THE internet SHUTDOWN GAME

GAME MANUAL

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Published by APC in 2023

ISBN 978-92-95113-66-4

APC-202311-APC-T-EN-DIGITAL-356

TABLE OF CONTENTS

ABOUT THIS GAME

We have created this game instructions with the aim of helping to organise an engaging and informative training activity that sheds light on the various methods of internet shutdowns and ways to counteract them.

Governments resort to internet shutdowns for a wide array of purposes. These range from taking precautionary and preventive measures to quell the spread of unverified information during turbulent situations, to upholding national security and ensuring the maintenance of law and order. Internet shutdowns are a troubling phenomenon that not only disrupt digital connectivity, but also pose a significant threat to human rights. Understanding the motivations and the distinct methods employed to block internet access is vital for individuals and organisations striving to safeguard internet freedom and protect human rights in the digital age.

Designed as a creative commons game that you can adopt and adapt, this document provides detailed instructions for game facilitators and suggested game dynamics, and a map and cards to play as an in-person game and also in an online environment.

We believe this game can be played for a variety of audiences and can serve as a valuable tool to raise awareness about the different tactics employed to restrict internet access, as well as to enhance participants' understanding of internet infrastructure, shutdown procedures, and the use of various tools to circumvent them.

The game instructions can be utilised by anyone, whether you're planning to facilitate it in person or in an online setting. The target audience for this game encompasses human rights advocates, concerned citizens, legal professionals, and anyone who has encountered government control over internet access and seeks to deepen their knowledge in this area.

Over the course of a 120-minute game, we will delve into the technical intricacies of various internet shutdown models. By incorporating real-world scenarios and "circumvention" cards, players will gain insights into the technical mechanisms behind shutdowns and understand more about the different strategies they can use to navigate around them.

We trust that you'll find the game enjoyable and the instructions valuable in expanding your knowledge about internet shutdowns and their circumvention mechanisms. Our commitment is to keep enhancing this tool for the broader community. We look forward to sharing updated versions to ensure its continued usefulness to all – please check for the latest version in the game website.

Please send us feedback, ideas for improvements and new scenarios, or let us know if you want to translate the game to other languages, at shutdowngame@apc.org.

Enjoy the game!

The APC technical team – Avi, Igu, Maja, Mirto, Adolfo, Liz and Roxana

https://shutdowngame.apc.org

Game version 1.11 March 2025

GAME BASICS

This document outlines the organisation and execution of the Internet Shutdown Game, an interactive human-led training session that can be conducted in-person or online. This game relies on facilitators who are essential for its success – individuals who possess the knowledge to adapt the game content, style, chosen scenarios, difficulty levels and dynamics to suit the needs of the participants.

Facilitators should have a solid understanding of internet infrastructure and its functioning. They must also be attentive to participants' questions and doubts, and ensure an inclusive and participatory environment for all.

The game employs a game map that serves as a simplified representation of an imaginary country's national telecommunications infrastructure, where players can position themselves and their devices. This map serves as a visual aid to explain fundamental concepts regarding data transmission basics, how the internet operates, and the challenges in the design of national telecommunication infrastructures.

Subsequently, this same map is utilised to introduce a scenario in which internet access is blocked in a certain way – based on real world examples – indicating the specific components on the map that have been blocked to restrict internet access. The game toolset offers 13 scenarios of different difficulty levels for facilitators to choose from, according to their participants' profiles, location and interests.

In the game, the participants, divided into teams, analyse the scenario and select a circumvention card to play in an attempt to bypass the blockage. Teams compete for points, but the true enjoyment arises from deliberating various solutions and their effectiveness within the chosen scenarios.

Having conducted the game with diverse audiences, we've come to appreciate that each game session represents an opportunity for sharing and learning. Every session can be cherished as a unique and enriching experience for everyone involved, and hopefully, each will also create more technically accurate knowledge on internet shutdowns and how to bypass them more effectively.

GAME NEEDS: IN-PERSON VERSION

The in-person version of the game is designed for an optimal group size ranging from 6 to 20 participants, organised into 2 to 3 groups. Its duration typically falls within the range of 90 to 120 minutes.

To facilitate this version, you'll require the following materials:

1. A surface, board, or cloth on which the network map is drawn. This map can be hand-drawn, printed, or created by printing individual components on paper and assembling them on the floor or wall connecting them with lines or threads. Alternatively, you can also project the map on a large screen.

2. Shutdown cards: These are several cards featuring a red X, preferably made of transparent material. These cards are used to indicate which components on the map are not functioning when you demonstrate the different shutdown scenarios.

3. A set of circumvention methods playing cards, with one set allocated per team. These cards are instrumental in the gameplay and help teams strategise on how to bypass the blockages.

With these materials and guidelines, plus your knowledge and imagination, you can successfully conduct an engaging and educational in-person session of the Internet Shutdown Game.

GAME NEEDS: ONLINE VERSION

The online version of the game is suitable for 6 to 20 participants, ideally organised into 2 to 3 groups that will use breakout rooms for their discussions. The online game's duration ranges from 90 to 120 minutes.

Due to the intricacies of remote play, it is advisable to have at least two facilitators who have coordinated the work and divided the various tasks. Their roles will include managing the presentation, breakout room setup, supporting the use of the online platform, overseeing the game's progression, and addressing participant questions and concerns.

To facilitate this version, you'll require the following:

1. Game presentation: Prepare a game presentation in PDF format. It should provide an overview of the game, instructions, and any necessary background information. The one we use is available here as part of our kit, in multiple formats.

2. Players' presentation: Create a players' presentation, which includes the different scenarios, the game map, and the cards that teams can use during the game. This presentation should be available to all participants and can be shared via a digital platform. Also available here as part of our kit, in multiple formats.

3. Meeting setup: You will need a main meeting room and breakout rooms, with one dedicated breakout room per team. Pre-load the players' presentation into each breakout room. It should contain the layout and cards for all scenarios, and these rooms should remain accessible throughout the entire session. A shared drawing board can also be used for the game map exercise.

4. Card selection: Implement a way for each team to send their selected card to the facilitator privately. This can be done, for example, through a private message feature within the online platform to ensure that no one else sees the chosen card.

By carefully considering these elements and preparations, you can successfully execute the online version of the Internet Shutdown Game, maintaining engagement and educational value while accommodating the unique challenges of remote play.

INTRODUCTION TO SHUTDOWNS AND THE GAME MAP

OBJECTIVES

It is good to begin the game by agreeing on the game's objectives and rules.

The game's objectives can be summarised as follows:

1. Understanding internet infrastructure: To provide participants with a comprehensive understanding of the fundamental technical concepts governing internet infrastructure. This includes reviewing the components of a national internet infrastructure and discussing diverse variations that exist. By doing so, participants will gain insights into how the various types of shutdowns are technically executed.

2. Circumventing shutdowns: To enhance participants' knowledge about the mechanisms and strategies that can be employed to circumvent internet shutdowns. This includes exploring ways to protect themselves from potential government retaliation, thereby empowering individuals with the skills and awareness needed to navigate and mitigate the impact of shutdowns effectively.

3. Facilitate learning in a safe environment where all can participate and all voices are respected.

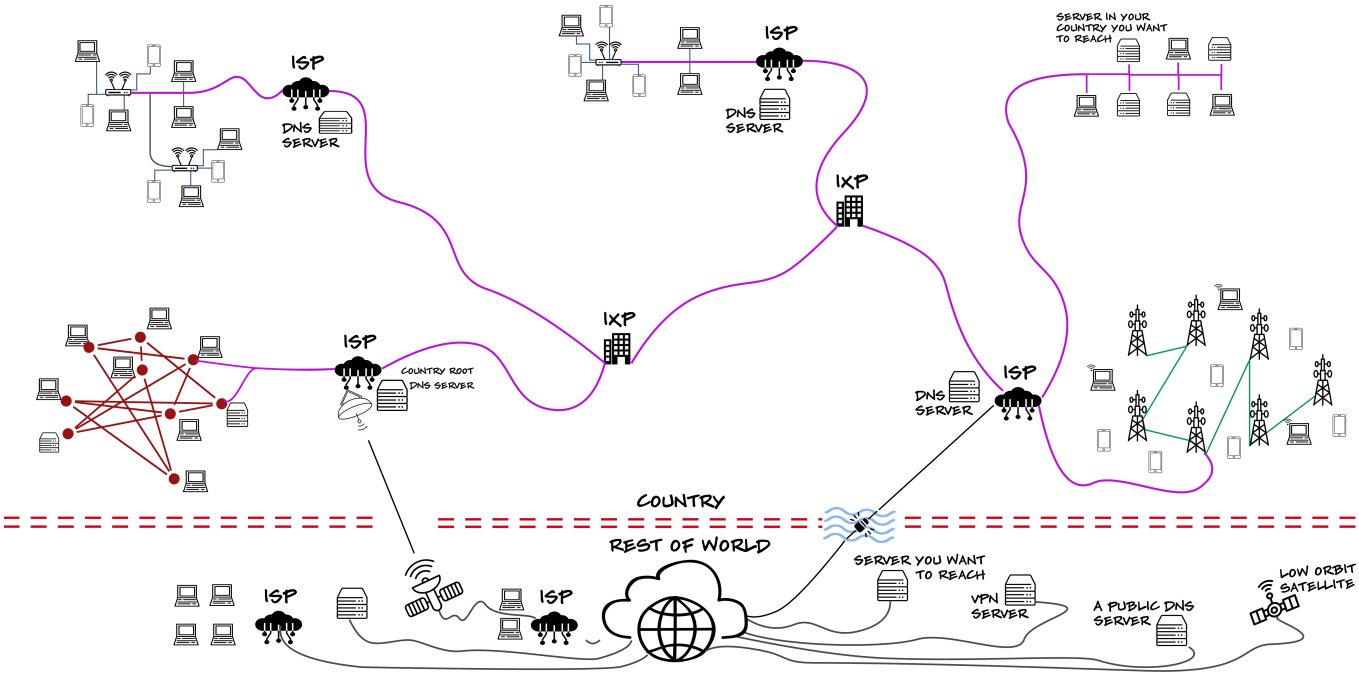
> Tip: If you are working with a specific group of participants with a certain profile (e.g. human rights defenders, lawyers) or from a specific organisation, country or region, or participating in an event, you can probably add other more concrete objectives to your game play.

INTRODUCTION TO SHUTDOWNS AND THEIR RELATION TO INTERNET INFRASTRUCTURE AND IMPACT ON HUMAN RIGHTS

An internet shutdown can be defined as “an intentional disruption of Internet-based communications, rendering them inaccessible or effectively unavailable, for a specific population, location, or mode of access, often to exert control over the flow of information.”[1]

Governments employ a myriad of techniques with different names to assert control over the internet. These methods are called shutdowns, disruptions, blackouts, blockages, curfews, internet throttling, banning, censoring, diverting traffic, DNS hijacking, geoblocking, fragmentation, among other terms used. The proliferation of these diverse tactics underscores the need to equip defenders with better preparation to be able to understand and bypass these blocking mechanisms.

Governments resort to internet shutdowns for a wide array of purposes. These range from taking precautionary and preventive measures to quell the spread of unverified information during turbulent situations, to upholding national security and ensuring the maintenance of law and order.



Internet shutdowns are a troubling phenomenon that not only disrupt digital connectivity, but also pose a significant threat to human rights. Shutdowns often occur in locations where governments wish to exert control over information flow and suppress dissent, effectively curtailing freedom of expression and access to information and services. Such actions violate the fundamental human right to freedom of speech and right to freedom of assembly as enshrined in international agreements like the Universal Declaration of Human Rights. But internet shutdowns have far-reaching consequences, extending beyond just freedom of speech and assembly. They impede access to essential services

[1] https://www.internetsociety.org/policybriefs/internet-shutdowns

like health, educational resources, business resources, and even emergency communications, directly impacting the right to education and the right to life in cases of crisis, wars or natural disasters. This interplay between internet shutdowns and internet infrastructure underscores the need for a more robust, decentralised and resilient internet ecosystem – a relationship that can become very clear though playing this game.

When shutdowns are underway, most governments would not acknowledge that they are happening and instead would blame the disruption on technical malfunctions, network congestions or cyberattacks. But all shutdowns are really enabled by the level of control that governments have over different pieces of their national telecommunications infrastructure. Government control over telecommunications networks and key infrastructure components, like internet service providers (ISPs), internet exchange points (IXPs), international gateways, telecommunications regulators, and/or top level domain name servers (DNS), makes it easier for authorities to enact these shutdowns, rendering the internet, which is now considered a basic service, a tool that can be weaponised against the very individuals it is meant to empower. And all this makes shutdowns in their many forms also almost almost impossible to prove.

Protecting human rights in the digital age requires a commitment to ensuring that the internet remains open and accessible to all, irrespective of political or social circumstances, and that its infrastructure is designed to resist undue government control and censorship.

Understanding how shutdowns take place, what components of the internet infrastructure are being jeopardised, and how to bypass these blockages is vital for individuals and organisations striving to safeguard internet freedom and protect human rights in the digital age.

If you wish to learn more about shutdowns and their consequences or refer participants who might be interested in further references to deepen their understanding of shutdowns and their consequences, you can find a set of annotated resources and suggested readings in Annex 3.

INTRODUCTION TO THE GAME MAP AND HOW THE INTERNET WORKS

The game employs a map representing an imaginary country's internet infrastructure.

This map serves as a shared visual reference point, grounding participants in a common space and aiding in their understanding of fundamental connectivity concepts.

Before commencing the game, it's essential to clarify that the map is a simulated exercise tool, representing a simplified illustration of a generic country's telecommunications infrastructure. Participants should be informed that real-world infrastructure varies significantly from one country to another, and is influenced in its design by a multitude of factors, including technical standards, legal frameworks, government policies, the land's topology, existing monopolies, commercial interests, geopolitical pressures, desire to control, and various others.

In the online version, this map can be shared through slides, while for in-person sessions, it can be printed, drawn on cloth, or dynamically created using pieces of paper and thread to represent and connect the individual components involved.

To introduce the game, you can utilise the map to explain the workings of the internet.

- In the online version, this can be accomplished by using different slides to gradually add components to the map, culminating in the presentation of the complete map. Check our example slides.
- In the in-person setting, a similar approach can be employed by using printed pieces and collaboratively constructing the map with the participants, adding the parts as you introduce the concepts, similarly to what is done in the online presentation.

This introductory phase helps establish a foundational understanding of how the internet functions within the context of the game. It requires about 20 to 30 minutes, including a couple of exercises done on the same map.

Components of the Map

Let's break down the components of the map and provide descriptions for each to help you facilitate the introductory section of the game:

Country limit (dotted line)

The dotted line at the bottom of the map represents the country's territorial boundary. Everything above this line is a component of the national internet infrastructure, which can be influenced and controlled by the government. Conversely, everything below this line represents the broader internet infrastructure, outside the control of the government.

Internet service providers (ISPs)

These are companies responsible for managing internet access infrastructure for individuals and organisations. Our map depicts various types of ISPs, including those managing broadband access (such as cable, ADSL, fibre optics), one with both mobile phone and broadband, and one connecting a mesh network. These networks, under the control of an entity, are also technically called autonomous systems.

Internet exchange points (IXPs):

IXPs are locations where ISPs connect their networks to others, facilitating the exchange of local internet traffic.The number and quality of IXPs in a country can significantly impact the efficiency of national traffic and reduce latency (delays of data reaching its destination) and telecommunication costs. In this example, there are two IXPs connecting ISPs to one another. IXPs can be privately owned, cooperatively owned, or managed by government organisations.

International connections

Our example country has two international connection points to the global internet, called gateways. These connections are represented by a satellite link and a submarine cable, each managed by a different ISP. Countries could also have landline connections (via cables or radio).

The number and type of international connection points depends on factors like a government's desire for control, economic resources, geographical location, topography, monopolistic market, etc. and can vary from one to hundreds of connection points to the “outside” world.

There is also a third option, a connection to a geostationary satellite constellation for direct international access (e.g. Starlink, Project Kuiper) that “bypasses” the national infrastructure.

Rest of the internet cloud

Beyond the country's boundary, we represent the rest of the internet, referred to as the "internet cloud". This encompasses various resources such as servers and other online services that we will use in this game. Remind participants that everything that is outside of the national infrastructure of our imaginary country is not under government control.

Connectivity options

On our map there are several ways for you to connect to the internet:

> **Cell phone network**: You can connect via a device to a cell antenna, with data travelling through the cellular network and eventually connecting to the national internet via an ISP. Highlight that antennas are connected in a hierarchical way.
>
> **Broadband**: This includes connections like fibre optics, DSL and cable, typically serving a limited geographic area with a high density of users.
>
> **Mesh network**: Specialised networks where access nodes are interconnected, often used in community networks. There is a server here that can offer services for this community. It is a very resilient infrastructure.

Satellite access: A direct connection to a low-orbit satellite (LEO) constellation bypasses the national infrastructure, connecting directly to satellites in orbit and relaying data to a ground station in another country. (examples Starlink, Project Kuiper, Oneweb, IRIS)

Wi-Fi: Wi-Fi access points provide short-range wireless connectivity, typically covering a limited area and linking to one of the other connection methods.

IP addresses

It's important to explain that every device connected to the internet, such as computers, phones and tablets, must have a unique identifier known as an IP address. Every server offering content also has an IP address.

IP addresses are essential for data to travel from its source to its destination on the internet: data packages carry the IP address of its origin and its destination.

Exercise: Tracing data paths

This exercise not only helps participants visualise data paths, but also serves as a practical and interactive way to reinforce the concepts presented on the game map. It fosters engagement and ensures that participants are comfortable with the map and its components before proceeding with the game.

For online play, using a shared board

Activate the shared board: Ensure that the shared board tool is accessible and ready for participants to use. In many online meeting platforms you can use a digital whiteboard or an external tool. Explain the exercise: Let participants know that they will be simulating data paths from different access locations to a server, both within the country and abroad. This exercise aims to reinforce concepts and familiarise participants with the game map.

- **Select locations:** Ask participants to imagine themselves in one of the access locations on the game map (e.g. Wi-Fi, cellular network, broadband, or mesh network). Participants can choose any location.
- **Data path drawing:** Using a coloured pencil tool, instruct participants to draw the path their data would take from their chosen access location to the highlighted server in the country (top right on the map). Encourage them to follow the components of the infrastructure shown on the map.
- **Discussion and review:** While participants are drawing their data paths, facilitate a discussion. Ask them to explain their choices and the route they drew. This is an opportunity to review concepts and clarify any mis-conceptions. Share with them how the path that data follows cannot be controlled by us, and that even different packets follow different routes based on cost, time, speed, etc. Once participants are comfortable with the exercise, run it again to a server located abroad.
- **Reiterate key concepts:** Throughout the exercise and as participants draw their data paths., reinforce key concepts, such as IP addresses, ISP involvement, connection of cell networks to internet connection, and the role of IXPs.
- **Encourage participation:** Encourage active participation and questions from participants. Ensure that everyone has the opportunity to contribute and gain a better understanding of internet infrastructure.

For in-person play, mark, indicate or walk on the game map

- **Explain the exercise:** Let participants know that they will be simulating data paths from different access locations to a server, both within the country and abroad. This exercise aims to reinforce concepts and familiarise participants with the game map.

- **Select locations:** Ask participants to place themselves in one of the access locations on the game map (e.g. Wi-Fi, cellular network, broadband, or mesh network). Participants can choose any location.

- **Data path drawing:** Instruct participants to indicate the path their data would take from their chosen access location to the highlighted server in the country (top right on the map). Encourage them to follow the components of the infrastructure shown on the map, using their fingers to show how data travels.

- **Discussion and review:** While participants are indicating their data paths, facilitate a discussion. Ask them to explain their choices and the route they are using. This is an opportunity to review concepts and clarify any misconceptions. Once participants are comfortable with the exercise, repeat it to a server located abroad.

- **Reiterate key concepts:** Throughout the exercise and as participants draw their data paths, reinforce key concepts, such as IP addresses, ISP involvement, connection of mobile phone networks to internet connection, and the role of IXPs.

- **Encourage participation:** Encourage active participation and questions from participants. Ensure that everyone has the opportunity to contribute and gain a better understanding of internet infrastructure.

DNS (domain name server) resolution

Once people are comfortable with the map structure, we will introduce the last critical component.

DNS resolution is a critical preliminary step in any internet communication. It allows your device to find out the IP address of the server hosting the website, content or service you wish to access. Once this IP address is known, data can be routed to its destination on the internet.

As a final step, explain that before data can travel from your device to its intended destination on the internet, a crucial step occurs called domain name system (DNS) resolution. Remind participants that for data to travel through the internet it needs to have the IP address of the destination server. The DNS process translates human-friendly domain names (like www.apc.org) into machine-readable IP addresses. This process is automatic, transparent and needed for any data to travel.

Here's an overview of DNS resolution, including queries to the nearest DNS, top-level DNS, and DNS servers located abroad:

- When you type a domain name (e.g. www.apc.org) into your web browser or any internet-connected application, your device needs to find the corresponding IP address for that server/resource.
- If the domain's IP address isn't cached locally, your device sends a query to the DNS server specified in its configuration or set by your internet service provider (ISP). This DNS server is typically the one closest to your location in terms of network topology.
- The nearest DNS server checks its own cache. If it has the IP address for the requested domain, it responds to your device with the IP address.
- If the nearest DNS server doesn't have the IP address in its cache, it initiates a recursive query to find the information. This query may involve multiple DNS servers along the way.
- Query to the top-level DNS:
    - If the nearest DNS server doesn't have the IP address, it needs to find out which DNS server is responsible for the top-level domain (TLD) of the domain you're trying to access. For example, in the case of www.apc.org, the TLD is ".org".
    - The nearest DNS server sends a query to the TLD DNS server, asking for information about the authoritative DNS server for the "apc.org" domain.
    - The TLD DNS server responds with the address of the authoritative DNS server for "apc.org".
- In some cases, particularly when accessing websites hosted abroad, your query might go beyond the borders of your country. Your nearest DNS server may not have information about the authoritative DNS server for the domain you're trying to reach, and the DNS server might need to send a query to a DNS server located abroad that specialises in handling international DNS queries. The DNS server abroad can then provide information about the authoritative

DNS server for the requested domain.

Use the map to draw the path of a couple of DNS request examples.

These map components and descriptions serve as foundational knowledge to help participants understand the basic concepts of internet infrastructure, connectivity, and the subsequent game scenarios.

Explaining the map and its related activities should take 20 to 30 minutes.

RUNNING THE GAME

RUNNING THE GAME IN-PERSON

Running the game in-person involves several steps and careful facilitation to ensure a smooth and engaging experience for participants. Here's a breakdown of how to conduct the game:

1. Share the game map and explain the rules:

- Begin by sharing the full game map with participants and providing a brief overview of the game rules.
- Explain the cards they have at their disposal for circumventing blockages.
- Clarify the point system used for scoring throughout the game.

2. Assign teams:

- Assign participants to teams.
- Ask them to designate one member from each team as the communicator responsible for sharing which card their team selected for each round.

Optional: instruct them to meet briefly and select a team name.

3. Initialise the scoreboard:

- Initialise the scoreboard using the team names if names were selected.

4. Introduce circumvention cards:

- Familiarise participants with the circumvention cards, emphasising that they can play only one card per scenario. The cards can be found in Annex 1.
- Explain the functionality of each card and the impact they have on the game scenario. Clarify how points are counted.
- Highlight that the "satellite" card can only be used once and that the "wildcard" card can represent any technically feasible and realistic scenario (except for satellite).
- Hand over a set of circumvention cards for each team.

5. Start with a scenario:

- Introduce the first scenario by blocking a specific component on the map. Use transparent cards with an “X” to block the relevant component(s).
- Explain the details of what is blocked, why it's blocked, and the level of government control over that infrastructure component.

6. Team discussions:

- Send teams to a private space nearby (e.g. a table) where they can also see the map if needed.
- Give them 10 minutes to analyse the scenario, discuss potential solutions, and select the card they want to play.

7. Share and compare solutions and discuss:

- As teams return, have each team place the selected card face down on the map surface.
- Once all the teams all back, show the selected cards. Have each team explain their rationale for choosing the particular card they used to bypass the blockage.
- Engage in discussion with the teams, evaluate their solutions, explain why it worked or didn’t work, ensure that wildcard solutions (if used) are technically feasible and accurate, and record points based on the decisions made.

8. Repeat with other scenarios:

- Repeat the process with three to six scenarios, as time allows and adjusting according to the participant’s engagement level. Explore various blockage scenarios to challenge participants' problem-solving and creativity skills.

9. Closing reflection:

- Conclude the game by facilitating a reflection session with participants. Encourage them to discuss what they have learned from the game, emphasising key takeaways, such as the challenges of proving shutdowns and the effectiveness of circumvention tools.
- Encourage participants to reflect on the real-world implications of these insights.

Game adaptations:

- Game scenarios can be found in Annex 2. Ideally you have to play three to four scenarios to make enough different blockage models clear to participants. Always start with an easy one, so people can understand the dynamics and it is not frustrating.

- For small and shy groups, and if you have the extra time, give them five minutes at the beginning to select a team name – it helps in building good team dynamics.
- The wildcard can be put to good use in the case of very fast response from the teams, or a very technically qualified audience. You could offer more points for the use of this card in a creative way (e.g. +2 points).
- If teams have difficulties reaching consensus, you might consider after going through a few scenarios to analyse them all together in the main space or room, and forget about the points or even separate spaces!

By following these steps above, we are sure that you can create an interactive and informative game experience that deepens participants' understanding of internet shutdowns and the strategies to counteract them.

Please send us feedback, ideas for improvements and new scenarios at: shutdowngame@apc.org .

RUNNING THE GAME ONLINE

Running the game online involves several steps to ensure a smooth and engaging experience for participants. Make sure you have prepared the online spaces beforehand and have assigned clear roles to each facilitator. Here's a breakdown of how we suggest conducting the game:

1. Share game map and explain rules:

- Begin by sharing the full game map with participants and providing a brief overview of the game rules.
- Explain the cards they have at their disposal for circumventing blockages.
- Clarify the point system used for scoring throughout the game.

2. Assign teams:

- Assign participants to teams. Optional: instruct them to move to breakout rooms to select a team name.
- Ask them to designate one member from each team as the communicator responsible for sharing which card their team intends to play.
- Encourage teams to communicate their chosen name via private chat for practice – so they are ready when they have to share the card they want to play.

3. Initialise the scoreboard:

- Initialise the scoreboard using the team names if names were chosen.

4. Introduce circumvention cards:

- Familiarise participants with the circumvention cards, emphasising that they can play only one card per scenario.
- Explain the functionality of each card and the impact they have on the game. Clarify how points are counted.
- Highlight that the "satellite" card can only be used once and that the "wildcard" card can represent any technically feasible and realistic scenario (except for satellite).

5. Start with a scenario:

- Introduce the first scenario by blocking a specific component on the map. Use an *X* to indicate the blocked component(s) and the *///* card to indicate filtered traffic.

- Explain the details of what is blocked, why it's blocked, and the level of government control over that infrastructure component.

6. Breakout room discussions:

- Send teams back to their respective breakout rooms with access to the scenario map and the cards they can play.
- Give them 10 minutes to analyse the scenario, discuss potential solutions, and select the card they want to play.
- Remind them to let facilitators know of their selected card using the pre-defined secret channel, and tell them return to the main room once their decision is made.
- Feel free to visit the virtual rooms in order to clarify doubts or guide the discussion. Call all the teams back to the main room once the allotted time is over.

7. Share and compare solutions and discuss:

- Once all the teams are back, share the different cards that each team played. Have teams present their rationale for choosing the particular card they used to bypass the blockage.
- Engage in discussion with the teams, explain why the card worked or didn’t work, evaluate their solutions, including ensuring that wildcard solutions are technically feasible and accurate, and record points based on the decisions made.

8. Repeat with other scenarios:

- Repeat the process with three to six scenarios, as time allows and adjusting according to the participant’s engagement level. Explore various blockage scenarios to challenge participants' problem-solving and creativity skills.

9. Closing reflection:

Conclude the game by facilitating a reflection session with participants.

- Encourage them to discuss what they have learned from the game, emphasising key takeaways, such as the challenges of proving shutdowns and the effectiveness of circumvention tools.
- Encourage participants to reflect on the real-world implications of these insights.

Game adaptations

- Running the online game requires some extra careful planning:
    - Set up the online spaces beforehand.
    - Explain carefully how to operate breakout rooms, and how to join and leave them.
    - Allow participants to download a copy of the scenarios and the cards they can play
    - Make sure teams are clear on how to let facilitators know of the card they have selected.
- Game scenarios can be found in Annex 2 on Page 25. Ideally you should play three to four scenarios to make enough different blockage models clear to participants. Select scenarios that are easier to begin with – and add complexity as needed, depending on the participants, the energy level and the competitiveness!
- For small and shy groups, and if you have the extra time, give them five minutes at the beginning to select a team name – it helps in building good team dynamics.
- If players are slow in selecting an answer, or have many tech doubts, play fewer scenarios and spend more time on the tech basics, explaining the blocking mechanisms and circumvention techniques in more detail.
- If players are very quick, use more time in discussing different alternative solutions to scenarios . You can even offer more points for any team that uses a valid wildcard solution!
- If teams have difficulties reaching consensus, you might consider after going through a few scenarios to analyse new scenarios all together in the main space or room, and forget about the points or even separate spaces!

Running the online game for a large number of participants: on occasion you might want to run the game online for 30 people or more. In this case, working in groups will be not be productive. A suggested variation is after you present each scenario, to have each participant select their desired card using an online survey/data collection tool, and then discuss the choices (both right and wrong ones) with all participants.

By following these steps, you can create an interactive and informative online game experience that deepens participants' understanding of internet shutdowns and the strategies to counteract them.

Please send us feedback, ideas for improvements and new scenarios at: shutdowngame@apc.org .

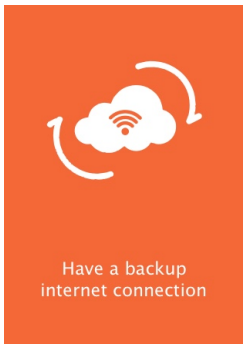
ANNEX 1: CIRCUMVENTION CARDS

The circumvention cards are the way in which participating teams choose a solution to a specific blockage scenario.

Teams can play only one card per scenario. The “satellite access” card can only be played once per game (otherwise they could play it for all scenarios and it will always work).

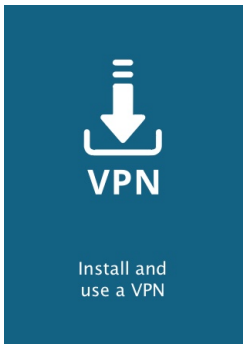
Correct cards played are +1 point, and wrong cards are -1 point.

The wildcard card can be used to represent any other creative but feasible solution. Wildcards provide space for lots of good ideas to debate, especially with more tech-savvy participants.



Backup Internet Connection

An alternative (secondary) connection to the internet, based on a different access technology and with a different ISP. For example if your main connection is broadband, the backup connection could be a 4G cell connection.



VPN

When introducing this card, first Explain how a VPN works – show on the map the location of the VPN server abroad.

Explain how data travels without a VPN and then using a VPN. Discuss how this is good but also slower.

Satellite Connection

A direct connection to a low orbit (LEO) satellite constellation that by-passes the whole national infrastructure, connecting to a ground station in another territory. Examples: Starlink, Project Kuiper, IRIS (EU)

Because this card bypassses the country infrastructure, it will circum-vent any blockage.

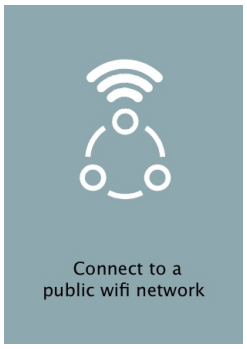
However, it can be expensive (though getting cheaper) and slow, and if not legal, there is also the risk that the antenna emitter could be located.

This card can be only played once in the game. Encourage players to use it only in scenarios where no other card will work.

Change the DNS configuration

Change the default DNS (Domain name service) to using a public DNS server (usually abroad), instead of the default DNS provided by your ISP.

It is recommended to refresh how DNS resolution works.



Use Public Wifi

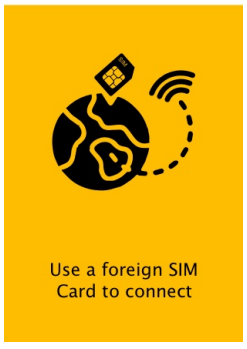
Explain that all users using a public access point share the same IP address, so no individual identification is possible.

Also, the public access point might use another, different ISP from another one in the same location

Use Tor

Explain how this provides anonymous web navigation using 3 anonymous servers located anywhere. Explain how onion layers encrypt the content and destination. Explain why this makes the connection slower but also how this can be very difficult to block.

The Tor network can be used with other services, e.g. by using tor as a socks proxy, but might be too complex for this game.



Use a Foreign SIM

For countries where each phone card must be associated with a national ID. It uses roaming agreements and the national cell phone infrastructure, but it might be blocked less because it has a foreign phone number.

In some cases where people live near the country limits they use it to connect to the neighbouring country's infrastructure

Wildcard

Any other solution – thinking outside of the box. It has to be creative but also technically viable, and not a duplication of other cards.

ANNEX 2: SCENARIOS

Below we provide 13 example scenarios that you can plan to use with your participants.

Give time constraints, you will be able to play four to six scenarios during a two-hour game. You can select which ones to play beforehand, or choose as the game evolves and if participants find the scenarios too hard or too easy. Participants in a specific country/region might benefit from scenarios that fit real blockages that they have experienced.

We suggest always starting with an easy one to let participants gain confidence as they learn and begin to understand the game rules.

For clarity, it is important to mark on the game map (whether playing in person or online) the parts of the infrastructure that are being blocked. Check our example slides.

We hope to add more scenarios as the game evolves with feedback. If you have ideas for more scenarios, please write to shutdowngame@apc.org.

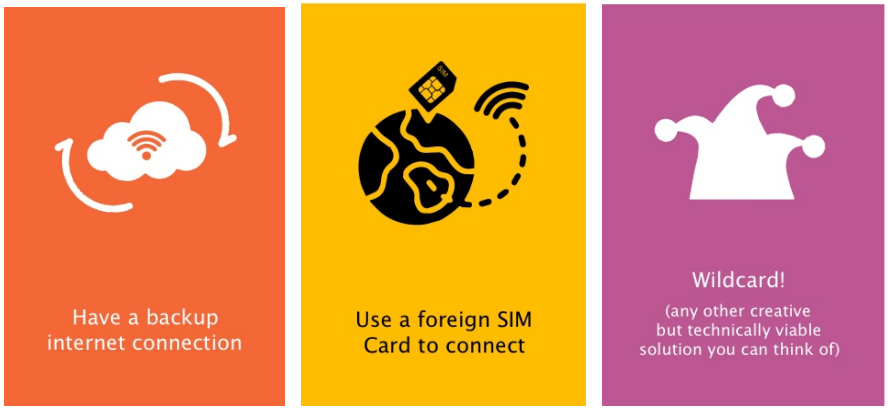
SCENARIO 1: CURFEW (ALSO CALLED NETWORK/ PARTIAL SHUTDOWN)

Difficulty: Easy

Scenario description: It is exam time and the government has imposed a broadband curfew. You have broadband at home, and your internet connection is down.

What to block: All broadband networks at the point where they connect to each ISP (see example).Cards that can be played

Cards that can be played



Wildcard:

– Move to another location

– Use another ISP (not broadband)

Things to explain

This is a good scenario to start with – most participants will realise they just need to use a different access network and ISP.

It is a good opportunity to highlight that it is important to have a backup connection always planned beforehand.

Real world examples

Used by many countries during elections, exams and festivals.
They normally block broadband and leave cell phone networks up – but some have blocked cell phone networks instead.

SCENARIO 2: CONTENT BLOCKING

Difficulty: Easy

Scenario description: To quell protests, the government has blocked access to Facebook, Twitter and WhatsApp during an election.

What to block: Filters on all the ISPs

Cards that can be played

Wildcard:

– Connect to a backup connection (maybe)

– Use another (less common) social media tool

Things to explain

This type of blockage can be achieved using commercial filtering applications and transparent proxy devices (which intercept an https re-quest and make it look like it was answered by the original site).

Solutions using Tor or http VPNs have to access the platforms via the browser and not the app.

Real world examples

Commonly used during protests and elections. They normally target mainstream social media tools and not alternative ones.

SCENARIO 3: INTERNATIONAL GATEWAYS CLOSED

Difficulty: Easy

Scenario description: You try to access a website abroad and you get an error message. You realise that this is happening with every site located abroad. You conclude that the internet international connection point(s) have been blocked by the government.

What to block: International gateways

Cards that can be played

Wildcard:

– If located close to another country, use that country's cell phone data network.

Things to explain

Low orbit Satellite constellation connections can be expensive, slow and potentially vulnerable, as it is easy to locate who uses them – but they effectively bypass all the national internet infrastructure. Of course, the solution must be installed beforehand, as it takes several days for setup.

Real world examples

This blockage is only possible in countries with just a few international gateways that can be turned off and are all under government control. In general, just a temporary measure.

SCENARIO 4: TRAFFIC BLOCKING

Difficulty: Easy

Scenario description: The government does not want you to access a foreign website with certain information. It has ordered all internet service providers (ISPs) in your country to delete traffic destined to this site's IP address.

What to block: Every national ISP icon, to represent routers.

Cards that can be played

Wildcard:

– Duplicate the site content locally using another IP address.

– Use a smaller ISP that doesn't obey government orders.

– Use a web proxy.

Things to explain

Review how data travels if a VPN or Tor browser are used. Remind participants that it is good practice to have one or more installed beforehand.

Foreign SIM cards will not work because they will still use the routing at the national level (cell phone company roaming agreements).

When packet filtering is used, only individuals within the affected net-work are able to detect the shutdown (using a technique called active probing).

Real world examples

Used to block abortion sites, online betting sites, content related to religion, prohibited or illegal substances, etc.

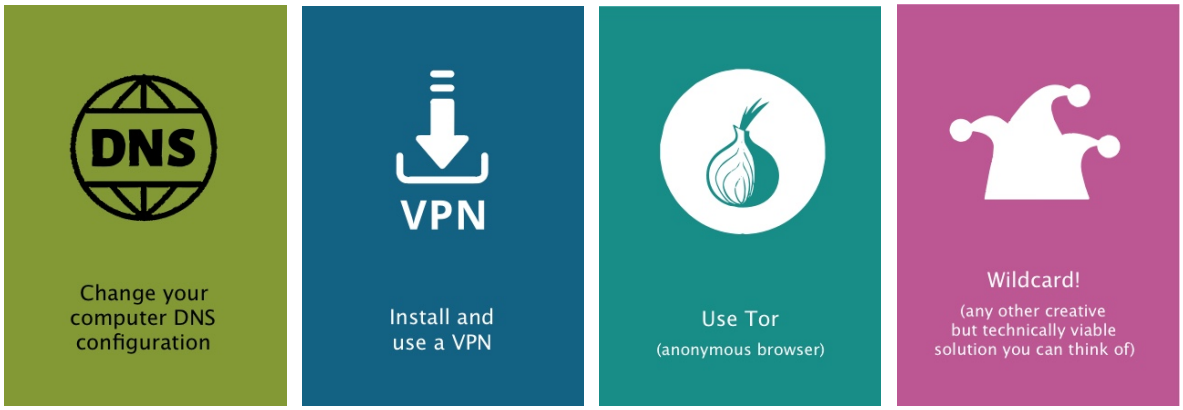
SCENARIO 5: DNS FILTERING (ALSO CALLED DNS HIJACKING, POISONING OR SPOOFING)

Difficulty: Medium

Scenario description: The government has ordered all national ISPs to change the DNS resolution for a domain where you could have accessed a protest site. When you try accessing the site, it sends you to a fake government-managed site instead.

What to block: Every national DNS icon.

Cards that can be played



Wildcard:

– Get the IP address of the site by asking a friend abroad or use an online tool to resolve – then use the IP address directly.

Things to explain

Review how a DNS works.

Note that when using a VPN, most use the DNS configured in the devices's setup, that is usually that of the ISP – so it can still be affected by the filtering.

Real world examples

Only effective when the government completely controls the network infrastructure. Quite easy to prove and bypass. Has been used to block access to search engines, to specific sites and to specific social network and video websites .

SCENARIO 6: PROHIBITED VPN

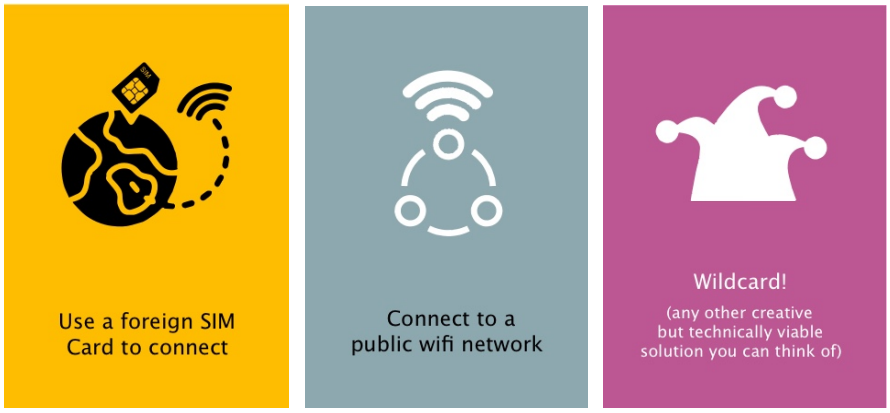
Difficulty: Hard

Scenario description: The government has said they will punish anyone they can prove is using a VPN… but you want to use a VPN to connect to a specific website.

How do you ensure that you cannot be caught?

What to block:

Cards that can be played



maybe

Wildcard:

- Tor can be used with bridges as an alternative to the VPN, or to access the VPN

Things to explain

Explain how a public Wi-Fi hotspot shares the IP address and it is not possible to single out devices/ people.

Foreign SIM cards might work, depending on whether the country does or doesn't have the possibility to match a mobile phone number with a physical device/citizen.

Real world examples

Belarus, China, Egypt, Iran, Iraq, North Korea, Oman, Russia, Syria, Turkey, Turkmenistan, Uganda, United Arab Emirates.

SCENARIO 7: GEOLOCATION

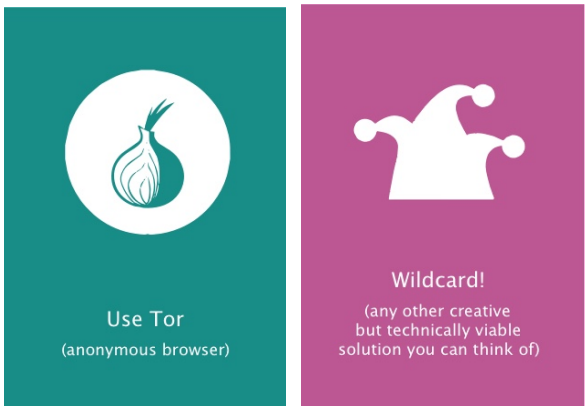
Difficulty: Easy

Scenario description: In your region, the government is preventing you from downloading certain apps (like social media platforms or Telegram) and blocking specific IP addresses associated with well-known VPNs.

How can you download and use these apps anyway?

What to block:

Cards that can be played



Wildcard:

– Another VPN service.

– Download tools from other sites (proxies).

– Change your physical location

Real world examples

Several countries have blocked access to specific applications like social media apps and communication apps so that they cannot be downloaded and installed from normal sources.

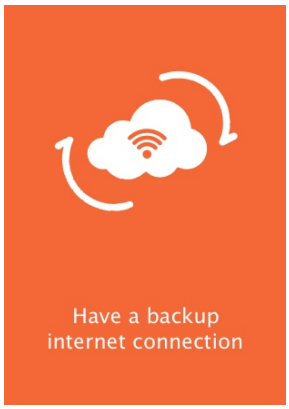
SCENARIO 8: CELL PHONE JAMMING

Difficulty: Hard

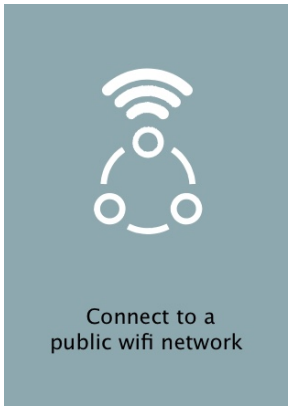
Scenario description: You are in a protest together with your friends. You are using the cell (mobile) phone network. You have good cell phone reception, but you are unable to send or receive messages. You suspect the network is jammed. What can you use to stay connected to your fellow protestors?

What to block: The cell antennas

Cards that can be played



(on the area, not cell phone)



(if not connected to the cell-phone network)

Wildcard:

– Change location – jamming devices cover a limited area.

– If using Wi-Fi, change the Wi-Fi frequency, e.g. to 5 GHz band

– Set up alternative peer-to-peer solutions

Things to explain

Jamming could target Wi-Fi, Bluetooth, GPS, radio communications or cell service (blocks phone calls, SMS and access to mobile data) for all users.

Explain limitations of the solution.

Real world examples

Usually applied in large concentrations of people, like festivals or protests. Jamming devices cover a very limited area.

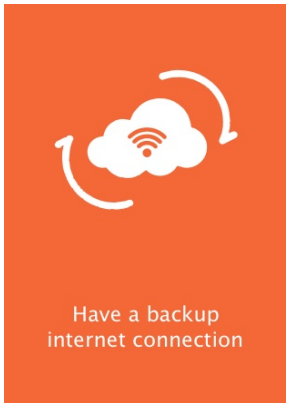
SCENARIO 9: LOCALISED SHUTDOWN

Difficulty: Medium

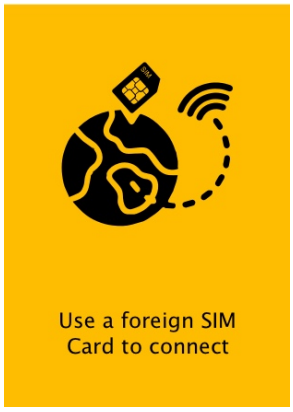
Scenario description: Due to protests, the government does not want citizens from your region to connect to the internet. It is said that when data packets with their IP addresses reach the government-managed IXPs, the packets are discarded. What can you do?

What to block: IXPs

Cards that can be played



(on the area, not cell phone)



(if not connected to the cell-phone network)

Wildcard:

– ?

Things to explain

The way to implement such localised shutdowns of mobile or fixed connectivity is through configuration changes in the telecommunications network. These changes can effectively disable telecommunications services without having to power down or physically damage the underlying infrastructure, and can prevent the routing of internet traffic to/from a local network provider.

Real world examples

Used to block access from certain regions and communities, especially controlled territories, refugee camps or war zones.

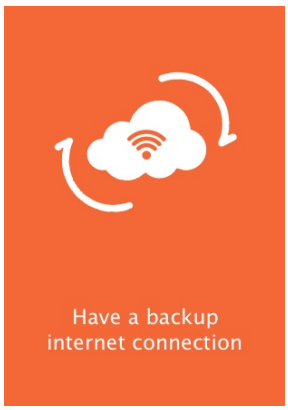
SCENARIO 10: ONLY VIPS CAN CONNECT

Difficulty: Easy

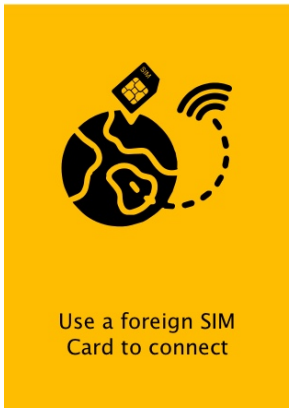
Scenario description: When you send information via the internet, it seems to be blocked, you can't reach any server! However, your neighbour and best friend who works in the government tells you that she can access all resources just fine. You are both connected to the same ISP.

What to block: locate the player in a certain broadband network, and block every connection except one.

Cards that can be played



(might work if filtering is done by some ISPs only)



(might work)

Wildcard:

– Connect to your neighbours' Wi-Fi.

– Connect to another ISP.

– Change location.

Things to explain

This type of filtering is achieved by changing BGP (Border Gateway Proto-col) routes or internal routing rules in the ISP. These are rare, because BGP routes can be publicly queried, so these blockages are easy to detect and traced back to individual service providers (and it is also easy to attack the VIP addresses).

The difference with other filtering scenarios is that this type of filtering checks the IP addresses of the source (sender) of the data package.

Real world examples

Requires a wide control of the infrastructure by the government. Used by some in order to allow only government officials to connect while the rest of the population is unable to do anything.

SCENARIO 11: INTERNET THROTTLING

Difficulty: Hard

Scenario description: Throttling is defined as “artificially restricting, but not stopping, the flow of data through a communications network”. In this scenario, your internet access may seem available, but it is extremely slow and is effectively unusable for information consumption and sharing.

What to block: A point where we can say the players are located.

Cards that can be played

any card (might work, depending on how the throttling is implemented)

Wildcard:

– ?

Things to explain

Throttling on mobile networks can be done by downgrading 3G and 4G connections to 2G.

Fixed network and application-level throttling can be achieved through the use of traffic management systems installed within a network provider’s infrastructure.

Real world examples

Throttling is hard to detect. These measures are normally temporary and related to events like national exams or elections, or protests, festival and other large gatherings.

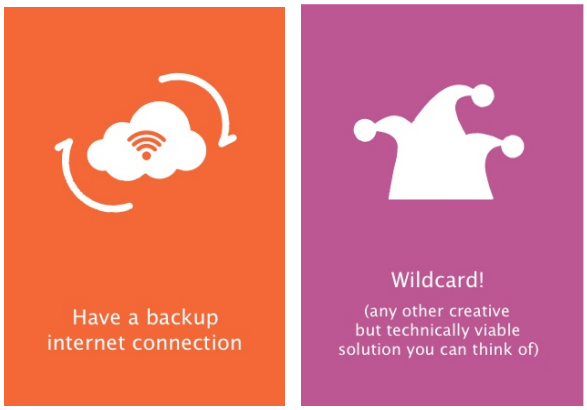
SCENARIO 12: ROGUE INFRASTRUCTURE ATTACK

Difficulty: Hard

Scenario description: You are in a protest. You can see “new” Wi-Fi access (or cell phone access) points that the government promotes as faster internet access, with a much stronger signal. The connection points are suspicious and seem to lead to government- controlled sites.

How to show it on the map: place a new wifi access point in another color

Cards that can be played



(not a controlled one)

Wildcard:

– If Wi-Fi is being intercepted, a wired (Ethernet) connection is an alternative.

– In cell phones, manually select access network.

Real world examples

Expensive to setup and normally restricted to an event (ie a large gathering) or a zone (ie refugee camp).

SCENARIO 13: DEEP PACKET INSPECTION (DPI, ALSO KNOWN AS PACKET SNIFFING)

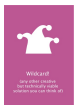
Difficulty: Hard

Scenario description: You conduct a search for certain politically controversial keywords in your favourite search engine, and the search fails. But you are certain it should be returning valid results, it is such a key issue!

You are also certain that Internet connectivity has been getting slower on average over the last few months...

What to block: Filtering symbols on all ISPs

Cards that can be played



Wildcard:

– encrypt traffic!

– Common VPNs will probably be well known and therefore, blocked. Use more obscure VPNs.

– https traffic could be opened (SNI filtering) and decrypted. There are tools to bypass this like GoodbyeDPI DPITunnel, Zapret and Geneva

Things to explain

This is a most sophisticated form of data traffic control, currently being used by some governments. It requires the capacity to impose the installation of hardware and software in every ISP.

To allow data to travel through their network, routing devices inspect the information in the packet's header, like the destination address, source address, and port number. DPI examines a larger range of metadata including the header and the data the packet is carrying.

When DPI is implemented, it examines the contents of all data packets using pre-defined rules that include what to do with specific content it might find. It can therefore be used to exercise a variety of blockages, depending on how it is configured. And so the bypassing tools have to be adapted to the DPI policies being implemented.

Real world examples

This is used in the Great Firewall of China, officially known the Golden Shield, at the national gateway level.

ANNEX 3: ANNOTATED LINKS AND RESOURCES

- **Internet shutdowns and human rights** (2022) by APC and Derechos Digitales https://www.apc.org/en/pubs/internet-shutdowns-and-human-rights has a very good intro to the use of shutdowns and the impacts on human rights, as well as examples of blockages all over the world, many of which have inspired our scenarios.
- An Interdisciplinary Exploration of Internet Shutdowns (2022) by Open Technology Fund https://www.opentech.fund/news/an-interdisciplinary-exploration-of-internet-shutdowns/ classifies the different types of shutdown. It used to have a good shutdown dashboard that now seems to be offline.
- **Policy Brief: Internet Shutdowns** (2019)by ISOC https://www.internetsociety.org/policybriefs/internet-shutdowns/ offers a good general introduction to the issue.
- In 2016, Access Now spearheaded the creation of the **Keep it On Coalition** https://www.accessnow.org/keepiton/, an alliance of over 300 groups collecting and sharing information about shutdowns and providing assistance to the people affected by them. Access Now's #KeepitOn campaign site contains statistics, useful data and relevant resources, including a **taxonomy of shutdowns** https://www.accessnow.org/publication/internet-shutdown-types/ that explains mitigation strategies and other **campaign resources** https://www.accessnow.org/keepiton/#resources
- **The Real Impact of Internet Shutdowns** (2023) by ISOC https://www.internetsociety.org/blog/2023/06/the-real-impact-of-internet-shutdowns/ measures the economic impact of shutdowns.
- **OONI** https://ooni.org/ Open Observatory of Network Interference, a global community measuring Internet censorship since 2012
- **OONI Technical multi-stakeholder report on Internet shutdowns: The case of Iran amid autumn 2022 protests** (2022) by OONI and ISOC https://ooni.org/post/2022-iran-technical-multistakeholder-report/
- **Internet Shutdowns in Paraguay** (2023) by TEDIC https://www.tedic.org/wp-content/uploads/2023/07/Internet-Shutdowns-Report-2023.pdf

- **Anatomy of Virtual Curfews** (2017) by Digital Empowerment Foundation https://www.apc.org/sites/default/files/Anatomy_of_Virtual_Curfews.pdf focuses on examples in India and and other South Asian countries.
- **Understanding Internet Shutdowns: A Case Study from Pakistan** (2018) by Benjamin Wagner https://research.wu.ac.at/en/publications/understanding-internet-shutdowns-a-case-study-from-pakistan-3
- On satellite constellations and sustainability https://manypossibilities.net/2023/11/starlink-and-inequality/
- On Low earth satellites for internet access https://www.internetsociety.org/resources/doc/2022/perspectives-on-leo-satellites/

ANNEX 4: CIRCUMVENTION TOOLS AND LINKS

We have been asked by participants to share with them links to help implement some of the circumvention techniques played in the game. Here are some useful resources

- Change your DNS configuration to use public DNSs (instructions for Windows, Mac, Linux and Android): https://proprivacy.com/guides/how-to-change-your-dns-settings-a-complete-guide
- Ceno Browser: https://censorship.no/en/about.html a mobile browser for bypasing censorship
- Hermes: https://www.rhizomatica.org/hermes/ an affordable digital telecommunication system over shortwave/HF radio
- Briar project: https://briarproject.org/ a tool for peer-to-peer encrypted messaging and forums
- Bridgefly https://bridgefy.me/ an offline messaging system for android phones
- VPN types and how to install a VPN:
    - Why you might want a VPN - A guide by Riseup: https://riseup.net/en/vpn/why-is-needed
    - Get Riseup's VPN: https://riseup.net/en/vpn
    - A detailed and technical guide from Freedom of Press Foundation: https://freedom.press/training/choosing-a-vpn/
- TOR Project site: https://www.torproject.org/
- Oui sync: Secure, open source, peer-to-peer file-sharing https://ouisync.net/
- Aidrop: https://en.wikipedia.org/wiki/AirDrop a proprietary software to connect Apple devices directly
- GoodByeDPI: has several mechanisms to bypass DPI blockages, https://github.com/ValdikSS/GoodbyeDPI
- Not used for the game (yet), TOR Bridges are relays that help you circumvent censorship, find more info at https://bridges.torproject.org/

CREDITS AND ACKNOWLEDGEMENTS

Several Icons and illustrations made by others were used in the design of this game and its associated materials, all of these were distributed under a CC-BY-3.0-DEED license. The list of credits follows:

Satellite by Creative Stall

shut down by P Thanga Vignesh

wifi by Richa

Radio tower by iconcheese

Satellite by SAADI ALA

Cable by IconMark

Building by iconsphere

Router by vectorstall

Laptop by Vectors Market

Cloud by cakslankers

water water by Manohara

server by Dika Neto

internet by RROOK

distributed network by Bruno Castro

Satellite dish by Meko

Satellite dish by AbtoCreative

Thanks to the APC staff, members and partners that provided feedback for this project, as well as all the online and onsite players, and Gaba and Jim (Tor Project)


APC
ASSOCIATION FOR
PROGRESSIVE
COMMUNICATIONS