



THE LONDON SCHOOL
OF ECONOMICS AND
POLITICAL SCIENCE ■

Ryng, Julia, Guicherd, Guillemette, Saman, Judy Al, Choudhury, Priyanka & Kellett, Angharad (2023) Internet shutdowns: a human rights issue. *RUSI Journal*, 167(4-5), 50 - 63. <https://doi.org/10.1080/03071847.2022.2156234>

<https://researchonline.lse.ac.uk/id/eprint/117573/>

Version: Published Version

Licence: [Creative Commons: Attribution-Noncommercial-No Derivative Works 4.0](#)

[LSE Research Online](#) is the repository for research produced by the London School of Economics and Political Science. For more information, please refer to our [Policies](#) page or contact lseresearchonline@lse.ac.uk



The RUSI Journal

ISSN: (Print) (Online) Journal homepage: <https://www.tandfonline.com/loi/rusi20>

Internet Shutdowns

A Human Rights Issue

Julia Rying, Guillemette Guicherd, Judy Al Saman, Priyanka Choudhury & Angharad Kellett

To cite this article: Julia Rying, Guillemette Guicherd, Judy Al Saman, Priyanka Choudhury & Angharad Kellett (2022) Internet Shutdowns, The RUSI Journal, 167:4-5, 50-63, DOI: [10.1080/03071847.2022.2156234](https://doi.org/10.1080/03071847.2022.2156234)

To link to this article: <https://doi.org/10.1080/03071847.2022.2156234>



© 2023 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 10 Jan 2023.



Submit your article to this journal [↗](#)



Article views: 293



View related articles [↗](#)



View Crossmark data [↗](#)

Internet Shutdowns

A Human Rights Issue

Julia Ryng, Guillemette Guicherd, Judy Al Saman, Priyanka Choudhury and Angharad Kellett

The internet is a double-edged sword: civilians can mobilise it to assemble and voice dissent, but illiberal regimes can also weaponise it to consolidate power and suppress any form of opposition. Internet shutdowns – intentional disruptions of internet services – represent one method used to limit citizens' freedom of expression, information, peaceful assembly and other associated rights in the name of national security. Julia Ryng, Guillemette Guicherd, Judy Al Saman, Priyanka Choudhury and Angharad Kellett examine the cases of Myanmar and Belarus: two distinct political regimes that nonetheless converge on similar strategies of repression. Through this comparative analysis, the authors highlight how future repression is likely to work and how compelling policy responses can be formulated.

Like so many other technologies, the internet poses a double-edged sword in the context of human rights.¹ While civilians can mobilise the internet to assemble and voice dissent, it can also be weaponised to consolidate power and suppress any form of opposition. Internet shutdowns, meaning intentional disruptions of internet services,² represent one method that limits citizens' freedom of expression, information, peaceful assembly and other associated rights in the name of national security. Access Now, a non-profit organisation defending and extending digital rights worldwide, documented at least 182 internet shutdowns in 34 countries during 2021.³ Their report shows an increase in the number, duration and sophistication of this form of control compared with previous years. This article examines the trends of digital

authoritarianism and securitisation in the cases of Myanmar and Belarus.

In 2021, internet freedom declined dramatically in Myanmar and Belarus. Although state-sanctioned internet shutdowns are not a new phenomenon in either state, Freedom House's 2021 'Freedom on the Net' report documented that Belarus and Myanmar had the greatest global deteriorations, with the latter's score decline being the largest recorded since the project began.⁴ While Myanmar and Belarus are situated within different local and geopolitical contexts, the governing regimes in both countries have employed similar tactics of online repression and justified these actions as emergency measures put in place in the name of national security. The trigger points to internet shutdowns in both states match the trends reported by Access Now, with disruptions occurring during protests, elections and

1. Since the first draft of this article was written, the UN has raised attention on the issue of internet shutdowns through a report by the Office of the High Commissioner for Human Rights and has increased efforts to coordinate international responses against these repressive tactics. See UN High Commissioner for Human Rights, 'Internet Shutdowns: Trends, Causes, Legal Implications and Impacts on a Range of Human Rights – Report of the Office of the United Nations High Commissioner for Human Rights', A/HRC/50/55, August 2022.
2. Alexander Lewis Passah, 'Internet Blackouts in Meghalaya: A Case of Emerging Complexities in the Digital Age', *Media, Culture and Society* (Vol. 43, No. 8, 2021), p. 1515.
3. Access Now, 'The Return of Digital Authoritarianism: Internet Shutdowns in 2021', May 2022, <<https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf>>, accessed 15 June 2022.
4. Adrian Shahbaz and Allie Funk, 'Freedom on the Net 2021: The Global Drive to Control Big Tech', Freedom House, September 2021.



Internet shutdowns limit citizens' ability to exercise certain fundamental rights and are often associated with other abuses of human rights, as governments attempt to hide their crimes. Courtesy of *photon_photo / Alamy Stock*

armed conflicts. Upon investigation, it becomes clear that the true causes of internet shutdowns in Myanmar and Belarus are the suppression of internal civilian upheaval, consolidation of authoritarian power and the limitation of democratic participation. The process through which this occurs can be examined using securitisation theory, which aims to develop strategies to counter and interrogate the 'exceptional' status of security issues. The consequences of internet shutdowns can also be analysed through the human rights framework, with various rights being violated through this repression tactic. Although states bear human rights obligations, framing internet shutdowns as human rights violations invokes responsibility on private companies and the international community to develop, enforce and coordinate prevention and mitigation strategies. This comparative analysis of the trends seen in Myanmar and Belarus, gathered in part through an interview with Access Now in February 2022,⁵ seeks to highlight how repression operates in the Information Age and provide guidance for crafting compelling policy responses by private and public actors.

Securitisation, Human Rights and the Internet

Securitisation theory refers to the process through which an issue is represented as an existential threat that urgently needs to be dealt with in the name of 'security'.⁶ This article adopts an expansive understanding of securitisation, recognising that restrictions to internet access are routine securitisation practices in Myanmar and Belarus, while investigating the increase in their severity and the continued reliance on emergency politics by the securitising actors. The sense of emergency created by securitising an issue allows for securitising actors to legitimately bypass public debate and democratic procedures in adopting exceptional measures responding to said threat.

Following from this, securitisation theory is used in this article to study how governments use public safety and security concerns to justify shutting down the internet. Indeed, securitisation theory has increasingly been used to study discourses and practices related to regulating the internet and cyberspace.⁷ As democratic and non-democratic

5. Author interview with Access Now, via online platform, 25 February 2022.

6. Ole Waever, 'Securitization and Desecuritization', in Ronnie D Lipschutz (ed.), *On Security* (New York, NY: Columbia University Press, 1995).

7. Lene Hansen and Helen Nissenbaum, 'Digital Disaster, Cyber Security and the Copenhagen School', *International Studies Quarterly* (Vol. 53, No. 4, 2009), p. 1155.

Internet Shutdowns

governments refer to cyberspace as a potential arena for the emergence of threats to national security,⁸ securitisation theory is used to develop strategies to counter and interrogate the ‘exceptional’ status of internet shutdowns.⁹

While securitisation theory steers this piece’s critical approach to internet shutdowns, the main aim is to highlight the real-life human rights implications of such practices. The UN Human Rights Council (UNHRC) and other international organisations have repeatedly declared access to the internet a catalyst for the enjoyment of various human rights, particularly the right to freedom of expression, to peaceful assembly and to freedom of association.¹⁰ In addition, studies show that internet shutdowns are often associated with other abuses of human rights, as governments attempt to hide their crimes.¹¹ Internet shutdowns directly interfere with citizens’ livelihoods, limiting access to vital information and resources such as government services, educational institutions, banks, hospitals and airports.¹² Losing the internet is further a matter of immediate safety and security, both in the context of the Covid-19 pandemic and of violent clashes

between governments and protesters in times of national crisis.¹³ Several studies have also highlighted the disproportionate effects of internet shutdowns on minority groups,¹⁴ such as women.¹⁵ Such reports have driven calls for ‘access to internet’ to be declared a human right in itself – empowering those affected by internet shutdowns with language that has the potential to stir the international community and private actors into action.¹⁶ This piece follows this trend, bringing attention to the consequences of state-imposed internet shutdowns.

Belarus and Myanmar

In 2021, Belarus and Myanmar experienced the largest declines in internet freedoms worldwide, as state forces cracked down on internet users amid electoral and constitutional crises.¹⁷

After years of military rule under the Tatmadaw,¹⁸ during which internet access was tightly controlled, expensive and slow, Myanmar’s telecommunication sector saw growth and liberalisation from 2011.¹⁹ Liberalisation of the internet was part of Myanmar’s

8. Louk Faesen et al., ‘Conflict in Cyberspace: Parsing the Threats and the State of International Order in Cyberspace’, The Hague Centre for Strategic Studies (Clingendael), 2019, <<https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/conflict-in-cyberspace/>>, accessed 27 June 2022.
9. Hansen and Nissenbaum, ‘Digital Disaster, Cyber Security and the Copenhagen School’.
10. Human Rights Council, ‘Report of the Working Group on the Universal Periodic Review: Mali’, A/HRC/38/7, April 2018; Human Rights Council, ‘Report of the Working Group on the Universal Periodic Review: Qatar’, A/HRC/42/15, July 2019; European Court of Human Rights, *Cengiz and Others v. Turkey*, December 2015, App Nos 48226/10 and 14027/11.
11. Samuel Woodhams and Simon Migliano, ‘Cost of Internet Shutdowns 2021: Government Internet Shutdowns Cost \$5.5 Billion in 2021’, *Top10VPN*, 2022, <<https://www.top10vpn.com/research/cost-of-internet-shutdowns/2021/>>, accessed 23 May 2022.
12. Kudzayi Savious Tarisayi and Everjoy Munyaradzi, ‘A Teacher Perspective on the Impact of Internet Shutdown on the Teaching and Learning in High Schools in Zimbabwe’, *Human Behavior and Emerging Technologies* (Vol. 3, No. 1, 2020), p. 169; Okwen Mbah, Miriam Nkangu and Zak Rogoff, ‘Don’t Ignore Health-Care Impacts of Internet Shutdowns’, *Nature* (Vol. 559, No. 7715, 2018), p. 477.
13. Amnesty International, ‘Myanmar: New Internet Blackout “Heinous and Reckless”’, press release, February 2022, <<https://www.amnesty.org/en/latest/news/2021/02/myanmar-new-internet-blackout/>>, accessed 5 July 2022.
14. Merlyna Lim, ‘The Politics and Perils of Disconnection in the Global South’, *Media Culture and Society* (Vol. 42, No. 4, 2020), p. 618.
15. Sandra Aceng, ‘The Gendered Impact of Intentional Internet Shutdowns’, *Digital Human Rights Lab*, 3 August 2021, <<https://digitalhumanrightslab.org/blog/the-gendered-impact-of-intentional-internet-shutdowns/>>, accessed 20 May 2022.
16. Frank LaRue et al., ‘Internet Mechanisms for Promotion of Freedom of Expression’, OECD, December 2006, <<https://www.osce.org/fom/23489>>, accessed 3 May 2022; K M Ferebee, ‘The Disconnected: Imagining Material-Infrastructural Rights’, *Prose Studies* (Vol. 38, No. 1, 2016), p. 34; Human Rights Council, ‘Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including Right to Development’, A/HRC/47/L.22, July 2021. It must be noted that restrictions to many human rights can be legally justifiable. International human rights law allows for freedom of expression, for example, to be limited if such restrictions meet the criteria of ‘legality’, ‘necessity’, ‘non-discrimination’ and ‘proportionality’. International Covenant on Civil and Political Rights, 1976, Article 19(3).
17. Shahbaz and Funk, ‘Freedom on the Net 2021’.
18. Tatmadaw is the official name of the armed forces of Myanmar.
19. International Crisis Group, ‘Myanmar’s Military Struggles to Control the Virtual Battlefield’, Asia Report No. 314, 2021.

democratisation process, which led to the victory for Nobel Peace Prize laureate Aung San Suu Kyi and her National League for Democracy Party (NLD) at the 2012 by-election and 2015 general election. Yet, the 2008 Constitution continued to grant the Tatmadaw control over the country's most important ministries. The constitution explicitly states that the military must 'participate in the National political leadership role of the State', and simultaneously grants military leaders immunity from prosecution for human rights abuses.²⁰ In November 2020, the NLD claimed a resounding victory in parliamentary elections, taking more votes than in 2015. The military refused to accept this result. In February 2021, it launched a deadly coup and a widespread detainment of members of parliament.²¹ This triggered waves of peaceful protest demanding the return of the country's elected leadership. The military junta quickly cracked down on this, forming a shadow government that led to civil war and a humanitarian crisis. Since the onset of the coup, Myanmar has seen widespread disruption in internet access and services across the country, reflecting a keen awareness on the part of the junta of the importance of the internet, social media and communications technology for suppressing opposition and consolidating control.

In contrast, since its independence from the Soviet Union in 1991, Belarus has been characterised by increasing authoritarianism.²² Among the former Soviet republics, Belarus maintained the closest political and economic ties to Russia. Alexander Lukashenko was elected in 1995 as the first president, and the following decades were marked by his consolidation of power. To remain in power, Lukashenko's government has rigged elections, arrested presidential candidates to dismantle the political opposition, and imposed draconian internet laws to suppress public and civil society protests.²³ This escalated in 2020, when the mass pro-democracy movement emerged in the run-up to the presidential election and triggered

unprecedented state repression against Belarusian online journalists, activists and internet users.²⁴ Under Lukashenko's ongoing rule, there have been widespread governmental restrictions on freedom of speech, of the press, of peaceful assembly and of religion that continue today. In February 2022, as the conflict in Ukraine escalated, Lukashenko further strengthened his grip on power through a constitutional referendum,²⁵ which granted him lifelong immunity from prosecution, allowed him to secure further time in office, and permitted Russian troops and nuclear weapons to be permanently stationed in Belarus.²⁶

A comparative analysis of the internet restrictions in Myanmar and Belarus points to trends in internet securitisation at times of political turmoil, and pro-democracy movements that threaten governments' attempts to consolidate control. The timing of these shutdowns is consistent with studies that have shown that 'Internet censorship is targeted during sensitive political time periods and periods of potential power transitions, such as elections and large-scale protests'.²⁷ Despite significant differences between Belarus and Myanmar, the similarity in behaviour and tactics of two states battling with authority crises sheds light on what repression looks like in the Information Age.

Justifying Internet Shutdowns

Myanmar's ruling military junta and Lukashenko's authoritarian government justify their actions as 'necessary' in the face of a national security threat. The use of securitisation discourse justifies reliance on emergency measures, which in turn allow governing bodies to draft, adopt and amend existing laws without due process. A brief analysis of the complex legal frameworks constructed in Myanmar and Belarus to justify and enact internet restrictions illustrates how securitisation operates.

-
20. Bertil Lintner, 'Why Burma's Peace Efforts Failed to End Its Internal Wars', United States Institute of Peace, Report No. 169, October 2020.
 21. Audrey Wilson, 'Myanmar's Tumultuous Year', *Foreign Policy*, December 2021.
 22. *The Economist*, 'Why Belarus is Called Europe's Last Dictatorship', 25 May 2021.
 23. Mike Harris, 'In Belarus, The Freedom of The Internet Is At Stake', *The Guardian*, 6 January 2012.
 24. Madeleine Schwartz, 'Adapting to Autocracy: How Journalists in Belarus, Jordan, Thailand, and Nicaragua are Fighting Back Against Government Intimidation', *Nieman Reports* (Vol. 75, No. 1, 2021), p. 26.
 25. Results of this referendum have not been recognised by Western states. *Reuters*, 'Belarus Referendum Approves Proposal to Renounce Non-nuclear Status – Agencies', February 2022.
 26. *Ibid.*
 27. Ramakrishna Padmanabhan et al., 'A Multi-Perspective View of Internet Censorship in Myanmar', *FOCI'21*, Virtual Event, August 2021, <<https://dl.acm.org/doi/pdf/10.1145/3473604.3474562>>, accessed 20 June 2022.

Internet Shutdowns

In the early stages of the coup in Myanmar, Deputy Information Minister Brigadier-General Zaw Min Tun announced that the military had ‘no plan’ to restore internet services.²⁸ Blaming the ‘internet and social media’ for the riots, the deputy justified the restrictions in the name of preserving ‘the rule of law and stability’. Under the 2013 Telecommunications Law, the government has the authority to direct telecommunication companies to suspend services or to block or filter content ‘when an emergency situation arises for public interests’.²⁹ The vaguely worded provision does not include due process or substantive safeguards that would limit the government’s powers to direct a licence holder to take these steps, nor does it provide a definition of ‘emergency situation’.³⁰ Myanmar’s democratically elected NLD government had previously invoked the law during the Rohingya crisis – shutdowns were ordered in the conflict regions to tackle the ‘threats to the public’ that the internet represented.³¹ This is a prime example of securitisation – by framing the internet and social media as a threat, the military can rely on existing ‘emergency’ legislation to restrict the expression of dissent. This discourse then allows the junta to put forward new laws that limit citizens’ access to the internet, including a ‘draconian cybersecurity bill’ which has been in preparation for several years but is yet to be adopted.³² The proposed law directly threatens citizens’ rights to privacy and expression by granting extensive powers to the authorities and allowing the junta to access user data, block websites, prosecute critics and order internet shutdowns. Especially concerning is the criminalisation of the use of virtual private networks (VPNs), which will heavily impact the work of civil society organisations and journalists that are key to providing information

about the military’s human rights violations to the outside world.

Myanmar’s ruling military junta and Lukashenko’s authoritarian government justify their actions as ‘necessary’ in the face of a national security threat

In the case of Belarus, the scale of the crackdown on independent online journalism and communication points to the fact that authorities view online activity as a primary driver of civic unrest. The government has not owned up to its use of internet shutdowns, blaming external actors for early internet outages instead.³³ Its role as orchestrator of the shutdown was, however, highlighted by the private information and communications technology (ICT) company A1, which acknowledged that ‘state bodies’ requested the reduction of 3G networks across Minsk in August 2020.³⁴ More covertly, internet securitisation occurred through laws designed to counter ‘extremism’ and protect ‘national security’. In 2021, the government passed a range of amendments de facto authorising the implementation of internet shutdowns, the banning of online or media websites, and the restriction of the free flow of information.³⁵ Most significantly, it amended the Telecommunications Law to allow it to shut down or limit the operation of telecommunications networks and facilities in response to alleged threats to national security involving the internet.

28. International Crisis Group, ‘Myanmar’s Military Struggles to Control the Virtual Battlefield’.

29. Telecommunications Law 2013 (Myanmar), Article 77.

30. Myanmar Centre for Responsible Business, ‘Policy Brief: The Legal and Policy Framework for Information Communication Technology (ICT) In Myanmar: Implications for Human Rights’, Draft for Myanmar Digital Rights Forum, January 2019, <https://www.myanmar-responsiblebusiness.org/pdf/2019-Policy-Brief-Myanmar-ICT-Legal-Framework_en.pdf>, accessed 8 June 2022.

31. Human Rights Watch, ‘Myanmar: End World’s Longest Internet Shutdown’, June 2020, <<https://www.hrw.org/news/2020/06/19/myanmar-end-worlds-longest-internet-shutdown>>, accessed 6 June 2022.

32. Human Rights Watch, ‘Myanmar: Scrap Draconian Cybersecurity Bill’, February 2022, <<https://www.hrw.org/news/2022/02/15/myanmar-scrap-draconian-cybersecurity-bill>>, accessed 22 May 2022.

33. Belta.by, ‘Lukashenko: internet v Belarusi otkljuchajut iz-za granitsy, eto ne initsiativa vlasti’ [‘Lukashenka: Internet in Belarus is cut off from abroad, this is not an initiative of the authorities’], 10 August 2022, <<https://www.belta.by/president/view/lukashenko-internet-v-belarusi-otkluchajut-iz-za-granitsy-eto-ne-initsiativa-vlasti-402299-2020>>, accessed 12 August 2022.

34. Shahbaz and Funk, ‘Freedom on the Net 2021’.

35. *Ibid.*

The above highlights a pattern reported by practitioners in this field.³⁶ Modern authoritarian actors consolidate their power by implementing emergency legislation and amending laws to repress and censor ICTs, amounting to ‘digital authoritarianism’. But why change the laws when the political system allows for the ruling actor to violate them without consequences? Arguably, it is for the illusion of legitimacy. Keeping up online repression with existing legal frameworks, amended to expand the power of the authoritarian ruler, helps to legitimise their actions against citizens to the international community – they can be seen to be in line with domestic law. Further, it impedes the ability of civilians and local civil society organisations to use the law as a recourse to claim their rights. Complex legal frameworks make claims of human rights violations more difficult to prove; state actors can point to the emergency and amended laws as markers of the ‘legality’ of restrictions to freedoms. In this context, transnational actors play a crucial role in monitoring the impacts of these laws, assessing them against internationally recognised human rights standards and holding governments to account on a global scale.

Modern authoritarian actors consolidate their power by implementing emergency legislation and amending laws to repress and censor ICTs, amounting to ‘digital authoritarianism’

Tactics

Internet shutdowns in Myanmar and Belarus exemplify the different tactics that governments around the world resort to in order to limit their

citizens’ access to internet services. These can be broadly categorised into overt blackouts, filtration of available websites, the use of checkpoints to identify VPN users, intimidation and use of economic disincentives.

Blackouts

In the early days of the coup, Myanmar was plunged into a communications blackout as the army forced all telecom operators to switch off phone and internet connections.³⁷ Businesses and banks affected by the shutdown pointed to the immense economic consequences of widespread shutdowns.³⁸ Their pressure led the military to restore access. However, blackouts of internet and phone services continue to take place on a regional level in areas where fighting between the military and resistance groups has intensified.³⁹ Similarly, on 9 August 2020 – election day – the Belarusian government initiated a nationwide blackout of the internet which lasted for 61 hours. Blackouts continued to occur in the aftermath of the election, particularly during the mass pro-democracy protests that took place each Sunday for the following two months.⁴⁰

Filtered Access

Due to the high cost of blackouts, governments of both countries have resorted to restoring a heavily filtered version of the internet, enabled by issuing blocking orders to telecommunications companies. During the 2020 election period and the ensuing protests, online information flow was heavily limited in Belarus.⁴¹ Some political and civil society websites were blocked, content critical of the government was removed, and Telegram channels organising protests were labelled as ‘extremist’. Popular social networks such as YouTube, Facebook, Instagram and TikTok were also taken off the internet. Similarly, after the coup, the Tatmadaw in Myanmar quickly ordered telecommunications operators to block access to social media platforms. In a country where Facebook is seen as synonymous with the

36. Author interview with Access Now.

37. *Economic Times*, ‘A Digital Firewall in Myanmar, Built with Guns and Wire Cutters’, *Bloomberg*, February 2021, <<https://economictimes.indiatimes.com/news/defence/a-digital-firewall-in-myanmar-built-with-guns-and-wire-cutters/articleshow/81188945.cms?from=mdr>>, accessed 7 July 2022.

38. International Crisis Group, ‘Myanmar’s Military Struggles to Control the Virtual Battlefield’.

39. *The Irrawaddy*, ‘Myanmar Junta’s Internet Blackout Violates Residents’ Rights’, *The Irrawaddy*, September 2021, <<https://www.irrawaddy.com/news/burma/myanmar-juntas-internet-blackout-violates-residents-rights.html>>, accessed 6 June 2022.

40. Shahbaz and Funk, ‘Freedom on the Net 2021’.

41. *Ibid.*

Internet Shutdowns

internet – half of Myanmar’s population are users – the measures had an immediate effect on people’s ability to access valuable information, communicate and organise protests.⁴²

Checkpoints for Identifying VPN and Social Media Users

The above restrictions led to mass gravitation towards VPN services. A VPN allows one to bypass localised website blocks and permits citizens to access censored information, such as critical commentary on the government, without being tracked and monitored. In an attempt to scare people off these platforms, authorities in both Myanmar and Belarus have been reported to stop civilians in the streets and search their mobile devices, looking for illegal social media content or VPNs.⁴³

Intimidation

The threatening atmosphere created by these arbitrary day-to-day checks has been strengthened by widespread intimidation of civil society and opposition leaders online. In Myanmar, online freedom of expression was already in decline under the NLD government, which was using vaguely worded clauses in a range of laws to jail activists and ordinary internet users for social media posts.⁴⁴ Once in power, the junta extended the range of these laws and called on them to arrest regime opponents with high-profile social media presence for allegedly spreading disinformation and threatening the public.⁴⁵

In Belarus, people are being arrested for reposting information from sources classified by the Ministry of Internal Affairs as ‘extremist’ in personal correspondence.⁴⁶ In May 2021, the Belarusian government went as far as to order a Ryanair flight to divert to Minsk so it could arrest Raman Pratasevich, cofounder and editor-in-chief of the country’s most popular online opposition news outlet, NEXTA.⁴⁷ Pratasevich later appeared in a video in which he confessed to organising anti-government protests. His supporters said visible marks on his face in the video indicated that he had been beaten.⁴⁸

Economic Barriers and Incentives

Myanmar has also erected economic barriers to limit citizens’ internet use. Last January, in a move to further curtail internet use and raise government revenues in a context of fiscal boycott by the population, the government raised the corporate tax rate for mobile and fixed-line internet providers from 5 to 15%.⁴⁹ It also put in place a one-time ‘activation fee’ of 20,000 kyats (\$11) for each new SIM card, on top of the price of the card itself.⁵⁰ The soaring internet prices, coupled with slower internet, continue to have a great impact on everyday working life. In a country where 40% of the population is living below the national poverty line,⁵¹ these costs will likely dissuade many people from accessing the internet. Instead, people may resort to greater use of phone calls and SMS, which are less expensive but much easier to track.

By contrast, internet access in Belarus is affordable for at least 90% of the population.⁵²

42. Beh Lih Yi, “Everything is Uncertain”: Myanmar Coup Hits Digital Entrepreneurs’, Thomson Reuters Foundation, February 2021, <<https://news.trust.org/item/20210209123537-6xlzh>>, accessed 7 June 2022.
43. International Crisis Group, ‘Myanmar’s Military Struggles to Control the Virtual Battlefield’.
44. *Ibid.*
45. *Ibid.*
46. Reform.by, ‘Semejnuju paru v devjatyj raz osudili za repost s «jektivisticheskij» kanalov v lichnoj perepiske Istochnik’ [‘Married couple convicted for the ninth time for reposting from “extremist” channels in personal correspondence’], November 2021, <<https://reform.by/274659-semejnuju-paru-v-devjatyj-raz-osudili-za-repost-s-jektivisticheskij-kanalov-v-lichnoj-perepiske>>, accessed 20 May 2022.
47. Luke Harding, ‘Belarus Journalist’s Father Says Video Confession Carried Out under Duress’, *The Guardian*, 25 May 2021.
48. *Ibid.*
49. Aung Naing, ‘Junta Says Hefty New Telecoms Taxes will Curb “Extreme Use of Internet Services”’, *Myanmar Now*, January 2022, <<https://www.myanmar-now.org/en/news/junta-says-hefty-new-telecoms-taxes-will-curb-extreme-use-of-internet-services>>, accessed 18 June 2022.
50. *Ibid.*
51. World Bank, ‘Myanmar Economy Remains Fragile, with Reform Reversals Weakening the Outlook’, press release, 21 July 2022, <<https://www.worldbank.org/en/news/press-release/2022/07/21/myanmar-economy-remains-fragile-with-reform-reversals-further-weakening-the-outlook#:~:text=About%2040%20percent%20of%20the,Myanmar%20Economic%20Monitor%20released%20today>>, accessed 26 July 2022.
52. Shahbaz and Funk, ‘Freedom on the Net 2021’.

However, the high accessibility of internet and phone services must be viewed in the context of strong state control of the ICT sector. The state-owned telecommunications company Beltelecom commands 81% of the broadband market. Foreign tech companies such as Google have preferential agreements with Beltelecom, allowing the latter to engage in predatory pricing.⁵³ The expansion of the digital economy is an important part of the national development strategy of Belarus,⁵⁴ with the ICT sector generating growth while simultaneously providing a prime space for control over information and communication over the majority of the population.

Global Policy Response

The human rights system creates obligations on states to protect their citizens. As a result, the governments of Myanmar and Belarus should ultimately be held accountable for the disproportionate and unnecessary use of internet shutdowns and their human rights impacts. However, neither Lukashenko's government nor Myanmar's junta operate in a vacuum. The actions and reactions of the international community, the private sector and civil society affect the scale and impact of internet shutdowns. Investigating the responses from these transnational actors allows one to identify a set of strategies to mitigate the human rights impact of digital authoritarianism.

The International Community

The governments in both Myanmar and Belarus have sought to justify internet shutdowns by framing the internet as a threat to national security, alluding to an internationally recognisable space in which

human rights may be restricted. The act of engaging with this language and justifying actions in a way the international community respects presents an opportunity. Indeed, their engagement in practices of legitimisation⁵⁵ suggests that criticism or actions from international actors may have an impact on national practices and help to prevent human rights abuses. The international community now concedes that the internet shutdowns imposed in Belarus and Myanmar do not meet the international human rights standards of justifiable restrictions.⁵⁶ But in practice, international action has been weak.

Neither Lukashenko's government nor Myanmar's junta operate in a vacuum

While the coup and ensuing violence in Myanmar have drawn near-universal condemnation, the response has been 'ineffectual' according to UN High Commissioner for Human Rights Michelle Bachelet.⁵⁷ Neither political actions on the part of the UN nor the ASEAN bloc, nor international sanctions, have yielded any change in the Tatmadaw's campaign of violence. In the case of Belarus, the EU's 'carrot and a stick' strategy of putting sanctions in place while offering a reward for a 'change of course' following the violent episode of 2020⁵⁸ has not had much impact on governmental practices. Furthermore, the international community has generally failed to take robust action in opposition to state-imposed internet shutdowns as forms of violence in themselves. Arguably, geopolitics play a role in this apprehension, as China and Russia support the Tatmadaw and Lukashenko's government. Until May 2021, UN Security Council discussions on developments in

53. *Ibid.*

54. Kirill Laptev and Pavel Lashuk, 'The Technology, Media and Telecommunications Review: Belarus', *Law Review*, January 2022, <<https://thelawreviews.co.uk/title/the-technology-media-and-telecommunications-review/belarus>>, accessed 8 July 2022.

55. States looking to be recognised as worthy members of the international community. See Thomas M Franck, *The Power of Legitimacy among Nations* (Oxford: Oxford University Press, 1990).

56. *Article 19*, 'Unplugged in Myanmar: Internet Restrictions Following the Military Coup', July 2021, <<https://www.article19.org/resources/unplugged-in-myanmar-internet-restrictions-following-the-military-coup/>>, accessed 4 June 2022; UN News, 'Internet Shutdowns Now "Entrenched" in Certain Regions, Rights Council Hears', July 2021, <<https://news.un.org/en/story/2021/07/1095142>>, accessed 16 July 2022; Human Rights Council, 'Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development: 15 June 2021', A/HRC/47/24/Add.2, June 2021.

57. UN News, "'Urgent, Renewed Effort" Needed to Restore Civilian Rule in Myanmar: Bachelet', January 2022, <<https://news.un.org/en/story/2022/01/1110792>>, accessed 16 June 2022.

58. European Commission, 'The European Union Outlines a €3 Billion Economic Support Package to a Future Democratic Belarus', press release, 28 May 2021, <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2685>, accessed 28 June 2022.

Internet Shutdowns

Belarus were limited to informal meetings, with both China and Russia maintaining that it was an internal matter with no effect on the broader stability of the region.⁵⁹ Similarly, Russia and China blocked the UN Security Council's official condemnation of the military coup in Myanmar.⁶⁰

In Myanmar, China and Russia have played key roles in explicitly endorsing the military government and implicitly supporting its repressive activities within the digital sphere. China has deep-rooted interests in Myanmar. It wants to: protect its infrastructure projects and investments; prevent civil war near its borders; maintain its dominance over the junta; and decrease the influence of the US.⁶¹ However, some military leaders are wary about China's growing sphere of influence, which has resulted in the junta seeking to strengthen its relations with Russia.⁶² Myanmar has been importing military equipment from Russia in return for raw materials, an import which has become critical with Russia's invasion of Ukraine.⁶³ Similarly, due to increasing Western pressure and isolation, Belarus has had to rely more heavily on Russia and China and is predicted to strengthen its defence cooperation with Russia and its economic ties with China.⁶⁴

In both cases, governmental repression within the digital sphere is aligned with that in Russia and China, which implicitly endorse a repressive approach abroad and domestically. Russia's and China's strategies of digital authoritarianism include the exportation of their models of online censorship and repression to other countries.⁶⁵ The Chinese model focuses more on censorship, proliferating

surveillance and monitoring systems to other countries based on its 'Great Firewall' of state-controlled internet and repression. Meanwhile, Russia's model focuses less on information filtering and more on a 'repressive legal regime and intimidation of key companies and civil society, a lower-cost ad hoc model more easily transferable to most countries'.⁶⁶ In both Myanmar and Belarus, various elements inspired by the Russian and Chinese digital authoritarianism models can be identified.

In Myanmar, China and Russia have played key roles in explicitly endorsing the military government and implicitly supporting its repressive activities within the digital sphere

In addition to geopolitical tensions dissuading the international community from robust action against Belarus's and Myanmar's authoritarian strategies, the (mis)understanding of violence may also be a factor. Political, legal or economic pressure seems to be reserved for 'serious' physical abuse, despite the fact that online repression often leads to or occurs alongside such human rights violations.⁶⁷ The idea that offline human rights are more important to protect than online

-
59. Security Council Report, 'Arria-Formula Meeting on the Situation in Belarus', *What's In Blue*, October 2021, <<https://www.securitycouncilreport.org/whatsinblue/2021/10/arria-formula-meeting-on-the-situation-in-belarus.php>>, accessed 18 June 2022.
 60. *France24*, 'China, Russia Block UN Security Council Condemnation of Myanmar Coup', February 2021.
 61. Lindsay Maizland, 'Myanmar's Troubled History: Coups, Military Rule, and Ethnic Conflict', *Council on Foreign Relations*, January 2022, <<https://www.cfr.org/backgrounder/myanmar-history-coup-military-rule-ethnic-conflict-rohingya#chapter-title-0-7>>, accessed 15 June 2022.
 62. International Crisis Group, 'Myanmar's Military Struggles to Control the Virtual Battlefield'.
 63. Allegra Mendelson, "'Stronger Together": Myanmar, Russia Parade Military Relationship', *Al Jazeera*, 27 March 2022.
 64. Huynh Tam Sang and Pham Do An, 'Belarus' Burgeoning Ties with Russia and China', *CHOICE*, February 2022, <<https://chinaobservers.eu/belarus-burgeoning-ties-with-russia-and-china/>>, accessed 5 May 2022.
 65. Elina Sinkkonen and Jussi Lassila, 'Digital Authoritarianism in China and Russia: Common Goals and Diverging Standpoints in the Era of Great-Power Rivalry', Finnish Institute of International Affairs, Briefing Paper 294, 2020 <<https://www.fiia.fi/en/publication/digital-authoritarianism-in-china-and-russia>>, accessed 10 May 2022.
 66. Alina Polyakova and Chris Meserole, 'Exporting Digital Authoritarianism: The Russian and Chinese Models', Brookings, August 2019, <https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf>, accessed 17 June 2022.
 67. In 2021, Freedom House reported that surveillance had increased even in the months prior to the military coup in Myanmar. In early February 2021, the military circulated a draft cybercrime law that would place private data under the military's control – since the coup, security forces have also seized the phones of those arrested and extracted data. Shahbaz and Funk, 'Freedom on the Net 2021'.

ones is a fallacy; the cyber and non-cyber worlds are intrinsically interlinked. The Russian invasion of Ukraine may, however, force the international community to steer away from this fallacy. On the one hand, the ongoing war has already caused – and will likely continue to cause – internet-shutdown-related human rights concerns to be subsumed by larger geopolitical concerns, particularly in Belarus. The country’s status as a quasi-satellite state in the conflict, coupled with the results of the recent constitutional referendum in which Belarus ‘voted’ to renounce its non-nuclear status, means that the international community’s relationship with Belarus is due to become considerably more tense. On the other hand, the tactics used by Russia to control its population in matters of the war should in effect be considered internet shutdowns. News of civilian intimidation and arrests for the consumption of ‘false’ or ‘blocked’ content⁶⁸ mirror the situations in Myanmar and Belarus. International efforts to support people trying to break through the internet firewall⁶⁹ provide hope that state-sanctioned online repression will become recognised as a form of violence that deserves a proportionate response on the part of the international community.

Private Actors

As providers of internet services and developers of technologies that can be used to extract information and facilitate the surveillance of citizens, private companies are key players in mitigating the effects of government-imposed internet regulations. In Myanmar, global reports of human rights abuses forced multinational companies operating on the

ground to evaluate their practices. Social media platforms such as Facebook and TikTok for example took steps to moderate content of the Tatmadaw, diminishing the military’s ability to reach mass audiences.⁷⁰ Unfortunately, competing interests often prevent effective human rights abuse mitigation. The Norwegian telecommunications company Telenor is an example of this. As one of the four telecommunications companies operating in Myanmar, Telenor voiced its disapproval of the draft cybersecurity bill for failing to consider human rights impacts.⁷¹ Yet, since early 2021, Telenor has complied with military requests for data without questioning the legality of these orders.⁷² Telenor is now in the process of selling its Myanmar operations: ‘it is precisely this conflict – between the requirement to comply with local law on the one hand and the concern about human rights and the risk of violations of Norwegian and European sanctions on the other – that leaves Telenor with no choice but to sell Telenor Myanmar.’⁷³ The process of choosing who to sell the operations to is a further missed opportunity by Telenor to act responsibly: the sale is likely to be made to M1Group in collaboration with Shwe Byain Phyu Group.⁷⁴ Both corporations have dubious human rights records and the latter has close ties with the junta, meaning the data of 18 million users may be on the verge of being handed over to the military.⁷⁵ According to Access Now, Telenor’s lack of transparency regarding the sale is making it even more difficult to come up with mitigation strategies to avoid serious human rights abuses.

In the case of Belarus, the government’s repression of the online sphere has been facilitated by the fact that Belarus’s ICT sector is largely state

-
68. Katie Balevic, ‘Moscow Police are Stopping People and Demanding To Read Their Text Messages, Reporter Says’, *Business Insider*, 6 March 2022.
 69. Mikael Thalen, ‘“The Kremlin is Lying”: Hackers Build Tool to Let Anyone Text Russian Citizens about the War in Ukraine’, *Daily Dot*, March 2022, <<https://www.dailydot.com/debug/anonymous-hackers-text-russia-ukraine-war/>>, accessed 17 May 2022.
 70. Fanny Potkin, ‘Facebook Faces a Reckoning in Myanmar After Blocked by Military’, *Reuters*, February 2021; Peter Guest, Emily Fishbein and Nu Nu Lusan, ‘TikTok is Repeating Facebook’s Mistakes in Myanmar’, *Rest of World*, March 2021, <<https://restofworld.org/2021/tiktok-is-repeating-facebooks-mistakes-in-myanmar/>>, accessed 20 May 2022.
 71. Richard Milne, ‘Norwegian Telecoms Chief Denounces Cyber Security Bill in Myanmar’, *Financial Times*, 15 February 2021.
 72. Access Now, ‘Update: Internet Access, Censorship, and the Myanmar Coup’, March 2022, <<https://www.accessnow.org/update-internet-access-censorship-myanmar/>>, accessed 10 May 2022.
 73. Telenor, ‘We Cannot Make Our Employees in Myanmar Delete Data and Break the Law’, February 2022, <<https://www.telenor.com/media/newsroom/announcement/we-cannot-make-our-employees-in-myanmar-delete-data-and-break-the-law-update-by-jorgen-c-arentz-rostrup-evp-and-head-of-telenor-asia/>>, accessed 4 June 2022.
 74. Telenor, ‘Sale of Telenor Myanmar Approved by Myanmar Authorities’, press release, March 2022, <<https://www.telenor.com/media/newsroom/press-releases/sale-of-telenor-myanmar-approved-by-myanmar-authorities/>>, accessed 4 June 2022.
 75. Access Now, ‘Update: Internet Access, Censorship, and the Myanmar Coup’, 2022.

Internet Shutdowns

controlled, allowing the government to throttle or cut connections at will. However, the authoritarian regime relies on purchased technology from private companies to extract information, facilitate surveillance and enforce internet shutdowns. As a result, the responsibility of private actors centres on limiting the potential use of their products to commit human rights violations. Reports from within the country show that the authorities have been using digital forensic technology from the Israeli company Cellebrite to extract sensitive information from the devices of activists and protesters since 2016.⁷⁶ Likewise, products developed by the US-Canadian firm Sandvine facilitated Belarusian authorities' shutdown of the internet during and after the 2020 election.⁷⁷ Such reports led both Cellebrite and Sandvine to terminate their business with the Belarusian government, while Sandvine further indicated that 'custom code was developed and inserted into Sandvine's products to thwart the free flow of information during the Belarus election'.⁷⁸ Despite the termination of sales, the government still uses the purchased equipment.⁷⁹

According to Access Now, the termination of Sandvine's contract with Belarus would have been inconceivable without public pressure emanating from efforts by civil society and the international community. This underlines the ways in which private companies can play a role in limiting further human rights violations, following joint efforts to bring these to the public eye. This chain of influence requires work from civil society and pressure from the international community to hold private actors to account. But as internet shutdowns make reporting abuses extremely difficult in the first place,

it is of utmost importance that companies working on the ground disclose any orders received from state bodies to limit internet access and coordinate with civil society organisations to determine legally and ethically responsible strategies to move forward.

In the case of Belarus, the government's repression of the online sphere has been facilitated by the fact that Belarus's ICT sector is largely state controlled

In addition to those companies directly involved in internet shutdowns, reports of human rights violations and the resultant reputational pressure can persuade *other* multinational companies to cease business with governing bodies. For example, Michelle Bachelet welcomed decisions by some private corporations to withdraw operations from Myanmar on human rights grounds, describing the move as a 'powerful tool to apply pressure on the financing of the military's operations against civilians'.⁸⁰ The business community can further exercise pressure on governments by invoking the economic implications of digital repression. In 2021, for example, the draft cybersecurity bill in Myanmar was 'quietly shelved' in response to the uproar from the business and international trade communities.⁸¹ The economic implications of the bill becoming law were too great, with companies and consumers alike relying on VPN technology to maintain operations.

-
76. Oded Yaron, 'Israeli Phone-Hacking Firm Cellebrite Vowed Not to Sell to Sanctioned Counties. So What's It Doing in Belarus?', *Haaretz*, 18 August 2020, <<https://www.haaretz.com/israel-news/2020-08-18/ty-article/.premium/whats-israeli-phone-hacking-firm-cellebrite-doing-in-sanctioned-belarus/0000017f-e198-d75c-a7ff-fd9dff0b0000>>, accessed 28 May 2022.
 77. Ryan Gallagher, 'American Technology Is Used to Censor the Web from Algeria to Uzbekistan', *Bloomberg UK*, 8 October 2020.
 78. Sean Lyngaas, 'Networking Firm Sandvine Cancels Belarus Contract, Citing "Custom Code" that Aided Censorship', *CyberScoop*, 16 September 2020, <<https://www.cyberscoop.com/sandvine-belarus-contract-censorship-human-rights/>>, accessed 9 June 2022.
 79. Marya Sadouskaya-Komlach, 'How Global Tech Companies Enable the Belarusian Regime – and the Belarusian Revolution', *Advox*, 15 December 2020, <<https://advox.globalvoices.org/2020/12/15/how-global-tech-companies-enable-the-belarusian-regime-and-the-belarusian-revolution/>>, accessed 9 June 2022.
 80. Office of the High Commissioner for Human Rights, 'Myanmar: One Year Into the Coup, Bachelet Urges Governments and Businesses to Heed Voices of the People, Intensify Pressure on the Military', press release, 28 January 2022, <<https://www.ohchr.org/en/2022/01/myanmar-one-year-coup-bachelet-urges-governments-and-businesses-heed-voices-people>>, accessed 20 May 2022.
 81. Thomson Chau and Dominic Oo, 'Myanmar Renews Plans to Curb Internet Usage with VPN Ban', *Nikkei Asia*, 21 January 2022, <<https://asia.nikkei.com/Spotlight/Myanmar-Crisis/Myanmar-renews-plans-to-curb-internet-usage-with-VPN-ban>>, accessed 8 June 2022.

Such a move would have further isolated Myanmar from ASEAN, harking back to the isolationist era and representing the country as hostile to business interests.⁸² It was unsurprising, therefore, that the draft law attracted the ire of commercial interests, in particular as Myanmar's 2021 internet outage cost the country \$2.8 billion.⁸³

The importance of the work carried out by NGOs to combat online repression makes them particularly vulnerable to targeted reactions from securitising actors

Civil Society

Grassroots advocacy, policymaker engagement, technical capacity-building and strategic litigation carried out by local and international NGOs are instrumental in preventing and mitigating internet shutdowns. For example, Access Now's #KeepItOn campaign, coordinated between 141 organisations in 59 countries, has led to ground-breaking development in digital rights protection. Since the campaign's launch in 2016, the UNHRC officially condemned internet shutdowns, 30 governments of the Freedom Online coalition spoke out against shutdowns, and the campaign strategy helped end major internet shutdowns in Cameroon and Gambia.⁸⁴ Access Now and partner organisations produce resources and give tailored advice to communities, organisations and individuals experiencing internet shutdowns and other digital rights violations. Information gathered throughout

the campaign allows these organisations to make insightful predictions for the future. In Myanmar for example, the #KeepItOn coalition, which includes Access Now, Free Expression Myanmar, Myanmar Centre for Responsible Business, Myanmar ICT for Development Organization and Phandeyar released a statement before the 2020 election, urging for open internet access before, during and after the general election in Myanmar and accurately predicted the violence that would follow the election results and accompanying internet shutdowns.⁸⁵

The importance of the work carried out by NGOs to combat online repression makes them particularly vulnerable to targeted reactions from securitising actors. The Belarusian anti-extremist crusade led to the liquidation of the majority of NGOs in Belarus. According to a review carried out by a Belarusian human rights organisation, by January 2022 governmental authorities liquidated 344 NGOs, while 208 NGOs decided to initiate the liquidation process themselves in fear of further persecution on extremist charges.⁸⁶ Support for and coordination with NGOs by other stakeholders is crucial to ensure the work done is not for nothing. This applies to universities and research institutes. Coordination on research and innovation in technology can lead to important awareness-raising initiatives⁸⁷ and product designs that advance digital rights. Ongoing dialogue and multistakeholder strategies must be pursued to ensure that 'leading democracies can offer a viable alternative to the authoritarian model of cyber sovereignty'.⁸⁸

What to Make of These Responses?

The responses from the international community, the private sector and civil society in the context of

82. *Ibid.*

83. Archana Chaudhary, 'World's Worst Internet Clampdown Cost Myanmar \$3 Billion in 2021', *Bloomberg UK*, 4 January 2022.

84. David Gilmour, 'Meet the Activists Fighting Internet Shutdowns Across the World', *Daily Dot*, 11 November 2018, <<https://www.dailydot.com/debug/internet-shutdown-activist/>>, accessed 20 June 2022.

85. KeepItOn, '#KeepItOn: We Continue to Call on the Republic of the Union of Myanmar to Lift the Internet Shutdowns Imposed in Rakhine and Chin States During Elections and Beyond', Letter addressed to President and State Counsellor of the Republic of the Union of Myanmar, 6 November 2020, <<https://www.accessnow.org/cms/assets/uploads/2020/11/KeepItOn-letter-Myanmar-elections-2020.pdf>>, accessed 20 November 2022.

86. Lawtrend, 'Situatsiya so svobodoj assotsiatsij i organizatsiyami grazhdanskogo obshhestva Respubliki Belarus: obzor za yanvar' 2022 g' ['The Situation with Freedom of Association and Civil Society Organizations in the Republic of Belarus: January 2022 Review'], *Lawtrend*, January 2022, <<https://www.lawtrend.org/freedom-of-association/situatsiya-so-svobodoj-assotsiatsij-i-organizatsiyami-grazhdanskogo-obshhestva-respubliki-belarus-obzor-za-yanvar-2022-g>>, accessed 8 June 2022.

87. According to the Freedom House 2021 'Freedom on Net' Report, studies show that when users become more aware of censorship, surveillance and disinformation, they often take action that enhances internet freedom and protects fellow users.

88. Shahbaz and Funk, 'Freedom on the Net 2021'.

Internet Shutdowns

internet shutdowns in Myanmar and Belarus offer a glimpse of optimism and potential strategies to help mitigate the human rights impact of internet shutdowns. They highlight the ways in which these strategies are dependent on work by and cooperation among the three groups of actors.

Internet shutdowns are a form of violence in themselves, stripping people's freedoms of expression, association, assembly and privacy

The termination of the Cellebrite and Sandvine contracts in Belarus most clearly exemplify this trend. Despite weak responses in practice, condemnation from the international community plays a role in establishing norms. Work by civil society organisations to document and report human rights abuses is equally key in ringing alarm bells. Both processes influence private companies operating on the ground and exert pressure to limit business involvement in the use of the internet as a tool of violence. Careful consideration must be given, however, to the impact of these strategies on citizens. Facebook's actions in Myanmar provide an example of the limitations of reactive strategies. After allegations of Facebook's complicity in the 2014 genocide of Rohingya Muslims, where Facebook's inaction towards hate speech and disinformation led to further violence between the Buddhist majority and the Muslim minority, the social media company took steps to actively remove hate speech from the platform.⁸⁹ Over the years, Facebook proceeded to ban the profiles and channels of Tatmadaw officials, finally reporting to have banned all accounts related to Myanmar's army in the weeks following the February 2021 coup.⁹⁰ In retaliation, the junta blocked the platform from the internet in its entirety. The true losers in this tit for tat were the 28 million Myanmarese for whom Facebook was a primary source of information, a vital organising tool and a connection to the outside world.

Innovation in adaptive technologies to circumvent government-imposed internet shutdowns is

therefore a key strategy that must be pursued alongside economic, political and social pressure. An online community of protest movements around the world has emerged to share documents, tips and recommendations on how to use these technologies to bypass censorship and shutdowns.⁹¹ The use of VPNs exploded in both Myanmar and Belarus in the early days of internet shutdowns, bypassing spying software by encrypting internet traffic and disguising identities. Proxy service Psiphon rotates various censorship circumvention techniques until one is successful, providing users in censored countries with technology to disguise their user identity.⁹² Use of this software is not exclusive to tech 'geeks' either – Psiphon's network in Belarus experienced a surge in use during the August 2020 protests, with 1.76 million daily active users, or roughly 30% of all internet users in Belarus.⁹³ Other loophole technology includes the app Bridgefy, which allows users to send offline messages to others within a certain range through Bluetooth. The willingness of the tech sector to support those experiencing internet shutdowns is vital to upholding human rights in Belarus, Myanmar and all over the world.

Conclusion

Internet shutdowns are a form of violence in themselves, stripping people's freedoms of expression, association, assembly and privacy. The cases of Myanmar and Belarus illustrate how such strategies of digital authoritarianism operate, affect citizens' human rights and impact international relations. The cases further highlight the range of actors active in this field, elongating the chain of influence and responsibility. A human-rights-centred approach is key to effectively interrogating this space, as it ensures that focus remains on those most acutely affected – the citizens. For example, multinational business decisions and international economic tools should be assessed with regard to the impact on the most vulnerable. Decisions to withdraw business operations or implement sanctions have great financial ramifications for state authorities, but the ultimate costs are often borne by the population. In addition, the Russia–Ukraine

89. Saira Asher, 'Myanmar Coup: How Facebook Became the "Digital Tea Shop"', *BBC News*, 4 February 2021.

90. *DW*, 'Facebook Bans all Myanmar Military-Linked Accounts', 25 February 2021.

91. Jamie Terabay, 'Myanmar Citizens Use Protester Toolkit to Skirt Internet Ban', *Japan Times*, 25 March 2021, <<https://www.japantimes.co.jp/news/2021/03/25/asia-pacific/myanmar-protesters-internet-ban/>>, accessed 9 July 2022.

92. Fabian Schmidt, 'Tor, Psiphon, Signal and co.: How To Move Unrecognized on the Internet', *DW*, 8 October 2021.

93. Psiphon Blog, 'Amid Major Network Disruptions, 1.76M Psiphon Users in Belarus', August 2020, <<https://blog-en.psiphon.ca/2020/08/amid-major-network-disruptions-176m.html>>, accessed 9 July 2022.

war has once again shown the shortcomings of these economic tactics, especially against isolationist states that have taken steps to limit their economic dependence on the West.⁹⁴ It should be further kept in mind, however, that securitisation of the internet takes place all over the world, in all types of political systems, and not only during times of political turmoil. Democratic and non-democratic governments around the world have referred to cyberspace as a potential arena for the emergence of threats to national security.⁹⁵ Such securitising practices should be assessed with equal scrutiny and present further research opportunities. ■

Julia Ryng is Digital IR Project Researcher and Coordinator at LSE IDEAS, the foreign policy think tank affiliated with the London School of Economics and Political Science. She is also a PhD candidate in Film Studies at University College London.

Guillemette Guicherd is a Research and Programme Associate at LSE IDEAS.

Judy Al Saman is an MSc International Relations graduate from the London School of Economics and Political Science, and a Research Assistant at LSE IDEAS.

Priyanka Choudhury is an MSc International Relations graduate from the London School of Economics and Political Science, and a Research Assistant at LSE IDEAS.

Angharad Kellett is an MSc International Relations graduate from the London School of Economics and Political Science, and a Research Assistant at LSE IDEAS.

-
94. Nikhil Kalyanpur et al., 'Weaponising the Global Economy', LSE IDEAS, Online Public Event, 3 May 2022, <<https://www.lse.ac.uk/ideas/podcasts/2022/weaponising-economy>>, accessed 10 July 2022. As many foreign businesses have halted their operations in the Russian market in response to the conflict in Ukraine, the International Chamber of Commerce is developing principles for companies leaving markets that are subject to sanctions as a result of conflict. See also remarks by John Denton, 'Russia-Ukraine Dialogues: Corporate Responses', LSE IDEAS, Online Public Event, 12 July 2022, <<https://www.lse.ac.uk/ideas/podcasts/2022/russia-ukraine-dialogues-12-july>>, accessed 15 July 2022.
95. Luisa Cruz Lobato and Kai Michael Kenkel, 'Discourses of Cyberspace Securitization in Brazil and in the United States', *Revista Brasileira de Política Internacional* (Vol. 58, No. 2, 2015), p. 23.