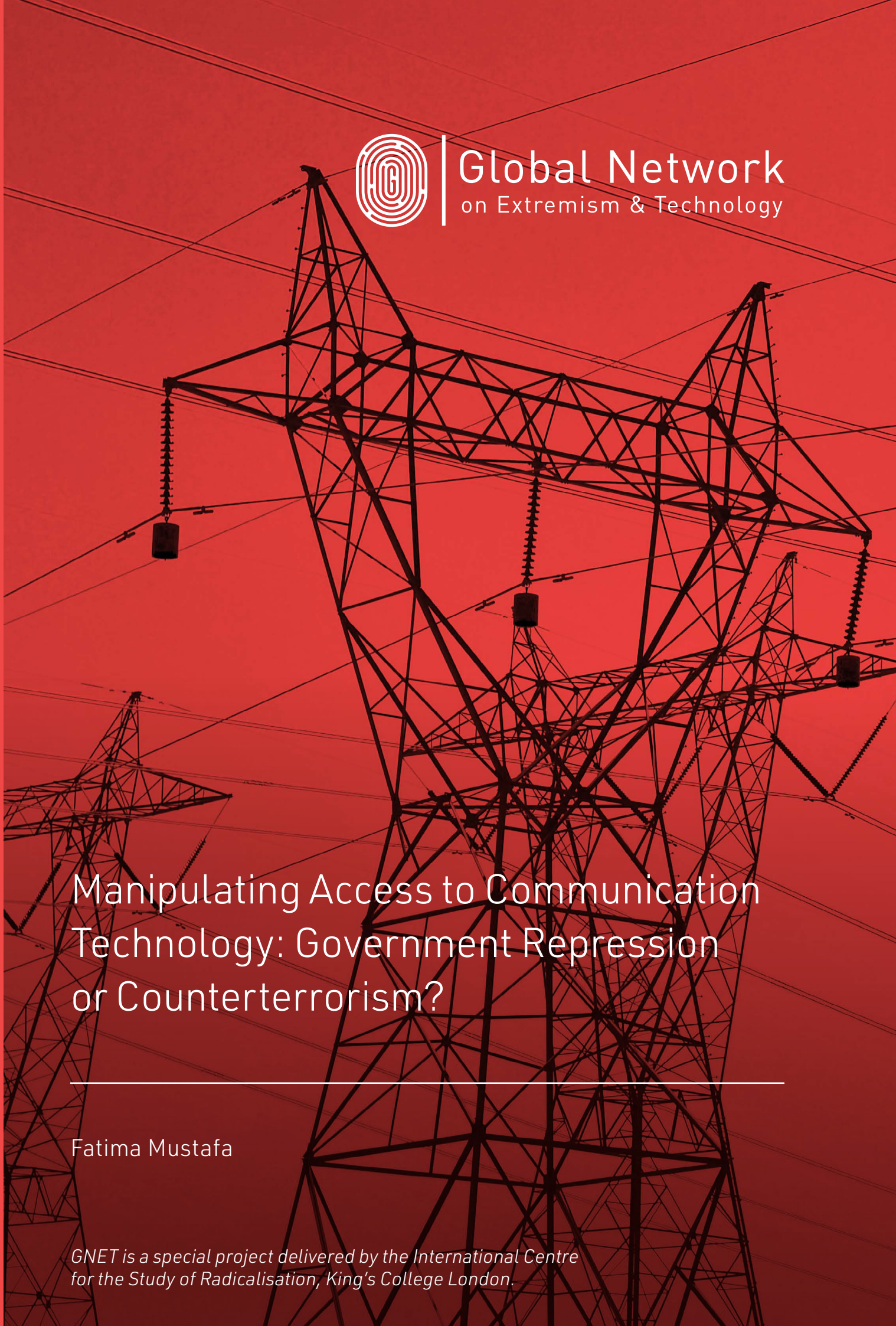


Global Network
on Extremism & Technology

Manipulating Access to Communication Technology: Government Repression or Counterterrorism?

Fatima Mustafa

GNET is a special project delivered by the International Centre for the Study of Radicalisation, King's College London.

The author of this report is
Fatima Mustafa

The Global Network on Extremism and Technology (GNET) is an academic research initiative backed by the Global Internet Forum to Counter Terrorism (GIFCT), an independent but industry-funded initiative for better understanding, and counteracting, terrorist use of technology. GNET is convened and led by the International Centre for the Study of Radicalisation (ICSR), an academic research centre based within the Department of War Studies at King's College London. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing those, either expressed or implied, of GIFCT, GNET or ICSR.

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.

Executive Summary

With increasing frequency, governments around the world – including both democracies and autocracies – have relied on Internet and cell phone disruptions to limit violence, tackle protests, hinder opposition and control the spread of information. According to data collected by Access Now, the number of network disruptions has increased steadily between 2016 (75 disruptions) and 2019 (213 disruptions), with a wide range of different countries, such as Venezuela, India, Egypt, Sudan and others, limiting access to communication technologies.[1] While governments commonly defend network disruptions as a necessary tool in their toolkit to tackle violence, human rights critics argue that such blunt instruments limit access to communication technology violate human rights, including the right to free speech, and severely disrupt access to healthcare, education and work. In addition, network shutdowns are costly in economic terms, with one estimate suggesting that the global economy lost $8 billion in 2019 alone due to such shutdowns.[2] Despite the heavy costs tied to network disruptions, there is little existing empirical work that examines whether network disruptions are effective at achieving the outcomes for which governments claim to use them. In the absence of such evidence, governments often use claims about tackling violence, national security or misinformation as a cover for network disruptions.

This report specifically focuses on one commonly provided justification for national-level network disruptions – to tackle terrorism – and evaluates the effectiveness of network disruptions in this regard. Using daily data on national-level Internet and mobile phone shutdowns, Internet throttling and social media bans between 2016 and 2019 in countries around the world (made available by Access Now and the #KeepItOn Coalition),[3] this report offers a preliminary analysis of the relationship between these various forms of network disruptions and terrorist violence. The data on daily deaths and injuries from terrorist attacks in countries around the world comes from the Global Terrorism Dataset.[4] Using these data sources, the fixed effects regression analysis in this report shows that network disruptions (that is, shutdowns and throttling) do not correlate with the number of people killed or injured in terrorist attacks. In addition, in a separate analysis, the report shows that a ban on social media platforms, such as Facebook, Twitter and WhatsApp, also does not correlate with deaths and injuries from terrorist violence. Given the limitations of the analysis, due to the fact that network disruptions are not random, it is difficult to make causal claims about the relationship between network disruptions and terrorist violence. However, this analysis provides a preliminary look at the impact of network

1 Access Now and #KeepItOn Coalition, "Shutdown Tracker Optimization Project (STOP)" https://www.accessnow.org/keepiton/ (accessed 8 November 2021).
2 Chloe Taylor (2020) "Government-led internet shutdowns cost the global economy $8 billion in 2019, research says" CNBC, 8 January 2020, https://www.cnbc.com/2020/01/08/government-led-internet-shutdowns-cost-8-billion-in-2019-study-says.html (accessed 6 November 2021).
3 Access Now and #KeepItOn Coalition, "Shutdown Tracker Optimization Project (STOP)".
4 National Consortium for the Study of Terrorism and Responses to Terrorism, Global Terrorism Dataset, https://www.start.umd.edu/gtd/ (accessed 6 August 2021).

disruptions on terrorism, paving the way for further research. The final section of this report looks past official government justifications for network disruptions to briefly explore other potential reasons why governments use network disruptions, such as to conceal repression and to prevent reporting. In addition, there is a brief discussion of other ways in which governments use communication technology and social media to tackle terrorism, such as by requesting that social media platforms remove extremist content online or provide user data for further scrutiny.

Overview

Governments face a dilemma as communication technologies such as the Internet and mobile phones have spread rapidly and become central to our lives, demonstrated recently by our dependence on these technologies during the global coronavirus pandemic. If governments allow the unrestricted use of communication technologies, they risk facing opposition organised through these technologies; if they restrict access to communication technologies, they might face a backlash. This, for Kedzie, is the "dictator's dilemma".[5] However authoritarian governments are not the only ones facing this dilemma: Agarwal, Howard and Hussain's well-known work on network blackouts between 1995 and 2011 shows that 39% of these network disruptions occurred in democracies.[6] Given the "dictator's dilemma", why have some democratic and non-democratic governments around the world increasingly limited access to communication networks at crucial points in time?

While governments often deny the deliberate use of network disruptions, on the occasions that they do acknowledge them, they present network disruptions as a tool to tackle violence, contain protests, ensure public safety, prevent the spread of misinformation and prevent cheating in exams.[7] Data made available by Access Now and the #KeepItOn Coalition on network disruptions around the world between 2016 and 2019 shows that counterterrorism was the most common government justification for national-level network disruptions. In some cases, governments claim that network disruptions prevent opposition or terrorist groups from being able to coordinate with each other to plan and execute attacks, and, more broadly, such disruptions help to overcome collective action problems.[8] Critics of network shutdowns argue that such disruptions in connectivity are detrimental to fundamental human rights, such as the right to free speech, as well as access to healthcare, education, and work. In addition, network shutdowns disrupt businesses and damage the economy. For example, India faced a huge cost of $2.8 billion last year due to Internet shutdowns.[9] Despite the costs associated with network shutdowns in terms of both human rights violations and economic losses, we still know relatively little about whether network disruptions actually work in the ways that governments claim they do.

This report offers a preliminary analysis of the effectiveness of network disruptions in achieving one specific outcome: tackling terrorist violence. It analyses the relationship between network disruptions and deaths and injuries from terrorist attacks to determine whether there

5 Christopher Kedzie (1997) "Communication and Democracy: Coincident Revolutions and the Emergent Dictators", Santa Monica, CA: RAND Corporation, https://www.rand.org/pubs/rgs_dissertations/RGSD127.html (accessed 6 November 2021).

6 P. N. Howard, S. Agarwal & M. Hussain (2011) The Dictator's Digital Dilemma: When Do States Disconnect Their Digital Networks? *Issues in Technology Innovation* vol. 13: pp.1–11. Washington, D.C.: Center for Technology Innovation at Brookings.

7 Access Now and #KeepItOn Coalition, "Shutdown Tracker Optimization Project (STOP)".

8 Fahad Desmukh (2012) "Ban on Cellphone Use in Pakistan," PRI, 31 December 2012, https://www.pri.org/stories/2012-12-31/ban-cell-phone-use-pakistan (accessed 13 September 2020).

9 Archana Chaudhary (2021) "World's Worst Internet Shutdowns Cost India $2.8 Billion in 2020", Bloomberg, 5 January 2021, https://www.bloomberg.com/news/articles/2021-01-05/world-s-worst-internet-shutdowns-cost-india-2-8-billion-in-2020 (accessed 6 November 2021).

is support for the commonly made argument that network disruptions are an important counterterrorism tactic. Using a panel dataset of daily incidents of national-level network disruptions and terrorist attacks globally between 2016 and 2019, a fixed effects regression model shows that national-level network disruptions are not correlated with the number of people killed or injured in terrorist attacks. In addition, there is no correlation between a ban on social media platforms – specifically Facebook, Twitter and WhatsApp – and deaths or injuries from terrorist violence. This analysis has some limitations that make it difficult to make a causal claim, such as the non-random assignment of the treatment (that is, network disruptions) and the absence of a control variable to capture increased security around network disruptions. In general, these findings offer another perspective on the debate on network shutdowns, which often centres on the implications of shutdowns for human rights and democratic engagement and does not typically delve into empirical evidence on what network shutdowns can or cannot accomplish.

The scant existing academic literature on the relationship between communication technology and the organisation and execution of violence offers conflicting findings. Some scholars argue that access to such communication technology as mobile phones and the Internet allows members of terrorist organisations to coordinate with each other and plan attacks,[10] while others argue that communication technology is a tool that civilians can use to report terrorist activity to governments, thereby hindering violence.[11] A few scholars have examined empirical evidence on levels of mobilisation and violence during network shutdowns to argue that network disruptions actually lead to an increase in violence and political mobilisation. Hassanpour shows this to be the case in Egypt,[12] while Rydzak presents a similar scenario in India;[13] in both cases network shutdowns were tied to an increase in certain forms of political mobilisation rather than a decline. In the case of Pakistan, Mustafa shows that terrorist attacks declined when the government imposed network shutdowns but increased the following day.[14] Much of the existing work on the link between communication networks and violence is based on country-specific analyses. This report analyses the impact of network disruptions on terrorist violence in countries around the world using a rich cross-country panel dataset, thereby offering generalisable findings that add to our existing knowledge.

10 Jan H. Pierskalla and Florian M. Hollenbach (2013) "Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa", *American Political Science Review* vol. 107, no. 2, pp: 207–24. https://doi.org/10.1017/S0003055413000075.

11 Jacob N. Shapiro and Nils B. Weidmann (2015) "Is the Phone Mightier Than the Sword? Cellphones and Insurgent Violence in Iraq", *International Organization* vol. 69, no. 2, pp: 247–74. https://doi.org/10.1017/S0020818314000423.

12 Navid Hassanpour (2014) "Media Disruption and Revolutionary Unrest: Evidence from Mubarak's Quasi-Experiment", *Political Communication* vol. 31, no. 1, pp: 1–24. https://doi.org/10.1080/10584609.2012.737439.

13 Jan Rydzak (2019) "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330413 (accessed 21 September 2021) .

14 Fatima Mustafa (2021) "Can Cellphone Shutdowns Stop Terrorist Violence? Evidence from Pakistan", *Terrorism and Political Violence*, https://doi.org/10.1080/09546553.2021.1908270.

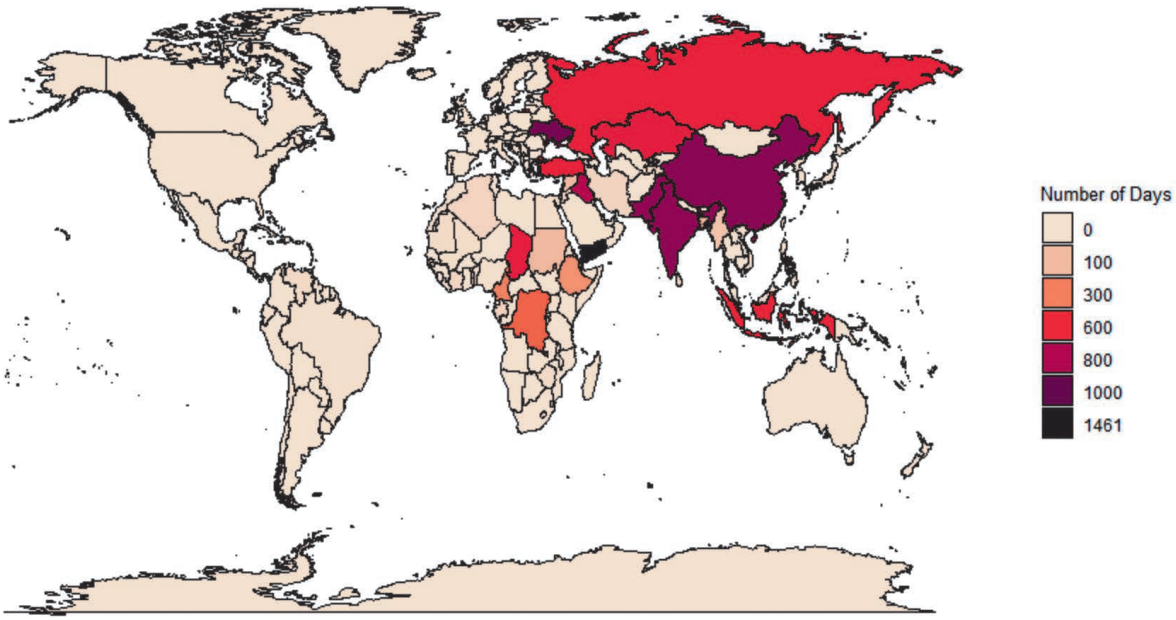
Contents

1 Introduction

At the time of writing, Sudan is in the midst of an ongoing Internet shutdown that was initiated when its military took over in a coup on 25 October 2021. The Internet shutdown has now lasted for sixteen days and counting, despite orders from a court in Sudan that Internet service be restored. While the Internet shutdown has obscured the events unfolding in Sudan, some accounts suggest that it is associated with an increase in militia attacks in Darfur.[15] Earlier this year, on 1 February 2021, Myanmar faced a national-level network shutdown as the army staged a coup. While mobile phone and Internet services were restored later in the day, protests against the coup gathered steam over the next few days, prompting the government to suspend access to Facebook, Instagram and Twitter on 4 and 5 February. The government also continued to suspend Internet services intermittently over the next few weeks.[16] These are just two cases drawn from the 21 countries that have relied on network shutdowns in the first five months of 2021. There has been an increase in network disruptions from 2016 to 2019, with almost three times the number of disruptions in 2019 (213 disruptions) compared to 2016 (75).[17] Map 1 below shows the number of days with network disruptions in different countries around the world from 2016 to 2019 and includes both local- and national-level network disruptions. The country with the highest number of days with network disruptions in this period was Yemen, followed by Ukraine, Bahrain, China, India and Pakistan. Yemen imposed a ban on Skype for the entire duration of the period covered by the map, in addition to other local-level, often short-lived disruptions in access to communication technologies.

As the cases of Sudan and Myanmar show, government-mandated network blackouts are often associated with an increase in government repression. Evidence from other contexts supports this conclusion as well as pointing to the role of network disruptions in concealing government repression from external scrutiny.[18] As Courtney Radsch, a human rights activist interviewed for this report, argued, network disruptions make it difficult for reporters and others to share information on the events unfolding in the countries that face such shutdowns. In addition, Radsch contended that it is important to think about whether network disruptions are necessary or proportionate in terms of the potential harm that they might cause, criteria by which it is difficult to justify any network disruption.[19] This is in line with a report by the United Nations Human Rights Office of the High Commissioner, which argues that a constraint on freedom should meet certain conditions such as "the need for restrictions to

15 Reuters (2021) "Sudan Court Orders Restoral of Internet, But No Sign of Services Returning", Reuters, https://www.reuters.com/world/africa/court-orders-restoration-sudan-internet-access-2021-11-09/ (accessed 12 November 2021).
16 Gian M. Volpicelli (2021) "The Draconian Rise of Internet Shutdowns", *Wired*, https://www.wired.co.uk/article/internet-shutdowns (accessed 12 November 2021).
17 Access Now and #KeepItOn Coalition, "Shutdown Tracker Optimization Project (STOP)".
18 Amnesty International, the Hertie School and Internet Outage Detection and Analysis (2021), "A Web of Impunity: The Killings Iran's Internet Shutdown Hid", https://iran-shutdown.amnesty.org/ (accessed 5 November 2021).
19 Courtney Radsch, interview by author over telephone, 26 October 2021.



Map 1: Number of Days with Local- and National-Level Network Disruptions in Countries (2016–2019)

be necessary, proportional, and non-discriminatory".[20] The United Nations regards the use of Internet shutdowns to be disproportionate and a violation of human rights and urges governments to allow Internet access to their populations.[21] Instead, governments often rely on claims about "national security" and "counterterrorism" to justify network disruptions as necessary, raising questions about the relationship between network disruptions and terrorist violence that this report will focus on.

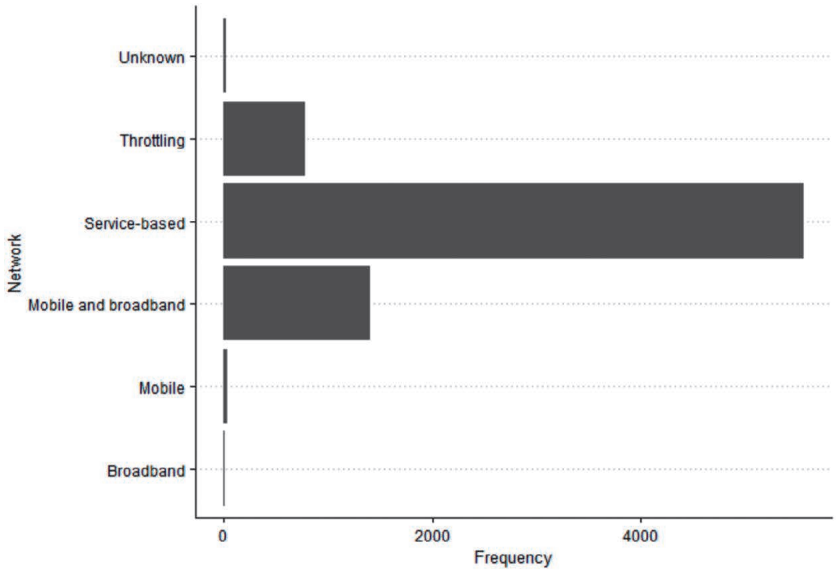
The next section of this report will offer an overview of the data on network disruptions between 2016 and 2019. This will be followed by a section that discusses the state of our existing knowledge on the impact of network disruptions on violence specifically and mobilisation more broadly. Next, the report will delve into a preliminary analysis of the relationship between network disruptions and terrorist violence using a fixed effects regression model and will offer a discussion of the results of this analysis. The final part of the report briefly examines other ways in which governments rely on communication technologies and social media platforms to tackle terrorism.

20 United Nations Human Rights Office of the High Commissioner, "Internet Shutdowns and Human Rights", https://www.ohchr.org/Documents/Press/Internet-shutdowns-and-human-rights.pdf (accessed 15 November 2021).

21 Frank La Rue (2011), "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue", in United Nations, General Assembly, Human Rights Council, https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (accessed 15 November 2021).

2 National-Level Network Shutdowns Across Countries (2016–2019)

Countries around the world rely on different tactics to control and manipulate access to communication technologies. Wilson argues that governments often target: a) the nodes of the Internet or the end users through spyware and viruses; or b) the physical lines and infrastructure that are central to the operation of the Internet; or c) the application layer, which often involves cutting off access to social media platforms and creating local alternatives.[22] According to Wilson, what determines why governments choose one approach over another is their technical know-how as well as the network layout and infrastructure in their countries.[23] While all of these forms of network disruption are problematic, this report focuses specifically on government manipulation of the physical infrastructure of the Internet to create network shutdowns and throttling as well as manipulation of the application layer to ban certain social media platforms. Network disruptions, as used in this report, include disconnecting Internet services, cutting off cell phone services, targeting specific platforms and services (for example, banning Facebook, Twitter and WhatsApp) and throttling (slowing down Internet speed to hinder connectivity). It is important to note that this report examines only national-level network disruptions (that is, network disruptions that affect all regions of a country as opposed to local network disruptions) and each separate day of network disruption in a particular country is counted as a separate incident. Graph 1 below shows different forms

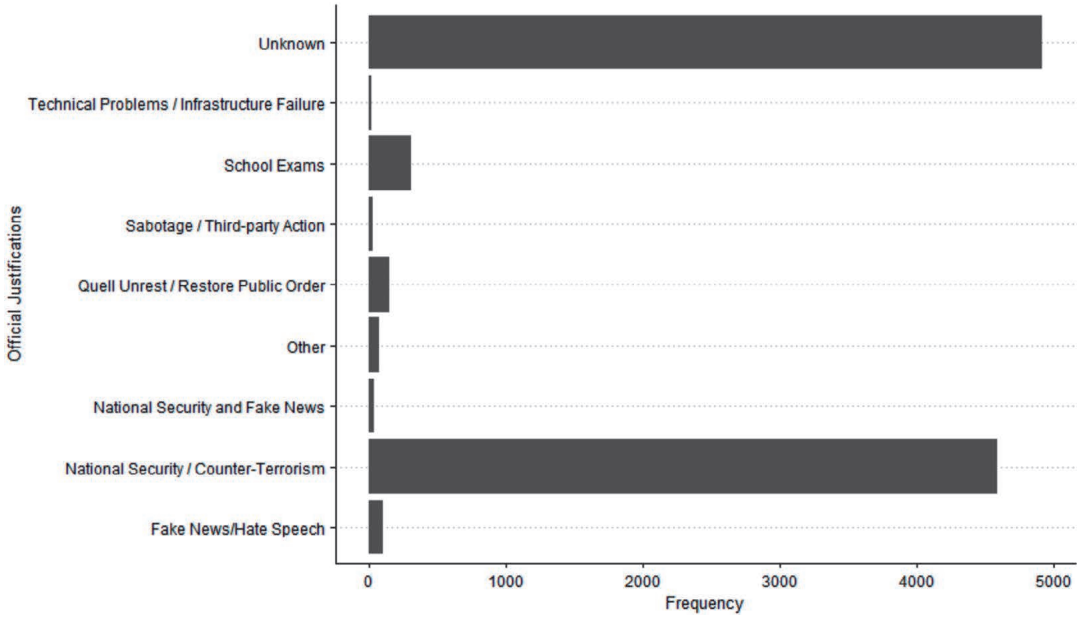


Graph 1: Forms of Network Disruption (2016–2019)

22 Steven Lloyd Wilson (2015) "How to control the Internet: Comparative political implications of the internet's engineering", *First Monday*, vol. 20, no. 2. http://dx.doi.org/10.5210/fm.v20i2.5228.
23 ibid.

of national-level network disruption in countries between 2016 and 2019 based on data from Access Now. At the national level, service-based network disruptions form the overwhelming majority of all network disturbances, followed by mobile and broadband shutdowns.

Governments around the world have offered a range of justifications for these national-level network disruptions, as illustrated in graph 2 below. The graph, also drawing on data from Access Now, shows that governments are often unwilling to comment on network disruptions but when they do, national security or counterterrorism forms the justification for them in a majority of cases. Other justifications for network disruptions include tackling fake news and misinformation, quelling unrest, ensuring that cheating does not occur in school exams and technical problems. In a very small number of cases, it appears that some third-party actors – militants, rebels or others – were possibly responsible for attacking the physical infrastructure of the Internet and disrupting connections.



Graph 2: Government Justifications for Network Disruptions (2016–2019)

The next section delves into the relationship between network disruptions and terrorist violence, examining the existing literature as well as offering preliminary cross-country analysis.

3 Do Network Disruptions Shape Violence and Political Mobilisation?

a. Existing Literature

The primary argument in support of the relationship between network disruptions and violence suggests that communication technologies, such as mobile phones and the Internet, allow terrorist groups to coordinate with each other, overcome collective-action problems and plan attacks. As Shirky argues, communication technologies reduce transaction costs and lower barriers to collective action, allowing individuals to organise for specific ends.[24] Others, such as Castells, have explained in greater detail how being able to convey emotions through communication technologies makes them important in organising social and political movements.[25] Due to the decline in barriers to communication and collective action that communication technology makes possible, terrorist violence, in addition to other forms of collective action, presumably becomes easier to organise. Pierskalla and Hallenbach, testing this hypothesis, show that in Africa expanding cell phone coverage has increased the probability of violence.[26] Other scholars (Warren 2015) make similar arguments about the impact of mobile phone and Internet communication technologies on violence.[27] Mustafa uses data from Pakistan to show that network blackouts lead to a temporary decline in terrorist violence on the day of the shutdown with an increase in violence on the next day when communication networks are accessible.[28] Overall, this evidence suggests that network disruptions should reduce violence, at least on the day of the disruption.

Yet a different body of research shows that network disruptions are associated with an increase in political mobilisation and violence, rather than a decline. Hassanpour examining network disruptions in Egypt,[29] and Rydzak looking at disruptions in India,[30] arrive at a similar conclusion: network disruptions lead to an increase in political mobilisation rather than a decline. Rydzak suggests that non-violent mobilisation needs a higher level of coordination among groups, which becomes difficult during network disruptions, so groups rely on violent mobilisation instead. In addition, other scholars point out that while cell phone and internet networks can be used by violent groups to organise and enact violence, such communication networks can also be used by civilians to report militant activity, thereby containing

24 Clay Shirky (2008) *Here comes everybody: The power of organizing without organizations*, New York: PenguinPress.
25 Manuel Castells (2013) *Communication power*, New York: Oxford University Press; Manuel Castells (2012) *Networks of outrage and hope: Social movements in the Internet age*, Cambridge: Polity.
26 Pierskalla and Hollenbach.
27 T. Camber Warren (2015) "Explosive Connections? Mass Media, Social Media, and the Geography of Collective Violence in African States", *Journal of Peace Research* vol. 52, no. 3, pp: 297–311. https://doi.org/10.1177/0022343314558102.
28 Mustafa.
29 Hassanpour.
30 Rydzak.

violence (Shapiro and Weidmann 2015).[31] Given this line of argument, network disruptions should make it harder for civilians to report terrorist activity to the relevant authorities, as well as making it difficult for law-enforcement officials to coordinate with each other to tackle terrorist threats, as noted by Courtney Radsch.[32]

There is growing evidence that governments sometimes use network disruptions to launch attacks against opposition groups and to repress dissent more broadly. Anecdotal evidence from various network disruptions across countries, such as the one earlier this year in Myanmar,[33] as well as the one in Iran in November 2019,[34] points to an increase in state repression during shutdowns. Anita Gohdes uses data from the civil war in Syria to show that network disruptions in Syria were associated with an increase in government repression and violence against opposition groups.[35] In another paper, she shows that network disruptions are associated with untargeted state repression while government surveillance of communication technologies is tied to more precise and targeted violence against oppositions.[36]

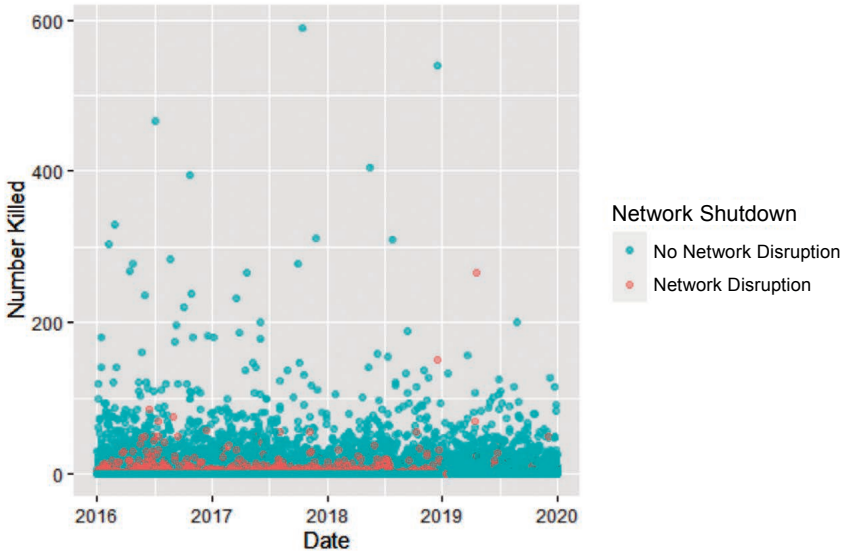
This report adds to the existing debate by presenting a preliminary panel data analysis of the relationship between network disruptions and terrorist attacks. Much of the existing work focuses largely on country-specific studies, which add depth to our understanding of the link between network disruptions and violence. However, many of these studies are not generalisable beyond the specific contexts on which they focus. A cross-country panel data analysis can allow us to move past country-specific idiosyncrasies that might drive the relationship between network disruptions and terrorist violence, and instead offer more generalisable results.

b. Network Disruptions and Terrorist Violence: A Preliminary Analysis

The analysis in this report uses daily-level data on national network disruptions between 2016 to 2019 collected by Access Now and the #KeepItOn Coalition. For the purpose of this analysis, network disruptions (blackouts and throttling) are coded as a dummy variable (variable name: *netwrk_disrup*) with a 1 for a national-level disruption and a 0 otherwise. This forms the primary independent variable in the analysis. In addition, this dataset includes information on whether each incident of network disruption involved a national ban on social media platforms, including Facebook, Twitter, WhatsApp and others. A separate analysis uses dummy variables for the Facebook ban (*facebook*), Twitter ban (*twitter*) and WhatsApp ban (*whatsapp*) as independent variables to understand whether these correlate with deaths and injuries from terrorist violence. Overall, this dataset shows 7,796 unique country-day combinations in 45 countries that witnessed some form of network disruption. The countries with the highest number of days with network disruptions and social media bans in this timeframe include Yemen, Ukraine, China and Kazakhstan.

31 Shapiro and Weidmann.
32 Radsch, interview by author.
33 Volpicelli.
34 Amnesty International, the Hertie School and Internet Outage Detection and Analysis (2021).
35 Anita R. Gohdes (2015) "Pulling the Plug: Network Disruptions and Violence in Civil Conflict", *Journal of Peace Research* vol. 52, no. 3, pp: 352–67. https://doi.org/10.1177/0022343314551398.
36 Anita R. Gohdes (2020) "Repression Technology: Internet Accessibility and State Violence", *American Journal of Political Science* vol. 64, no. 3, pp: 488–503. https://doi.org/10.1111/ajps.12509.

This data on network disruptions has been combined with data on terrorist attacks between 2016 and 2019 attained from the Global Terrorism Database (GTD), made available by the National Consortium for the Study of Terrorism and Reponses to Terrorism. The GTD contains daily-level data on different forms of terrorist violence across countries against civilian and government targets.[37] The analysis in this report relies on two key indicators of terrorist violence from the GTD dataset: the number of people killed (*n_killed*) and the number of people injured (*n_injured*) by terrorist violence. The number of daily deaths from terrorist attacks in the dataset varies from 0 to 590 while the number of daily injuries varies from 0 to 1,532. Graph 3 below shows a scatter plot of the number of people killed in terrorist attacks over time with the points colour-coded to represent network disruptions or their absence.



Graph 3: Number Killed in Terrorist Attacks across Countries (2016–2019)

This analysis includes several control variables. One key variable used from the GTD dataset as a control variable captures the nature of the attack type (*attack_type*) and includes categories such as assassination, hostage taking, armed assault, bombing and others. It is anticipated that the attack type determines the number of deaths and injuries from terrorist attacks, with targeted violence, such as assassinations, more likely to lead to fewer deaths on average compared to attack types such as bombing. Aside from *attack_type*, this analysis controls for year, month and country fixed effects to account for time invariant country-specific characteristics as well as year and month specific shocks. It also includes lagged *n_killed* and lagged *n_injured* variables in the model to account for the correlation in the number of deaths and injuries from terrorist violence over time in different countries. Lag and lead *netwrk_disrup* variables are also included to test for the possibility that network disruptions displace terrorist violence from one day to the next. Network disruptions, especially those that are imposed due to government intelligence about possible unrest, are likely to be associated with increased security,

37 The GTD database uses a broad definition of terrorist violence available at: https://www.start.umd.edu/gtd/.

such as greater police presence. Unfortunately, due to the absence of precise data on police and law-enforcement activity, this analysis does not account for increased security. Thus, in the analysis, the dummy variable for network disruptions also encompasses the effect of increased security on terrorist violence. This makes it more likely for the analysis to show a statistically significant negative relationship between the network disruption variable and the number killed and injured in terrorist attacks. Given that the analysis in this report uses a country, year and month fixed effects model on a panel dataset, standard control variables that are typically included in such analyses, such as population and GDP, are considered to be time-invariant and are not included as control variables.

Using this data, a fixed effects regression model with clustered standard errors is used to analyse the relationship between network disruptions (primary independent variable) and deaths and injuries from terrorist violence (dependent variables). This analysis relies on four waves of data – 2016, 2017, 2018 and 2019 – and the panel variable is country. The condensed results of this analysis are in Table 1 below. Table 2 shows the results of the fixed effects regression model with clustered standard errors for the relationship between social media bans and deaths from terrorist attacks.

VARIABLES	(1) **Number Killed in Terrorist Attacks**	(2) **Number Injured in Terrorist Attacks**
Network Disruption Dummy	1.775	3.088
	(1.608)	(2.472)
Number Killed$_{t-1}$	0.0786**	0.0667**
	(0.0327)	(0.0323)
Network Disruption$_{t-1}$	-2.188	-4.475
	(1.500)	(2.845)
Network Disruption$_{t+1}$	-0.886	0.154
	(0.665)	(0.807)
Attack Types	☑	☑
Year Fixed Effects	☑	☑
Month Fixed Effects	☑	☑
Country Fixed Effects	☑	☑
Constant	3.720***	2.764***
	(0.605)	(0.438)
Observations	210,520	209,813
R-squared	0.063	0.066
Rho	0.082	0.050
Number of Countries	146	146
Avg Observations Per Group	1442	1437

Robust standard errors in parentheses
**** p<0.01, ** p<0.05, * p<0.1*

Table 1: Fixed Effects Regression Model for the Relationship between Network Disruptions and Number Killed and Injured in Terrorist Violence

VARIABLES	(1) Number Killed in Terrorist Attacks	(2) Number Killed in Terrorist Attacks	(3) Number Killed in Terrorist Attacks
Facebook Ban	5.441		
	(3.372)		
Number Killed$_{t-1}$	0.0804**	0.0804**	0.0803**
	(0.0353)	(0.0353)	(0.0353)
Facebook Ban$_{t-1}$	-5.124		
	(3.403)		
Facebook Ban$_{t+1}$	0.140		
	(0.842)		
Twitter Ban		6.153	
		(4.578)	
Twitter Ban$_{t-1}$		-6.570	
		(5.063)	
Twitter Ban$_{t+1}$		1.046	
		(1.504)	
WhatsApp Ban			6.110
			(4.901)
WhatsApp Ban$_{t-1}$			-6.540
			(5.327)
WhatsApp Ban$_{t+1}$			0.775
			(0.639)
Attack Types	☑	☑	☑
Year Fixed Effects	☑	☑	☑
Month Fixed Effects	☑	☑	☑
Country Fixed Effects	☑	☑	☑
Constant	3.730***	3.730***	3.728***
	(0.604)	(0.604)	(0.604)
Observations	210,520	210,520	210,520
R-squared	0.062	0.062	0.062
Rho	0.077	0.077	0.077
Number of Countries	146	146	146
Avg Observations Per Group	1442	1442	1442

Robust standard errors in parentheses
**** p<0.01, ** p<0.05, * p<0.1*

Table 2: Fixed Effects Regression Model for the Relationship between Social Media Bans and Number Killed in Terrorist Violence

The results in Table 1 do not show a statistically significant relationship between network disruptions and the number of deaths and injuries from terrorist attacks. The fact that the network disruptions variable in this analysis also captures the effect of increased security on terrorist violence should have made it more likely to see a statistically significant decline in terrorist violence in the results. Instead, the absence of a statistically significant effect, despite strong reasons to expect it, suggests that network disruptions may not impact terrorist violence. Table 2 shows that there is no statistically significant correlation between Facebook, Twitter and WhatsApp bans and deaths from terrorist violence. The data on network disruptions used in this report shows that there are a number of cases where countries banned certain social media platforms for long durations of time, such as months or years. This is the case in Yemen, which banned Skype for the entire period on which this report focuses. Similarly, citizens of Chad have lacked access to Facebook, Twitter and WhatsApp for more than a year in the period covered by the report. A long-term ban on social media platforms is more likely than long-term mobile phone and Internet blackouts, which typically tend to be short-lived (that is, several days or weeks). Given how lengthy some social media bans have been, it is not clear whether social media bans are associated with an increase in state security to counter violence. The absence of a control variable for security makes it harder to interpret the results. Although these preliminary results should be interpreted with caution, they are not suggestive of a statically significant relationship between social media bans and deaths from terrorist violence. This analysis examines only national-level network disruptions and social media bans, rather than not local-level ones. In addition, the Intraclass Correlation Coefficient is low for all the models in this report – this is because there is substantial variation in the lethality of terrorist attacks over time in each country. Finally, this report also does not limit the data on network disruptions only to those incidents where the official justification was counterterrorism; instead, all national level network disruptions are included.

It is important to note that there are some limitations to this preliminary analysis. First, as mentioned earlier, it does not account for possibly increased security around network disruptions. Second, it is difficult to discount the possibility of reverse causality – that is, levels of terrorist violence might determine the decision to impose network disruptions rather than network disruptions shaping terrorist violence. However, existing research, using a large panel dataset of network disruptions, provides evidence that political violence does not influence governments' decision to limit access to communication technologies.[38] This existing research suggests that the problem of reverse causality may not be significant in the current analysis. Finally, the "treatment", in this case network disruptions, is not randomly assigned, which is problematic. Due to this, the report discusses the link between network disruptions and terrorist violence in terms of correlation rather than making a causal claim. The results in this report should be interpreted as a preliminary examination of the data on network disruptions and terrorist violence, useful as a first step towards a more exhaustive analysis.

38 Jan Rydzak (2018) "The Digital Dilemma in War and Peace: Determinants of Digital Network Shutdown in Non-Democracies", Conference: International Studies Association 57th Annual Convention (ISA 2016), Atlanta, GA, United States.

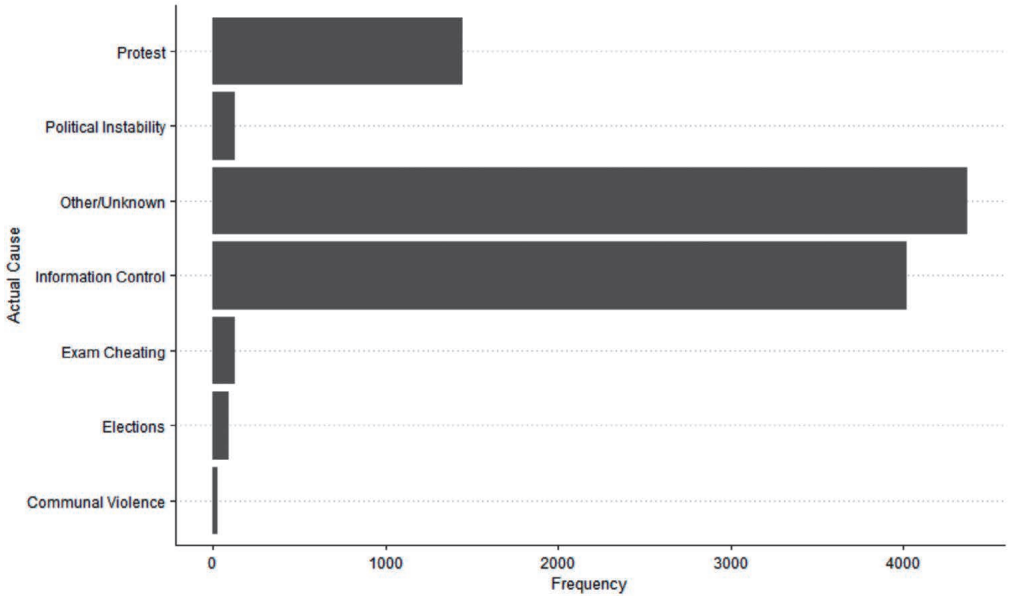
4 Government Approaches to Countering Terrorism through Communication Technology

The preliminary analysis in the report, using data on network disruptions and terrorist violence in countries around the world, indicates that network disruptions are not correlated with terrorist violence. This is in line with some of the existing research that focuses on particular countries to show that network disruptions are either ineffective at tackling violence in the long term or lead to an increase in mobilisation and violence.[39] One possible explanation for these results is that, as governments increasingly use network disruptions and social media bans, terrorist groups have learned to circumvent them through the use of VPN, satellite phones and other kinds of technology. Although Internet blackouts are almost impossible to circumvent, there is some evidence that points to the use of technology to evade social media bans,[40,41] or even disruptions in cell phone access.[42] Another explanation for these results is the one offered by the literature: while a network disruption might hinder coordination among terrorist groups, it also prevents citizens from reporting militant activity and law-enforcement officials from coordinating with each other.[43] This might mean that the net effect of network disruptions on terrorist violence is insignificant.

Why do governments continue to rely on highly expensive measures such as network disruptions in the name of security when there is limited evidence to support their effectiveness? One obvious possibility is that counterterrorism and public safety are simply not the real reasons for government-mandated network disruptions, even though they are the most cited reasons for national-level network disruptions in the data used by this report. In their data on network disruptions, Access Now and the #KeepItOn Coalition includes information on what they think is the actual reason for each network disturbance (as opposed to the official justification offered by governments). This information is visualised in graph 4 below for the years from 2016 to 2019. While the most common official justification for disruptions is counterterrorism, the graph below shows that the most common plausible reason for national-level network disruptions is information control. There is a wealth of anecdotal evidence that suggests that governments do use network disruptions

39 Hassanpour; Rydzak; and Mustafa.
40 Oliver Linow and Fabian Schmidt (2021) “Bypassing Censorship with VPNs – Is That Really Safe?”, dw, https://www.dw.com/en/bypassing-censorship-with-vpns-is-that-really-safe/a-56836645 (accessed 26 November 2021).
41 Amarnath Amarasingam and Rukshana Rizwie (2020) “Turning the Tap Off: The Impacts of Social Media Shutdown After Sri Lanka’s Easter Attacks”, Strategic Communications Project Report, e International Centre for Counter- Terrorism (ICCT) – the Hague, https://icct.nl/app/uploads/2020/10/StratComms-Report-2.pdf (accessed 10 December 2021).
42 Jeremy Kahn (2008) “Mumbai Terrorists Relied on New Technology for Attacks”, *The New York Times*, http://www.nytimes.com/2008/12/09/world/asia/09mumbai.html (accessed 13 September 2021).
43 Shapiro and Weidmann.

to control and contain information. Amnesty International's remarkable investigation with the Hertie School and the Internet Outage Detection and Analysis project showed that network shutdowns in Iran in November 2019 allowed the government to use deadly force against protestors while preventing the flow of information to observers outside the country.[44] Another detailed report, this time by Amarasingam and Rizwie41, shows how the government of Sri Lanka has blocked social media platforms at different times to prevent the spread of misinformation. There are many other similar cases. More generally, governments often continue to use network disruptions because they help them to achieve other ends, such as suppressing dissent or controlling information.



Graph 4: Potential Reasons for Network Disruptions (2016–2019)

While this report looks at the impact of network disruptions and social media bans on terrorist violence, it is important to note that governments also use communication technology to tackle terrorism in other ways. There is research pointing to the use of spyware by governments for the surveillance of groups considered a threat to the state.[45] There has also been an increase in software packages and new technology that claims to use artificial intelligence to analyse the online presence of individuals to make judgements about their ideological affiliations and likelihood of engaging in violence. As a *Guardian* report shows, police departments in the USA have shown an interest in such technology to tackle violence.[46] Another way in which governments seek to tackle terrorism through communication technology is by requesting social media platforms remove extremist content online and provide user data. In its transparency reports,[47]

44 Amnesty International, the Hertie School and Internet Outage Detection and Analysis (2021).
45 Steven Lloyd Wilson (2015).
46 Johana Bhuiyan and Sam Levin (2021) "Revealed: The Software that Studies Your Facebook Friends to Predict Who May Commit a Crime", *The Guardian*, https://www.theguardian.com/us-news/2021/nov/17/police-surveillance-technology-voyager?s=08 (accessed 8 November 2021).
47 Facebook Transparency Reports, https://transparency.fb.com/data/government-data-requests/country/.

Facebook publishes data on government requests for user information that shows that between 2016 and 2019 formal requests for user data often came from countries including the United States, India, the United Kingdom, France and Germany, among others. It is not clear to what extent these requests for user data concern individuals tied to terrorism since that information is not available. While there has been a great deal of research on how terrorist groups operate and recruit through social media and communication technologies, there has been much less focus on understanding how governments use communication technologies to tackle the threat of terrorism. This is an area that requires additional research.

5 Conclusion

This report has examined the impact of national-level network disruptions on terrorist violence between 2016 and 2019. The existing literature on this topic is largely comprised of country-specific studies that are divided on whether network disruptions shape terrorist violence. A preliminary analysis of a large panel dataset of incidents of network disruptions and terrorist violence globally between 2016 and 2019 shows that network disruptions and social media bans do not have a statistically significant correlation with deaths and injuries from terrorist violence. However, there are a number of limitations of this analysis, such as the lack of a control variable for security, the possibility of reverse causality and the fact that network disruptions are non-random. These limitations mean that the results of the analysis should not be taken to reflect a causal link between network disruptions and terrorist violence. Finally, this report briefly touched on other ways in which governments use communication technology to tackle terrorism with further research needed to understand the effectiveness of such strategies in tackling terrorism.

Policy Section

This policy section has been written by Inga Kristina Trauthig, Research Fellow, and Amarnath Amarasingam, Senior Research Fellow, at the International Centre for the Study of Radicalisation (ICSR) at King's College London. It provides policy recommendations and is produced independently by ICSR. Recommendations do not necessarily represent the views of the report author.

The key findings of this report carry corresponding policy implications for governments around the world as they have been at the centre of the analysis around network shutdowns and social media bans assessed in this report. At the same time, technology companies are well aware that they are facing challenges with regard to repeated requests by governments, citing their fight against terrorism and violent extremism, to reveal data related to user accounts. The following section seeks to achieve a threefold aim: first, to deliver concrete policy recommendations for governmental stakeholders; second, to outline policy options and strategic foresight for technology companies; and, finally, in line with [1] and [2], to serve as a reference point for future evaluation of tech policies in order to assess dos and don'ts of technology legislation around the globe.

With this, the policy section ensures that the Global Network on Extremism and Technology (GNET), the academic research arm of the Global Internet Forum to Counter Terrorism (GIFCT), is academically advising and supporting technology companies and policymakers on how to better understand the ways in which terrorists are using information technology. This is designed to fulfil not only GIFCT's pillar of learning, but ultimately to improve prevention and responses to terrorist and violent extremist attacks.

1. Focus: Policymakers

The analysed measures of network shutdowns and social media bans of varying length usually imposed by national governments raise relevant points that should be addressed and factored in by governmental stakeholders planning to pursue similar tactics in the future. In addition to national governments, international (EU, UN, and so on) policymakers, especially security policymakers, should take note and consider the effectiveness of potential network shutdowns and social media bans for their policymaking.

- As this report has outlined, governments often rationalise network shutdowns or social media bans by citing national security concerns and counterterrorism efforts. In order to avoid criticism, **governments should be more transparent about what they are doing, how long such a ban will last and should also publish reports clearly noting** what has been achieved during that time in broad terms. **Time limits on both network shutdowns and social media bans** in legislation are also useful, requiring domestic security stakeholders to apply and provide a rationale for an extension every few weeks. Government should include

human rights safeguards in all counter-terrorism initiatives, including regulation and operational collaborative arrangements which target online space.

- This report has also emphasised not only that it is unknown how these measures have averted extremist violence, but also that these measures do not take into account the broader impact on the economy and innocent bystanders. In addition, and with direct relevance to governmental stakeholders, network shutdowns actually hinder law enforcement's ability to do its job by making it harder for civilians to report terrorist activity to the relevant authorities, as well as making it difficult for law-enforcement officials to coordinate with each other to tackle terrorist threats. Therefore, governments should make sure to **internally coordinate and consult different branches participating in counterterrorism operations** in order to get a balanced picture of whether network shutdowns are worth the effort overall.

- While the previous recommendations are relevant for democratic governments, this report has pointed out **that authoritarian regimes, such as Syria under Bashar al-Assad, use network disruptions** to scale up their already intense government repression and violence against opposition groups, likely because they know that news won't get out as fast. When authoritarian regimes engage in network shut downs, international pressure will often be required to ensure that human rights are being protected.

2. Focus: Technology Companies

Next to the necessary (re-)evaluations that governmental stakeholders should engage in when it comes to network shutdowns and bans on social media, certain steps can be taken by technology companies to work to alleviate some negative repercussions of these measures.

- Similar to how some social media companies publish data on removal requests and information requests they receive from governments, they could also provide evidence of network shutdowns in their transparency reports. This may aid members of the international community in cross-checking data and information coming from activists on the ground, especially in authoritarian regimes.

- In terms of lobbying, tech companies could aim **to work closely with governments to advocate for freedom of access to the Internet**, which is a fundamental part of people's lives around the globe. This is especially important as this GNET report has provided limited support for the argument that network disruptions help counterterrorism efforts, under which they are usually rationalised.

- Finally, while this report has argued that social media bans are not correlated with terrorist violence, there are other forms of violence that might still be tied to access to social media, such as the spread of hate speech and incitements to violence on social media platforms. Therefore, continued efforts to **provide rigorous and appropriate content moderation** is recommended.

3. Focus: Strategic Foresight and Broader Implications

Next to the policy recommendations derived directly from the quoted GNET report, broader implications and strategic deliberations can be retrieved from this study of network shutdowns and social media bans and their corresponding effectiveness at foiling terrorist and violent extremist attacks.

- Since this GNET report has focused on network shutdowns and bans on social media initiated by national governments, a related matter is government requests of social media platforms, asking them to remove accounts related to dissidents and activists, as well as requests to remove certain kinds of content governments deem to be critical of them. To their credit, some social media companies release transparency reports in which they note clearly which governments made these kinds of requests most often and the percentage of these requests that were approved. These transparency reports should be continued and indeed be adopted by social media companies that do not publish such reports, as they provide a window into political interference in activist spaces and how some of these governments treat dissidents.

- Broadly speaking, cultivating a media landscape that is professional and independent is also important. As many of these governments use the spectre of terrorism to engage in practices that violate the human rights of activists, journalists and dissidents, a vibrant media landscape is important for illustrating how governments are wielding institutions, including social media companies, for their own political purposes.

Global Network
on Extremism & Technology

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.