taxonomy-of-internet-shutdowns-the-technologies-behind-network-interference.pdf [Accessed 28 January 2025].

Access Now (2023) *Shrinking democracy, growing violence: internet shutdowns in 2023*. Available at: https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf [Accessed 12 July 2024].

Lehr, W., Clark, D. and Bauer, S. (2019) 'Regulation when platforms are layered', *International Telecommunications Society (ITS)*. Available at: https://www.econstor.eu/handle/10419/205193[Accessed 10 April 2025].

Rydzak, J., Karanja, M. and Opiyo, N. (2020) 'Dissent does not die in darkness: network shutdowns and collective action in African countries', *International Journal of Communication*, 14(0), p. 24.

E:ammara.yasin.22@ucl.ac.uk E: anna.mandalari@ucl.ac.uk E: volker.stocker@weizenbaum-institut.de

University College London, Roberts Building - Department of Electronic & Electrical Engineering, 1108 Torrington Place, London, WC1E 7JE, United Kingdom