

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

As network shutdowns become increasingly prevalent -with 283 shutdowns in 2023 marking the highest number of shutdown incidents in a single year- their use as weapons to quell protest and within inter-country conflicts (see Russia/Ukraine and Palestine/Israel) is also increasing, emphasising **that the need for resilient communication solutions is more critical than ever** (Access Now, 2023).

There is a history of affected populations using the tools at their disposal to circumvent these shutdowns, but a comprehensive study of the **security and privacy** implications of these does not yet exist. The goals of this paper are as follows:

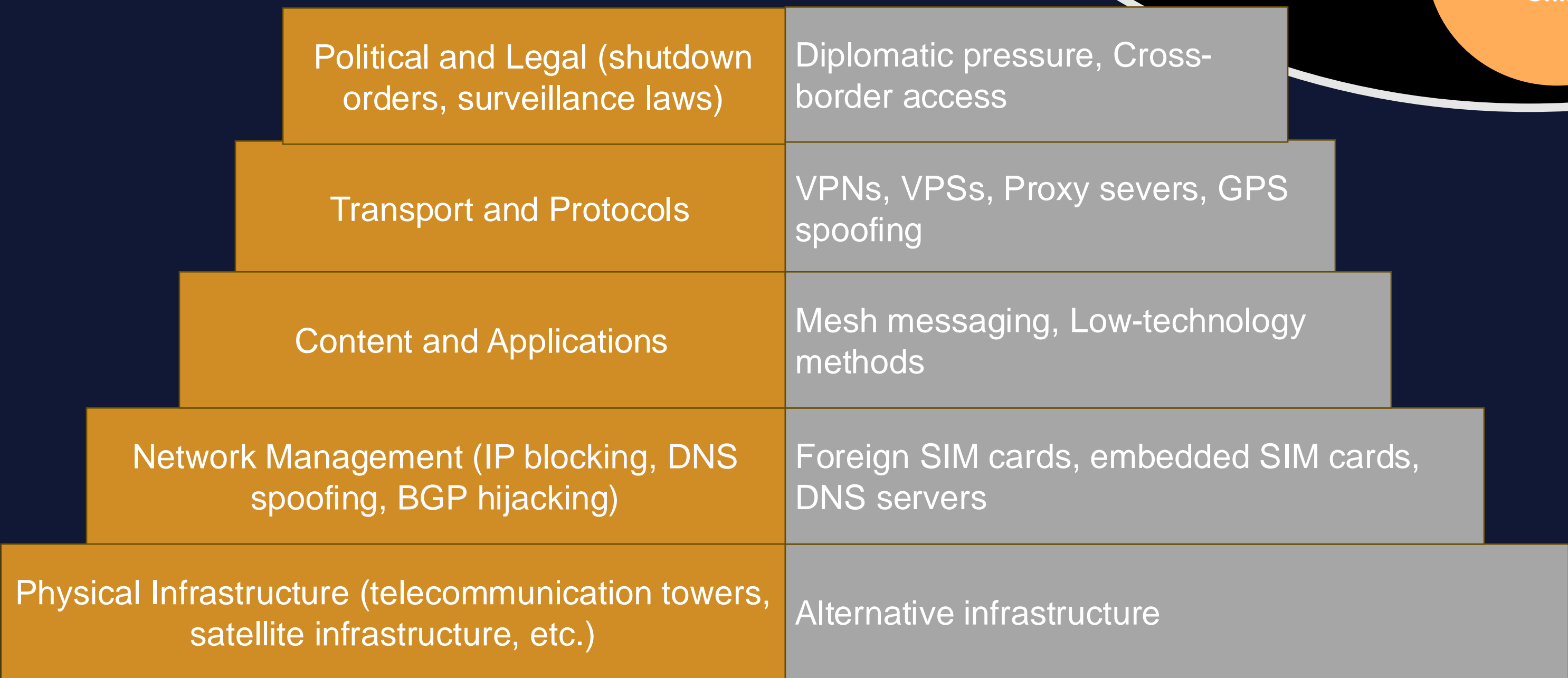
- 1 To systematically extract and classify existing circumvention technologies
- 2 To critically assess the effectiveness of these technologies in adversarial settings, identifying user safety implications
- 3 To investigate the socio-political and infrastructural factors that shape the operational success of these technologies in adversarial settings

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**.

Unlike traditional models that focus solely on technical infrastructure, 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:



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.

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, and only considers complete shutdowns of Internet connectivity.

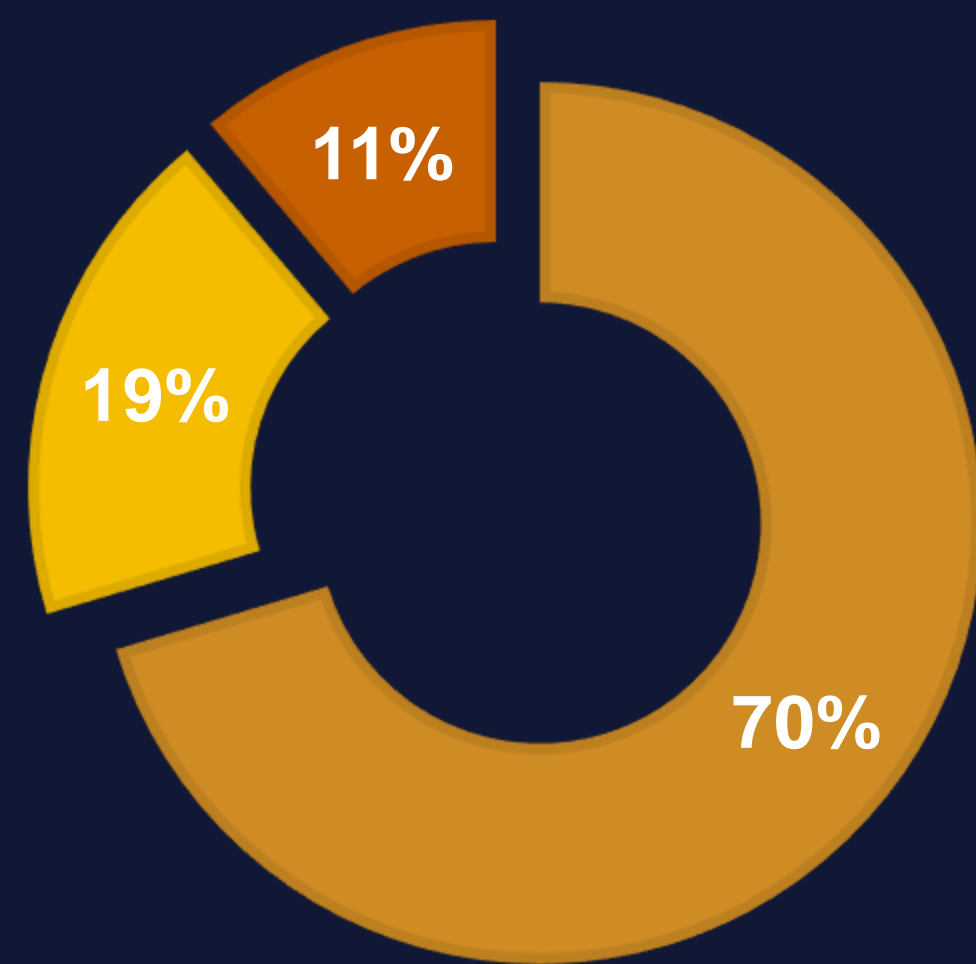
HOW IS A SHUTDOWN IMPLEMENTED?

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.

SHUTDOWN IMPLEMENTATION METHODS

- Routing
- Fundamental Infrastructure Shutdown
- Rogue Infrastructure Attack



CIRCUMVENTION TECHNOLOGIES



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:



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

As network shutdowns become increasingly prevalent -with 283 shutdowns in 2023 marking the highest number of shutdown incidents in a single year- their use as weapons to quell protest and within inter-country conflicts (see Russia/Ukraine and Palestine/Israel) is also increasing, emphasising **that the need for resilient communication solutions is more critical than ever** (Access Now, 2023).

There is a history of affected populations using the tools at their disposal to circumvent these shutdowns, but a comprehensive study of the **security and privacy** implications of these does not yet exist. The goals of this paper are as follows:

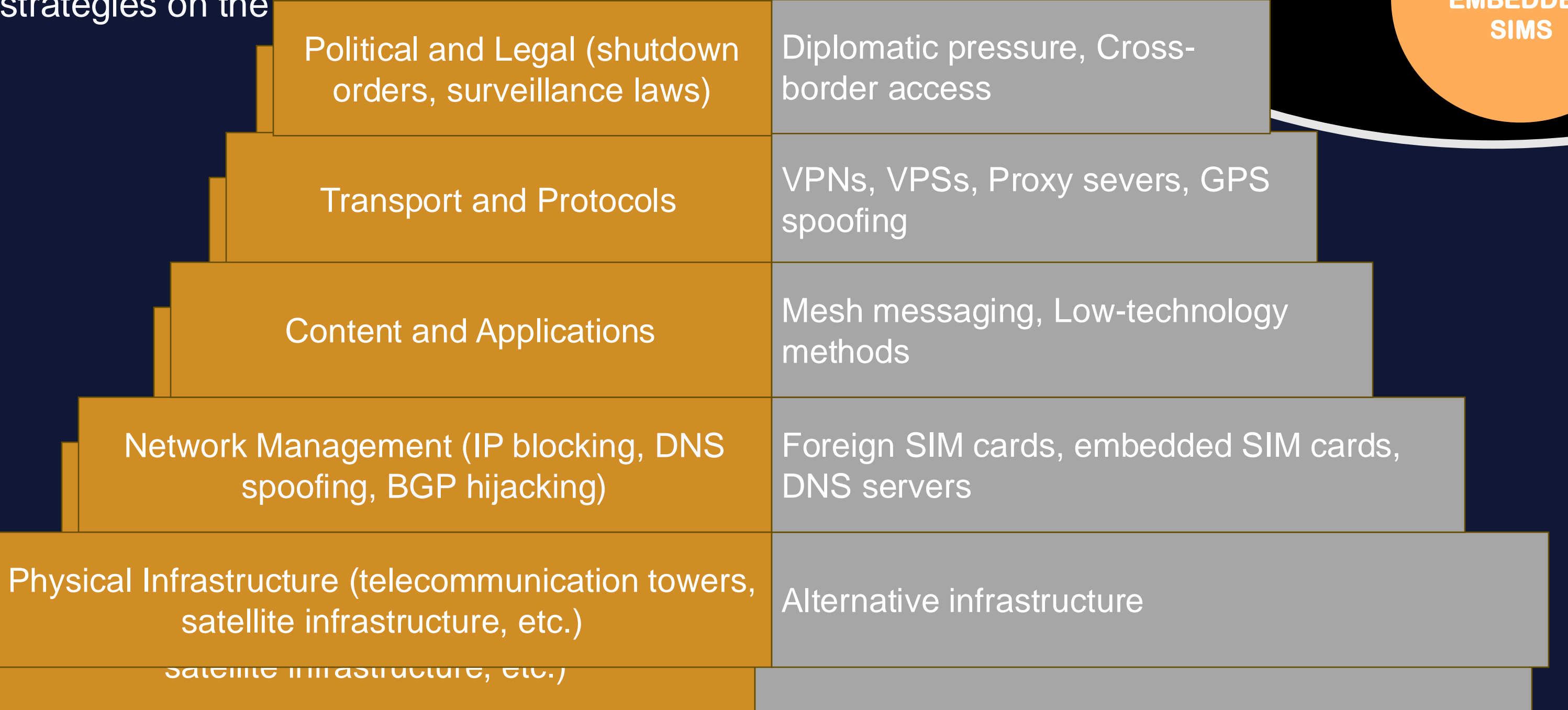
- 1 To systematically extract and classify existing circumvention technologies
- 2 To critically assess the effectiveness of these technologies in adversarial settings, identifying user safety implications
- 3 To investigate the socio-political and infrastructural factors that shape the operational success of these technologies in adversarial settings

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**.

Unlike traditional models that focus solely on technical infrastructure, 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:



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.

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, and only considers complete shutdowns of Internet connectivity.

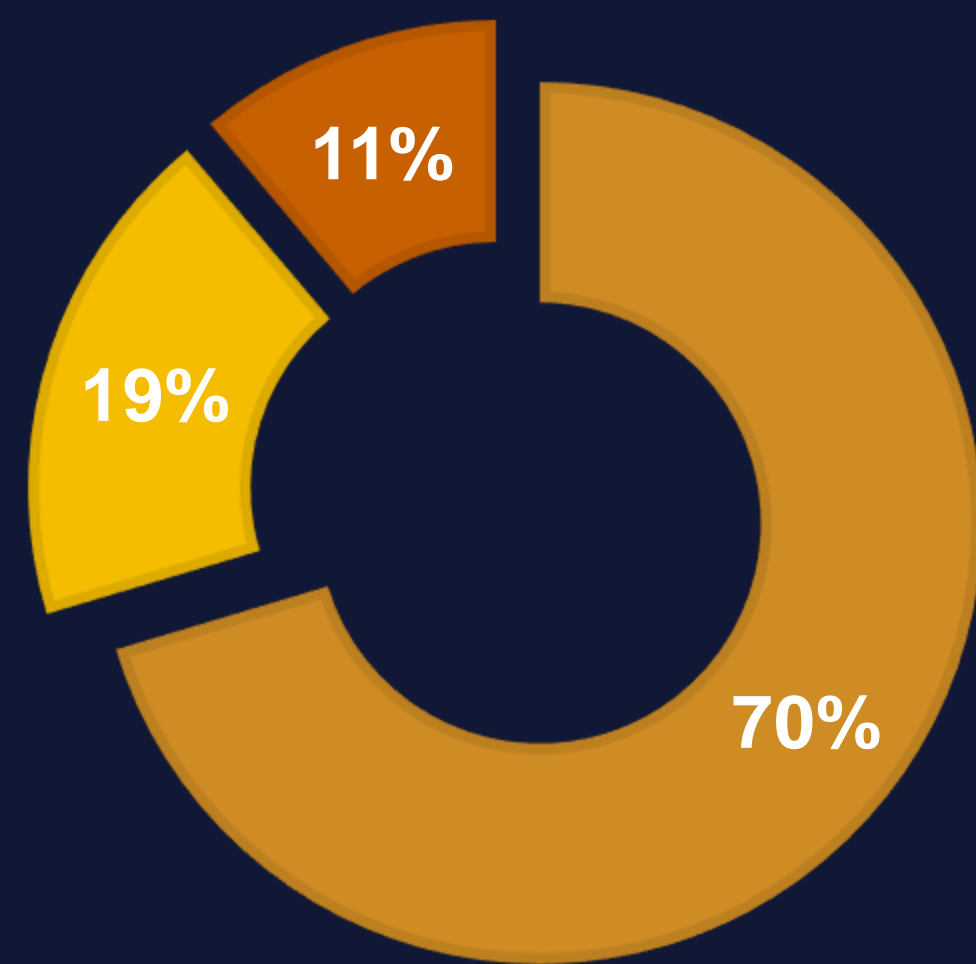
HOW IS A SHUTDOWN IMPLEMENTED?

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.

SHUTDOWN IMPLEMENTATION METHODS

- Routing
- Fundamental Infrastructure Shutdown
- Rogue Infrastructure Attack



CIRCUMVENTION TECHNOLOGIES

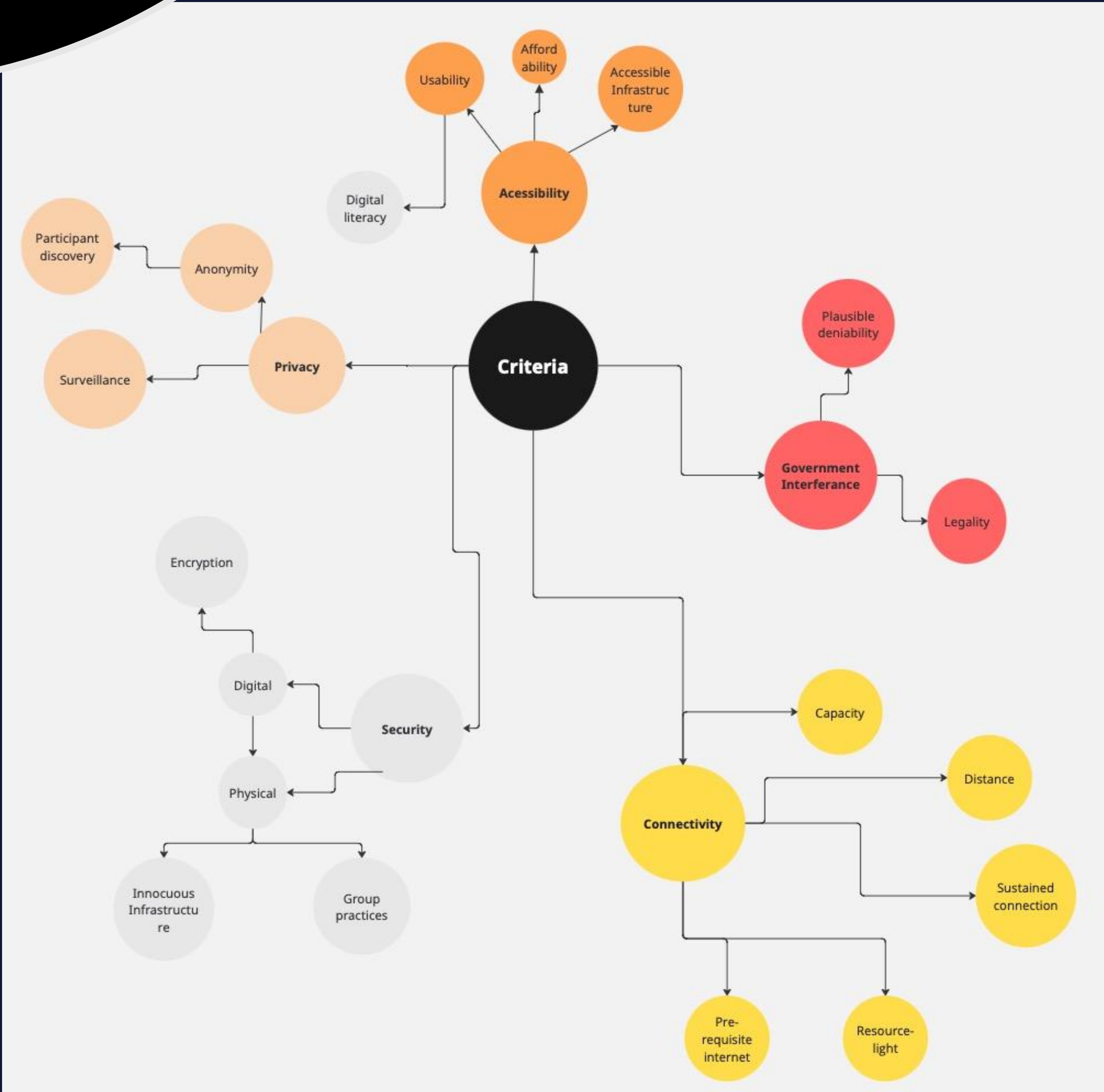


CRITERIA

- 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:



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



Abstract

Network shutdowns are a common tool used by governments to suppress dissent and control information flow. This paper presents a layered taxonomy of network shutdown circumvention technologies, ranging from satellite-based systems to SIM-based solutions. The taxonomy is structured into three layers: the first layer focuses on the underlying technology, the second layer on the specific circumvention method, and the third layer on the user interface and deployment. The paper also discusses the challenges and opportunities associated with these technologies in adversarial settings.

1. Introduction

Network shutdowns have become a widespread phenomenon in many countries, particularly in the Middle East and Africa. Governments use various techniques to block access to the internet, including blocking specific websites, throttling bandwidth, and shutting down entire networks. These shutdowns are often justified as necessary for national security or public order, but they also have significant negative impacts on human rights and economic development.

2. Background

Network shutdowns can be categorized into two main types: targeted shutdowns and blanket shutdowns. Targeted shutdowns involve blocking access to specific websites or services, while blanket shutdowns involve shutting down the entire internet or mobile network. Both types of shutdowns can be circumvented using various technologies, which are the focus of this paper.

3. Layered Taxonomy

The taxonomy is structured into three layers:

- Layer 1: Technology** - This layer focuses on the underlying technology used for circumvention, such as satellite-based systems, SIM-based solutions, and proxy servers.
- Layer 2: Method** - This layer focuses on the specific circumvention method, such as using a satellite-based system to bypass ground-based network restrictions.
- Layer 3: User Interface and Deployment** - This layer focuses on the user interface and deployment of the circumvention technology, such as the ease of use and the ability to be deployed in large-scale operations.

4. Challenges and Opportunities

There are several challenges associated with network shutdown circumvention technologies, including the need for technical expertise, the risk of detection and prosecution, and the potential for misuse. However, there are also opportunities for these technologies to be used for positive purposes, such as providing access to information and services in areas with limited internet access.

5. Conclusion

This paper presents a layered taxonomy of network shutdown circumvention technologies, ranging from satellite-based systems to SIM-based solutions. The taxonomy is structured into three layers: the first layer focuses on the underlying technology, the second layer on the specific circumvention method, and the third layer on the user interface and deployment. The paper also discusses the challenges and opportunities associated with these technologies in adversarial settings.

5.1. Satellite-based systems

Satellite-based systems are a type of network shutdown circumvention technology that uses satellite communication to bypass ground-based network restrictions. These systems are typically used in areas with limited internet access, such as rural areas or disaster zones. They provide a reliable and secure means of communication, but they are also expensive and require specialized equipment.

5.2. SIM-based solutions

SIM-based solutions are a type of network shutdown circumvention technology that uses SIM cards to bypass ground-based network restrictions. These solutions are typically used in areas where mobile network access is available but internet access is blocked. They provide a simple and easy-to-use means of circumventing network shutdowns, but they are also vulnerable to detection and prosecution.

5.3. Proxy servers

Proxy servers are a type of network shutdown circumvention technology that uses a server to act as an intermediary between the user and the internet. These servers are typically used in areas where internet access is available but specific websites or services are blocked. They provide a simple and easy-to-use means of circumventing network shutdowns, but they are also vulnerable to detection and prosecution.

6. Future Work

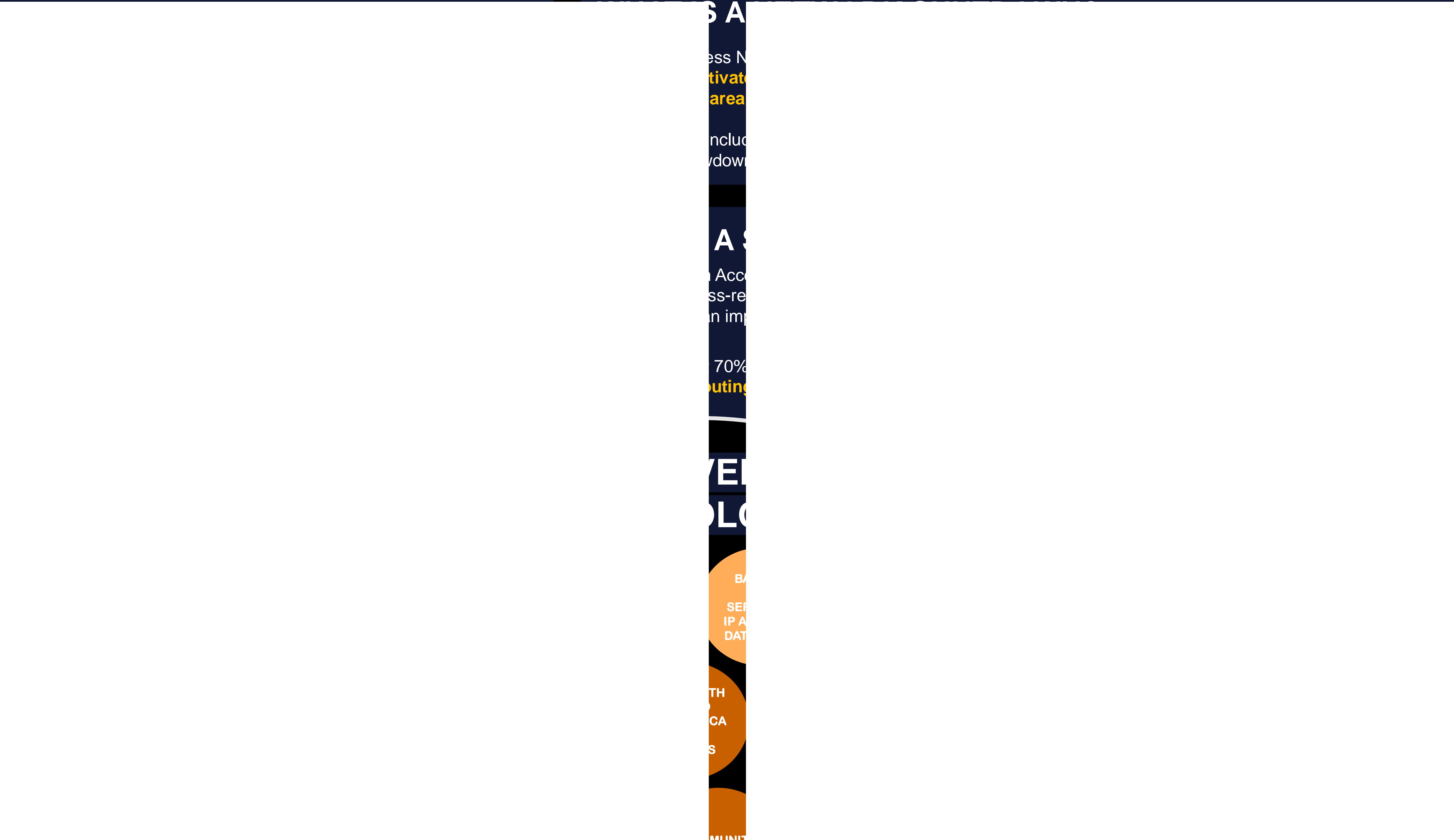
There are several areas for future work in network shutdown circumvention technologies, including the development of more advanced and secure technologies, the improvement of user interfaces and deployment methods, and the exploration of new applications and use cases.

collective action in African countries', *International Journal of Communication*, 14(0), p. 24.

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



We recontextualise it to analyse both **network shutdown mechanisms** and **circumvention strategies**. **privacy concerns of each context**, including the monitoring or surveillance of users, can pose a greater threat than that posed by

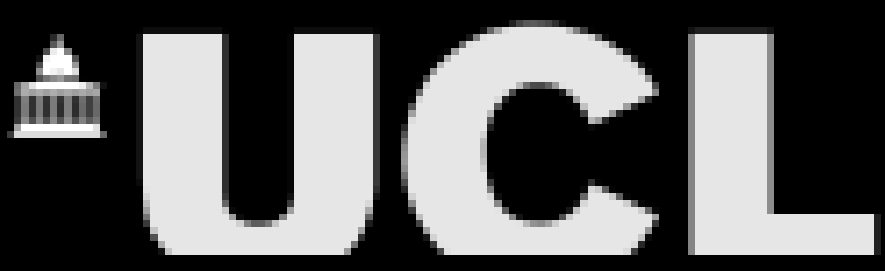


collective action in African countries', *International Journal of Communication*, 14(0), p. 24.

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

Ammara Yasin, Anna Maria Mandalari, Volker Stocker

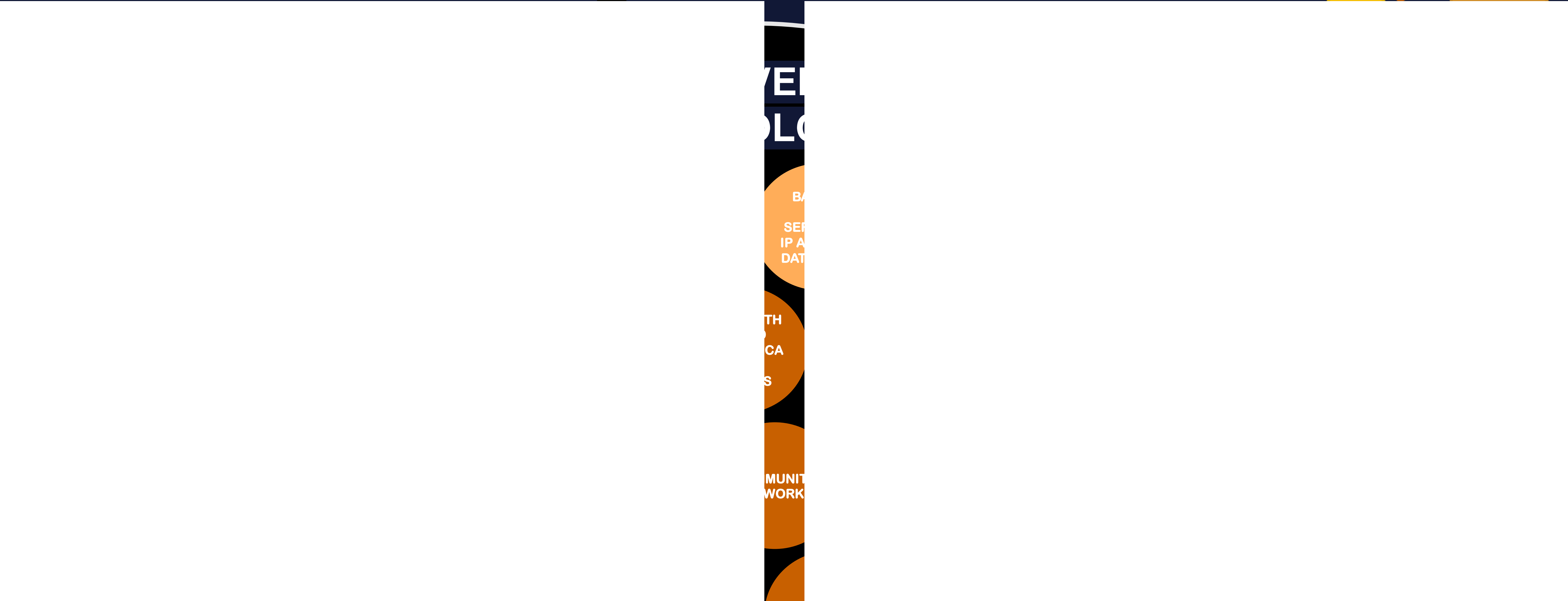
University College London, Weizenbaum Institute for the Networked Society



1 To systematically extract and classify existing circumvention technologies

We found that 70% of shutdowns were implemented through a **manipulation of network routing**, 19% through **physical damage to communications**

11%



technical infrastructure, this framework incorporates political, legal, and socio-technical dimensions, reflecting the complexities that exist

MESH

WALKIE TALKIES

SPOOFING APPLICATIONS

GRAFFITI

criteria by which to assess each technology, through a system of coding



[the-technologies-behind-network-interference.pdf](#) [Accessed 28 January 2025].



collective action in African countries', *International Journal of Communication*, 14(0), p. 24.

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



1 To systematically extract and classify existing circumvention technologies

We found that 70% of shutdowns were implemented through a **manipulation of network routing**, 19% through **physical damage to communications**

11%



collective action in African countries', *International Journal of Communication*, 14(0), p. 24.

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



This taxonomy adapts and extends the **layered model** proposed by Lehr et. al [1]. It is structured into three layers: Physical Infrastructure (telecommunication towers), Network Infrastructure (SIM cards, mobile phones, and network operators), and Application Layer (walkie talkies, spoofing applications, and graffiti). The taxonomy is designed to assess each technology based on its effectiveness, scalability, and the criteria by which to assess each technology, through a system of coding.

- This taxonomy adapts and extends the **layered model** proposed by Lehr et. al [1].

The taxonomy is structured into three layers: Physical Infrastructure (telecommunication towers), Network Infrastructure (SIM cards, mobile phones, and network operators), and Application Layer (walkie talkies, spoofing applications, and graffiti). The taxonomy is designed to assess each technology based on its effectiveness, scalability, and the criteria by which to assess each technology, through a system of coding.

Physical Infrastructure (telecommunication towers)

The taxonomy is structured into three layers: Physical Infrastructure (telecommunication towers), Network Infrastructure (SIM cards, mobile phones, and network operators), and Application Layer (walkie talkies, spoofing applications, and graffiti). The taxonomy is designed to assess each technology based on its effectiveness, scalability, and the criteria by which to assess each technology, through a system of coding.

collective action in African countries', *International Journal of Communication*, 14(0), p. 24.

Click to add title - Arial bold 72pt

A MULTI-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

As network shutdowns become increasingly prevalent -with 283 shutdowns in 2023 marking the highest number of shutdown incidents in a single year- their use as weapons to quell protest and within inter-country conflicts (see Russia/Ukraine and Palestine/Israel) is also increasing, emphasising **that the need for resilient communication solutions is more critical than ever** (Access Now, 2023).

There is a history of affected populations using the tools at their disposal to circumvent these shutdowns, but a comprehensive study of the **security and privacy** implications of these does not yet exist. The goals of this paper are as follows:

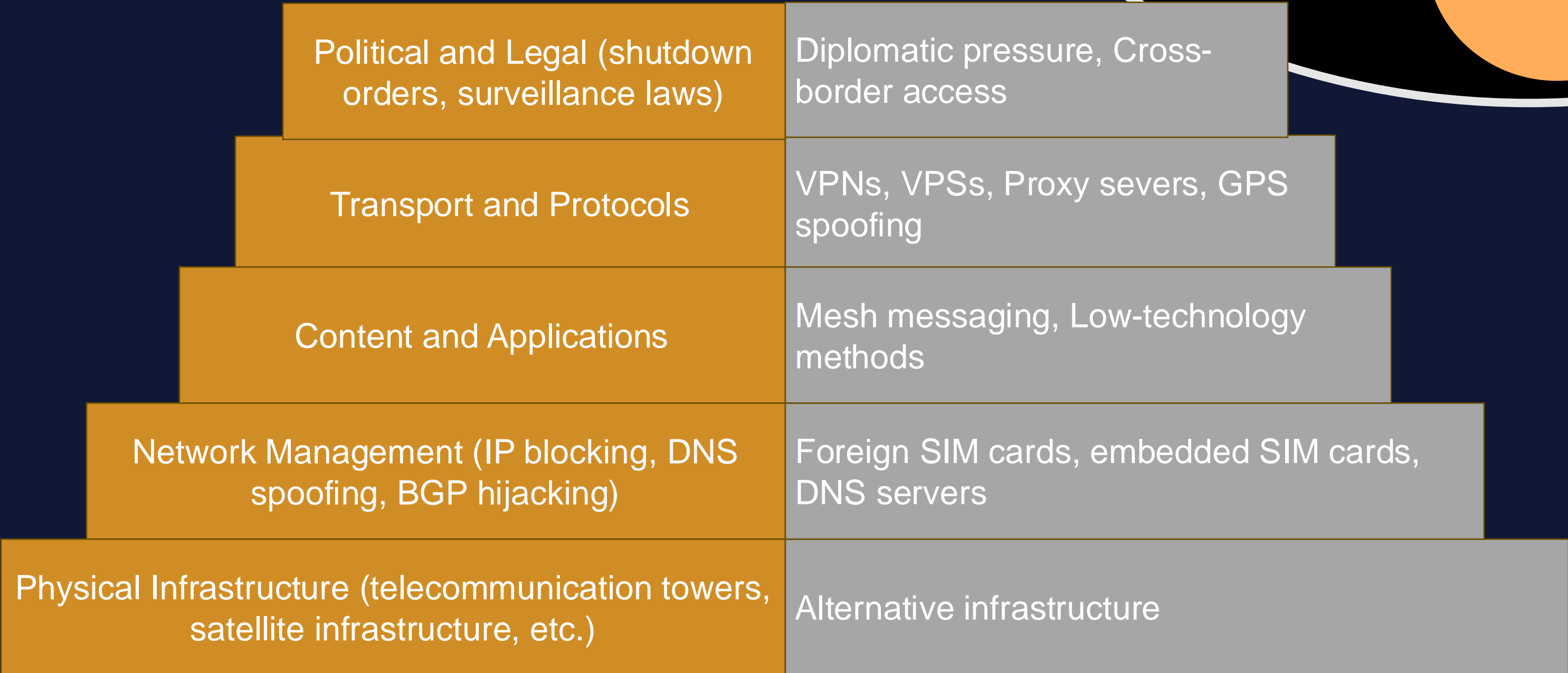
- 1
- To systematically extract and classify existing circumvention technologies
- 2
- To critically assess the effectiveness of these technologies in adversarial settings, identifying user safety implications
- 3
- To investigate the socio-political and infrastructural factors that shape the operational success of these technologies in adversarial settings

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**.

Unlike traditional models that focus solely on technical infrastructure, 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:



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.

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, and only considers complete shutdowns of Internet connectivity.

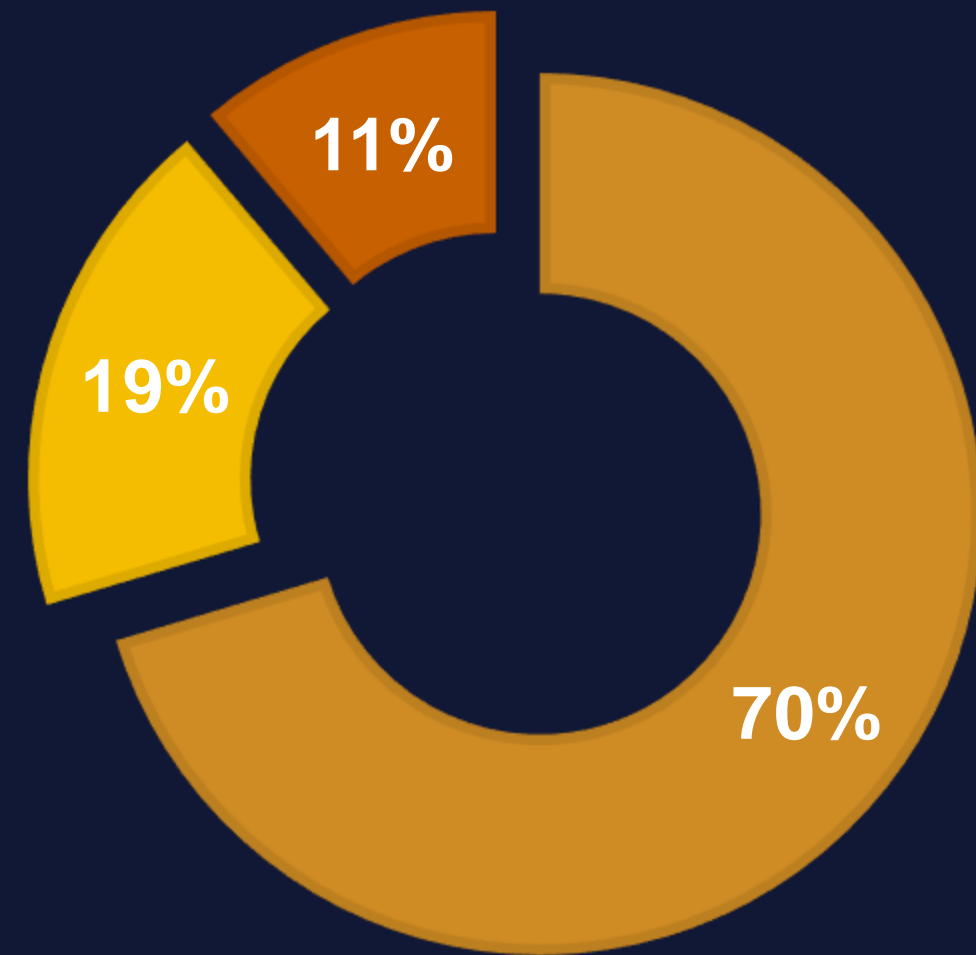
HOW IS A SHUTDOWN IMPLEMENTED?

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.

SHUTDOWN IMPLEMENTATION METHODS

- Routing
- Fundamental Infrastructure Shutdown
- Rogue Infrastructure Attack



CIRCUMVENTION TECHNOLOGIES

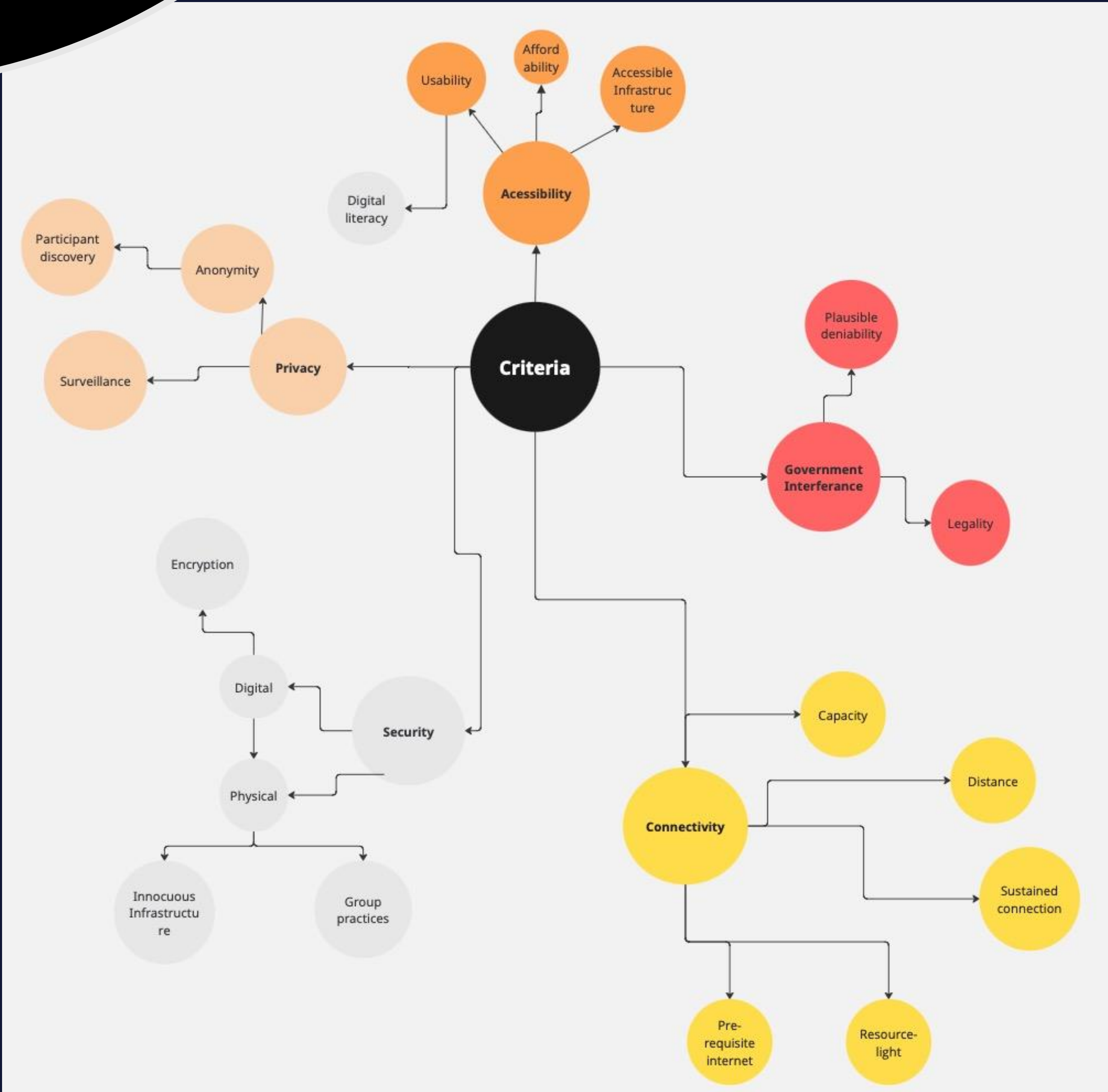


CRITERIA

- 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:



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



collective action in African countries', *International Journal of Communication*, 14(0), p. 24.